Wireless Design Considerations for Industrial Applications

Preface

Wireless communication in the industrial market has been practiced for many years, often targeted at point-to-point data transfer for supervisory control and data acquisition (SCADA) purposes. Today, plants increasingly use wireless networks for critical Industrial Automation and Control System (IACS) applications that require reliable data transmission with low levels of latency and jitter.

Wireless local area networks (WLANs) differ significantly from traditional wired LANs in their use of shared radio frequencies, susceptibility to interference and coverage impairments. Deploying a wireless network requires thoughtful planning and design, as well as periodic monitoring to meet expectations for bandwidth, throughput, reliability and security.

This application guide details the solutions from Rockwell Automation and Cisco for successful WLAN design and implementation that meet the performance requirements of industrial control applications.

This guide describes the following:

• Industrial wireless use cases and recommended topologies
• Important steps and considerations for WLAN implementation with industrial control applications
• Wireless performance test results and observations
• IACS application recommendations for wireless communication
• Radio frequency (RF) design and WLAN configuration recommendations

A summary of recommendations provided throughout this guide can be found in Chapter 5.

Rockwell Automation and Cisco Four Key Initiatives:

• **Common Technology View:**
  A single system architecture, using open, industry standard networking technologies, such as Ethernet, is paramount for achieving the flexibility, visibility, and efficiency required in a competitive manufacturing environment.

• **Coverged Plantwide Ethernet Architectures:**
  These manufacturing focused reference architectures, comprised of the Rockwell Automation Integrated Architecture™ and Cisco’s Industrial Intelligence, provide users with the foundation for success to deploy the latest technology by addressing topics relevant to both engineering and IT professionals.

• **Joint Product and Solution Collaboration:**
  Stratix Industrial Ethernet products incorporating the best of Cisco and the best of Rockwell Automation.

• **People and Process Optimization:**
  Education and services to facilitate Manufacturing and IT convergence and allow successful architecture deployment and efficient operations allowing critical resources to focus on increasing innovation and productivity.
1. Introduction

1.1 Technology Overview

1.1.1 Industrial Wireless Technologies

A variety of wireless technologies have been established in the industrial space with different characteristics and areas of use (see Table 1-1). The scope of this document is wireless communication based on the IEEE 802.11n standard, with focus on the IACS applications.

Use of wireless communication based on the IEEE 802.11 standards for IACS applications provides the following benefits over other wireless technologies:

- Widely adopted standard-based technology
- Direct transmission of Ethernet-based industrial protocols such as EtherNet/IP™
- Convergence with the existing enterprise WLAN infrastructure
- WLAN mobility and fast roaming capabilities
- Higher throughput and reliability for real-time applications
- 5 GHz spectrum availability with more bandwidth and less interference

Table 1-1 Industrial Wireless Technologies

<table>
<thead>
<tr>
<th>Name</th>
<th>Standard</th>
<th>Frequency Band</th>
<th>Maximum Data Rate</th>
<th>Primary Industrial Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11n</td>
<td>IEEE 802.11</td>
<td>Unlicensed 2.4/5 GHz</td>
<td>300 Mbps</td>
<td>Monitoring and supervisory control Distributed I/O and peer-to-peer control Mobile HMI Outdoor mesh networks Long haul SCADA applications</td>
</tr>
<tr>
<td>802.11a/g</td>
<td>IEEE 802.11</td>
<td>Unlicensed 2.4/5 GHz</td>
<td>54 Mbps</td>
<td>Monitoring and supervisory control Distributed I/O and peer-to-peer control Mobile HMI Outdoor mesh networks Long haul SCADA applications Asset tracking and RFID</td>
</tr>
<tr>
<td>Cellular networks</td>
<td></td>
<td>Licensed and fee-based 700...3600 MHz</td>
<td>Varies</td>
<td>Long haul SCADA applications Remote site connectivity</td>
</tr>
<tr>
<td>Frequency Hopping (FHSS)</td>
<td>Proprietary</td>
<td>Unlicensed 900 MHz 2.4 GHz</td>
<td>11 Mbps</td>
<td>Long haul SCADA applications</td>
</tr>
<tr>
<td>ISA-10011a</td>
<td>IEEE 802.15</td>
<td>Unlicensed 2.4 GHz</td>
<td>250 Kbps</td>
<td>Process control, wireless sensors</td>
</tr>
<tr>
<td>WirelessHART</td>
<td>IEEE 802.15</td>
<td>Unlicensed 2.4 GHz</td>
<td>250 Kbps</td>
<td>Wireless sensors and instrumentation</td>
</tr>
<tr>
<td>VHF / UHF radios</td>
<td>Proprietary</td>
<td>Licensed 150...470 MHz</td>
<td>65 Kbps</td>
<td>Long haul SCADA applications</td>
</tr>
</tbody>
</table>

1  4x4 MIMO, 20 MHz channel
2  Depends on the carrier and distance, theoretical data rates up to 100 Mbps for 4G LTE
A wide number of Ethernet-based industrial protocols exist in IACS networks. This guide covers wireless communication with EtherNet/IP and the Common Industrial Protocol (CIP™) family. EtherNet/IP is a leading open industrial Ethernet network capable of handling the widest range of applications, including discrete, safety, motion, process and drive control. EtherNet/IP uses standard, unmodified IEEE 802.3 Ethernet, IP and TCP/UDP protocols as a mechanism to transport application data between IACS devices. EtherNet/IP is not dependent on the physical media and data link layer and can be run transparently over the 802.11 wireless media as long as adequate performance can be achieved.

EtherNet/IP offers the ability to create a single network infrastructure that integrates industrial and enterprise systems. To support and accelerate this network convergence, Rockwell Automation and Cisco collaborated to develop Converged Plantwide Ethernet (CPwE) Architectures to provide design guidance, recommendations and best practices for wired networks. This document assumes that the reader is familiar with concepts and best practices outlined in the CPwE guide.

1.1.2 Characteristics of Wireless Networks

There are numerous advantages that wireless networks can bring to manufacturing and process applications:

- Lower installation costs due to cabling and hardware reduction
- Lower operational costs by eliminating cable failures
- Ability to connect hard-to-reach and remote areas
- Gains in productivity and efficiency due to equipment mobility
- Higher productivity and less downtime due to personnel mobility

These benefits can only be realized when characteristics of wireless networks are taken into account. Just installing WLAN equipment and eliminating wires will not be enough. WLAN implementation typically requires changes or adaptations on the application level and often in the network infrastructure. After WLAN becomes operational, it needs to be monitored and maintained to a higher degree than a wired network, specifically in regards to radio frequency (RF) spectrum and security.

Here are some of the characteristics that make wireless communication fundamentally different from wired media.

- *There are no clear boundaries within which the wireless network packets are guaranteed to be received.* The wireless signal propagation and the ability to receive it correctly can be influenced by many factors, for example antenna parameters and orientation, absorption and reflection of signal by obstacles, amount of noise in the channel and so on. These factors are dynamic and subject to change for any WLAN environment. As a result, a wireless coverage area cannot be precisely determined and is always designed with some margin. A site survey is a requirement for a WLAN deployment.

- *The wireless signal has time-varying and asymmetric properties.* Not just mobile, but also stationary devices may suddenly experience poor signal because of changing environment or increased interference. In addition to that, wireless signal can be asymmetrical (i.e. having good signal properties in one direction but not in the opposite direction).

- *Wireless signal may reach beyond the intended area.* Logically separated WLAN networks on the same radio channel can interfere with each other at large distances. This can be a challenge for high-density deployments where wireless channels have to be reused. Another concern is that WLAN security attacks are possible that can bypass physical guard measures.
• The throughput is limited due to half-duplex shared medium. Wireless nodes in the channel have to share the medium and can only transmit one at a time. Half-duplex communication and collision avoidance mechanism in the 802.11 wireless limits the throughput. The number of nodes and their traffic patterns are as important for performance as the amount of data being transmitted.

• Wireless media is not lossless compared to the wired Ethernet. In the normally functioning full-duplex switched wired network, there should be no lost or corrupted frames. On the contrary, even a lightly loaded wireless network has some amount of frames lost due to collisions. These frames have to be retransmitted which increases latency and jitter, or may even be dropped altogether. The application should be designed to tolerate this behavior.

• Wireless communication is less protected from interference. Poor performance or loss of service may be caused by interference from the neighboring WLANs and non-Wi-Fi devices. This risk should always be considered and evaluated for the application.

• Wireless networks have dynamic topologies. In many WLAN implementations, wireless nodes change association from one access point to another. Such wireless roaming changes their place in the overall network infrastructure which rarely happens for wired nodes. The roaming behavior may require certain level of WLAN design and configuration to meet the application requirements.

1.1.3 Wireless Client Types

There are several methods of how a client device can be connected to a WLAN:

• Embedded wireless adapter and antennas

• External wireless adapter for a single client (bridge)

• Wireless bridge to connect multiple wired clients (workgroup bridge)

1.1.3.1 Embedded wireless adapter

Conventional wireless clients such as laptops or phones, as well as mobile HMI devices, use built-in wireless adapters and antennas. However, having an embedded wireless module for each IACS device such as PAC or I/O chassis is not feasible for the majority of applications. The main reasons are antenna type limitations, cabinet placement restrictions, and excessive number and density of wireless nodes.

Although embedded 802.11a/b/g adapters for PAC and I/O platforms exist, they are not considered in this guide. Mobile HMI is the main class of devices with an embedded wireless adapter that are commonly used with IACS applications.

1.1.3.2 Single Client (Universal) Bridge

An external adapter (a wireless Ethernet bridge) for each individual PAC or I/O device can solve the placement and antenna problems of the embedded adapters. The limitation of the traditional wireless bridge is that it can only connect a single wired client (one MAC address). It cannot be used to manage multiple devices over the wireless link (including the bridge itself).

This mode is called Universal Bridge in Cisco documentation. It is not considered in this guide because of the single MAC address limitations and lack of other features.
1.1.3.3 **Workgroup Bridge**

The ability to connect several wired clients with a single wireless bridge can solve many of the mentioned problems. This feature is implemented in a workgroup bridge (WGB) which is a proprietary mode of operation supported by Cisco autonomous access points (AP).

A workgroup bridge learns MAC addresses of its wired clients on the Ethernet interface and reports them to the AP using Inter-Access Point Protocol (IAPP) messaging. A WGB establishes a single connection to the AP and is viewed as a single wireless client in the network.

- This guide is focused on WGB topologies as the primary method of connecting IACS devices to a WLAN.

An example of a topology using different types of wireless clients is shown below.

![Figure 1-1 Wireless Client Types](image)

1.1.4 **Wireless Cell/Area Zone**

A number of wireless stations (clients) communicating to a single AP on the same channel is known as a *Basic Service Set* (BSS) in IEEE terms. Multiple BSS within the same WLAN infrastructure create an *Extended Service Set* (ESS). Within the ESS, each AP coverage area typically overlaps with adjacent coverage areas for continuous wireless coverage.

The ESS is identified by a service set identifier (SSID), commonly called a “network name.” An ESS can be loosely compared to a VLAN in a wired network, and there can typically be a one-to-one relation between them. There could be several SSIDs defined on a single AP to serve different types of clients, for example: guests, corporate users, or wireless phones. It is important to note that while these clients are logically separated within the network, they may still share the same radio channel and interfere with each other on the physical layer.
The BSS/ESS concepts should be matched with the Cell/Area Zone concept in the IACS reference model. A Cell/Area Zone is a set of IACS devices that communicate with each other to control a particular functional aspect of the industrial process. For more details, refer to chapter 2 of the Converged Plantwide Ethernet (CPwE) Design and implementation Guide.

A wireless Cell/Area Zone can span one or many wireless coverage areas, depending on the application. For the purposes of this guide, this is defined as a Control Cell/Area Zone. The subset of the zone that is served by a single AP (i.e., a wireless cell coverage area) is defined as Coverage Cell/Area. A Coverage Cell/Area may also have two BSS operating on two radios, for example one for machine control purposes using 5 GHz radio, and the other for operator access using 2.4 GHz radio.

Figure 1-2 Wireless Cell/Areas Zone Example

1.1.5 WLAN Architecture Types

1.1.5.1 Autonomous WLAN Architecture

The autonomous architecture consists of standalone access points that implement all of the WLAN functions – management, control, data transport, client access, and distribution system across several APs. An example of an autonomous access point is any Cisco access point capable of using Cisco IOS software, like Cisco 2600 series.

- WGB mode is only supported by autonomous APs.

Each autonomous AP is configured and managed individually, with limited coordination of operation between autonomous APs. This makes it difficult to implement scalable solutions for configuration and firmware management, radio resource management, user mobility, interference monitoring, security enforcement, and threat prevention.
The limitations of the autonomous architecture make it unsuitable for large scale plant-wide deployments with wide range of clients and applications. Autonomous WLAN architectures are normally used in small scale deployments and/or for specialized areas of use, for instance a remote office, wireless hotspot, point-to-point communication and so on.

For industrial networks, autonomous architectures can be used to support stand-alone IACS applications with fixed number of clients, tightly controlled data traffic, and in the dedicated set of radio channels. An example of the autonomous WLAN is shown below.

**Figure 1-3 Autonomous WLAN Example**

1.1.5.2 **Unified WLAN Architecture**

Unified WLAN architecture is a scalable solution for large scale plant-wide deployments of wireless infrastructure. In the Unified Access architecture, the WLAN functionality is split between lightweight access points (LAP) and wireless LAN controllers (WLC).

The key concept is that non-real-time 802.11 control and management functions are centralized in the WLC allowing operation optimization and scalability of WLAN infrastructure. The real-time 802.11 functions, such as client association and encryption, are distributed to lightweight or “thin” APs (see Figure 1-4).

In addition to base functionality provided by LAP and WLC, Unified Access network platform includes comprehensive solutions for:
- WLAN management, end-user connectivity, and application performance visibility with Cisco Prime Network Control System (NCS)
- Advanced spectrum analysis, location services, and wireless intrusion prevention system (wIPS) with Cisco Mobility Services Engine (MSE)
- Design and implementation of security policy across the entire network with Cisco Identity Services Engine (ISE) software

Click on the following for more information on:
- Cisco Unified Access products and solutions
- Enterprise Mobility 7.3 Design Guide

Figure 1-4 WLAN Functional Implementation

The lightweight APs are typically “zero-touch” deployed and individual configuration is not required. The configuration parameters, firmware updates, diagnostic information, and other control traffic are exchanged between LAPs and WLCs in the CAPWAP (Control and Provisioning of Wireless Access Points) protocol. CAPWAP control messages are secured in a Datagram Transport Layer Security (DTLS) tunnel.

Autonomous APs in WGB mode can join Unified WLAN and communicate with LAPs and WLCs using IAPP protocol. They are, however, managed separately from the lightweight APs.

**Data Flow in Unified Architecture**

The WLAN client data packets can be carried to the WLC (centralized data switching) or bridged locally on the LAP (local data switching), depending on the mode of operation.

In a centralized data switching by a WLC, the traffic flow is as follows (assuming wired to wireless client communication):

- Data packets are encapsulated in the CAPWAP tunnel by the LAP and forwarded to the controller.
- WLC receives the encapsulated packet, removes the CAPWAP header, and switches the packet onto a VLAN in the wired infrastructure.
When a client on the wired network sends a packet to a WLAN client, the packet first goes into the WLC, where it is encapsulated with a CAPWAP header and then forwarded to the LAP.

The LAP extracts the data from the CAPWAP packet and transmits it in the WLAN.

The CAPWAP data path between controller and AP can be optionally secured through DTLS which can make it more secure than the normal wired Ethernet communication.

An example of Unified WLAN architecture is shown in Figure 1-5.

**Unified vs. Autonomous Architecture**

Unified Access WLAN architecture presents a number of advantages even for smaller deployments (fewer than 10 APs) and the only practical choice for large scale plant-wide WLAN infrastructure. The main advantages of the Unified Access WLAN architecture:

- Ability to support large scale WLAN deployments with reduced operating expenses through centralized management and control of lightweight APs
- Zero-touch deployment and replacement of the APs
- Reduced efforts and consistency when updating configuration and firmware
• Dynamic adaptive RF configuration and built-in radio spectrum analysis
• Increased reliability with failover and self-healing mechanisms
• Enhanced security services with centralized control and visibility
• Support for contextual mobility applications such as location services, intrusion prevention, and wireless guest access

Autonomous architecture can offer the following advantages:
• Lower initial costs without requiring a WLC
• Lower expertise level and simplified initial setup
• More granular control of certain WLAN parameters

Autonomous architectures can be selected for IACS applications because of lower capital cost and certain configuration and performance requirements. Both types can coexist in the WLAN infrastructure with autonomous WLANs deployed in some Control Cell/Area Zones, and Unified WLAN being used in other zones and throughout the plant.

In the mixed environment, Cisco WLCs and NCS can provide limited management features and visibility for the autonomous APs and WGBs. Most Cisco APs can be converted from autonomous to lightweight mode in the field. This provides an upgrade path to the Unified architecture.

### 1.1.5.3 Wireless Mesh Architecture

A wireless mesh network consists of mesh APs that communicate with each other using wireless backhaul connections and do not require a wired Ethernet as a backbone. A mesh network is beneficial for areas where it is not feasible to install wired Ethernet cabling, (i.e., large outdoor areas, auditoriums, stadiums, and construction sites). Mesh technologies are successfully used in heavy industries such as mining, energy, and oil and gas. Outdoor mesh APs can provide point-to-point and point-to-multipoint connectivity between remote sites for SCADA applications.

In the Cisco Unified Access platform, lightweight APs can be configured in the mesh mode and used in the WLAN infrastructure along with non-mesh LAPs (see Figure 1-6 as an example). Access points within a mesh network operate in one of the following two ways:

• Root access point (RAP) with wired connectivity to the WLC
• Mesh access point (MAP) with wireless only connectivity

The limitations of mesh architecture for IACS applications are:
• Increased latency due to number of wireless hops and reduced backhaul rate
• Increased roaming time compared to normal Unified architecture

Because of the limitations mentioned above, mesh architectures are currently not recommended for real-time control purposes such as CIP Class 1 I/O or Produced / Consumed traffic.

Wireless mesh architectures are out of this guide’s scope. Information about Cisco wireless mesh products and solutions can be found at:

**Outdoor Wireless Network Solution**

**Cisco Wireless Mesh Access Points Design and Deployment Guide**
1.2 Wireless Equipment Use Cases

The main usage classes for wireless in the industrial environment are:

- Wire Replacement / Equipment Mobility
  - Hard to reach (costly) and inaccessible areas
  - Moving parts on static machines
  - Portable or moving equipment
- Long Haul SCADA Communication
- Process Instrumentation
- Personnel Mobility
  - Mobile HMI and operator access
  - Maintenance and engineering access
  - Wireless voice communication
  - Vendor guest access
• Asset and Personnel Tracking
  - Radio Frequency Identification (RFID)
  - Real Time Location Services (RTLS)
• Remote Device Monitoring
  - Condition-based maintenance
  - Instrumentation of existing machinery
  - Video surveillance

This section describes the main network topologies for Wire Replacement and Equipment Mobility use case, the main focus of this guide. This use case includes a wide variety of applications that may have very different characteristics and require different approach to WLAN design and implementation.

The main characteristics by which these applications can be classified are:
• Type of wireless client (embedded or bridged) – as described in the section 1.1.3
• Equipment mobility type (1.2.1)
• Wireless topology type (1.2.2)
• IACS protocol type (2.2.1)

1.2.1 Equipment Mobility Type

Wireless equipment can be characterized by the type of mobility and operational requirements when relocating within the WLAN infrastructure. When connected to a particular SSID in a Control Cell/Area Zone, wireless equipment may stay in the same Coverage Cell/Area (i.e., remain associated to one AP) until powered down or disconnected, or it may move between the coverage cell/areas (roam) while remaining operational.

1.2.1.1 Single Coverage Cell/Area Operation

The single Coverage Cell/Area use cases can be defined as:
• Fixed Position – equipment is static while operating and has a permanent location. This is an alternative to a wired connection for hard to reach and remote locations where cabling is too expensive or impossible to install. Typical usage areas are process control, machine condition monitoring, fixed environmental monitoring, RTU for water/wastewater and energy industries, etc.. An example could be a stand-alone OEM machine that needs to be integrated into a production line over a wireless link.
• Nomadic (Non-operational Relocation) – equipment stays in place while operating and then moves to a new location in the shutdown state. After relocation, new wireless connection needs to be established. For example: process skids, storage tanks, reactors, and portable manufacturing equipment in a variety of industries.
• Mobile (Operational Relocation) – equipment changes position during the operation while remaining in the same Coverage Cell/Area. For example: rotary platforms and turntables, Automated Storage and Retrieval Systems (ASRS), assembly systems with tracks, overhead cranes and similar machinery that use wireless as a replacement for often not reliable wired solutions (such as inductive rails and slip rings). These applications may require rapid changes in position and orientation of the wireless client relative to the access point.
### 1.2.1.2 Multiple Cell Operation (Roaming)

Examples of roaming equipment are devices that operate in large areas such as automatic guided vehicles (AGV), large ASRS, overhead cranes, and train cars. When a wireless client roams to the new Coverage Cell/Area, it associates to a new AP. The association process causes a delay in communication (roaming time) due to security credentials exchange and network convergence. Roaming time depends on several factors:

- Roaming in a single channel versus between channels
- Type of security authentication
- Fast roaming protocol supported by APs and clients
- Criteria that triggered roaming (e.g., signal strength, data rate change, loss of AP beacons)
- Autonomous versus Unified WLAN

Roaming time may cause the application connection loss depending on the update rate and timeout parameters. The application can be designed to tolerate this behavior and reestablish connections as needed. In other cases, application parameters may need to be adjusted to allow for roaming delays.

It is important to remember that roaming may occur even when equipment is static or not intended to move beyond its Coverage Cell/Area. For example, the original AP may fail or its signal quality may degrade below the roaming threshold. In such case, the wireless client may be able to associate to another AP in the overlapping coverage area, or to a backup AP in the same area.

The use cases described above and symbolic icons for them are shown in Figure 1-7.

**Figure 1-7 Equipment Mobility Types**
1.2.2 Wireless Equipment Topologies

A number of different topologies are presented here that are the most common wireless use cases for IACS equipment. The pictures below use autonomous architectures with WGBs as examples.

1.2.2.1 Wired PLC to Wireless I/O

In this topology, a fixed PLC communicates with a number of mobile I/O devices behind WGBs. This use case has the following characteristics:

- Each wireless link may carry data for several individual CIP connections, depending on the application:
  - Rack optimized discrete I/O connections
  - Analog or discrete direct I/O connections
  - Safety I/O connections
- Large connection counts increase the packet rate in the channel and limit the scale of this topology (see 2.1.2)
- Packet sizes are usually small (less than 200 bytes for Ethernet frames)
- Traffic flow may be more predictable, for example due to the PLC-driven I/O update mechanism.

Figure 1-8 Wired PLC to Wireless I/O Topology
In general, more than one EtherNet/IP I/O device can be connected to a WGB (in linear topology or via a switch). However, since each EtherNet/IP adapter, an analog I/O or a safety I/O module adds to the CIP connection count and increases the packet rate, the total number of devices is limited by the available bandwidth in the channel (see 2.1.2).

### 1.2.2.2 Wired PAC to Wireless PAC

In this topology, a fixed PAC communicates with a number of mobile PACs behind WGBs (peer-to-peer communication). This use case has the following characteristics:

- Each wireless link carries several classes of data:
  - Produced / Consumed tags
  - Safety Produced / Consumed tags
  - Virtual Produced / Consumed motion axis
  - CIP Sync™ communication
  - Message instructions
  - HMI and tool traffic (RSLogix™, RSLinx®, HTTP etc.)
- Data can be aggregated into fewer Produced / Consumed tags of larger size which lowers the total packet rate
- Packet sizes can be medium to large (up to 572 bytes Ethernet frames) depending on data structures
- PAC to PAC communication is less predictable since each data stream is produced independently

Figure 1-9 Wired PAC to Wireless PAC Topology
Each mobile PAC may have wired I/O or drives connected using a linear topology, a switch, or a second Ethernet module. While these devices can be reached over wireless for diagnostic or configuration purposes, it is assumed that all real-time control is done locally by a mobile PAC.

The advantage of dual Ethernet modules on the mobile PAC is reducing unnecessary broadcast and multicast traffic across the wireless link. However, physical segmentation via the ControlLogix backplane does not allow non-CIP traffic to reach remote devices over wireless, for example to browse diagnostic webpages or configure the switch.

### 1.2.2.3 Wireless PAC to Wireless PAC or I/O

In certain applications, a mobile PAC may need to communicate to another mobile PAC or a mobile I/O device in the same Coverage Cell/Area. An example would be machine interlocking, safety status, and listen-only I/O connections. In the traditional (not a mesh or ad-hoc) wireless mode, such topology requires data to be send upstream from the WGB to the AP and then downstream to another WGB.

- Wireless to wireless topology doubles the number of packets that needs to be transmitted and inefficiently uses the available bandwidth. Network latency can be more than twice as high.
- Wireless PAC to wireless PAC or I/O communication should be limited and kept at low rates.

Wireless to wireless topology is not covered in this guide.

**Figure 1-10 Wireless to Wireless Topology**
1.2.2.4 **Fast Roaming Topology**

The roaming topology can be viewed as an extension of wired PAC to wireless PAC or I/O topologies described above. This use case has the following characteristics:

- Mobile machinery that moves between Coverage Cell/Areas during the operation, typically following a predetermined path.
- Coverage areas have to overlap to allow for seamless roaming.
- Wireless infrastructure supports fast roaming with typical times below 50ms.
- Total convergence delay during the roaming process should not cause application timeouts.
- Unified WLAN architecture is preferred for these reasons:
  - Proven and tested fast roaming mechanisms
  - Better support for plant-wide coverage with large number of APs
  - Reuse of existing plant WLAN infrastructure that already support fast roaming

Wireless roaming implementation details and recommendations will be covered in the future versions of the guide.

*Figure 1-11 Fast Roaming Topology with Unified Architecture*
1.2.3 Mobile HMI and Engineering Access

Other important use cases for plant-floor wireless communication are:

- Mobile HMI and operator access
- Maintenance and Engineering Access
  - RSLogix5000 and other programming tools
  - Webpage configuration and diagnostics

There are several places where HMI devices can be used in the WLAN (see Figure 1-12):

- Infrastructure HMI (wired) shows the global view of the system (consolidating some of the mobile information) and on-demand copies of the individual mobile views (per machine or zone).
- Mobile Equipment HMI (wired) shows the global view over wireless and the local view over a wired network.
- Mobile Operator HMI (wireless) shows the consolidated global view and on-demand mobile views (per machine or zone) depending on where the operator is located.

A wireless HMI client or an engineer’s laptop can communicate with the AP using either 2.4 GHz or 5 GHz radio, and can operate within the same SSID in the Cell/Area Zone, or use a dedicated SSID for logical segmentation. This type of traffic should be prioritized as “best effort” in the Quality of Service (QoS) configuration.

Figure 1-12 Mobile HMI and Engineering Access
2. Application Considerations

2.1 General Considerations

2.1.1 Preparing for a WLAN implementation

There are many factors that need to be considered before implementing a WLAN with industrial control applications. The first step is to obtain detailed information about the location and existing network infrastructure, and identify application and network requirements.

2.1.1.1 Site Requirements

A successful WLAN implementation should consider requirements and characteristics of the industrial facility. Proper RF design and comprehensive site survey are crucial for any WLAN installation, but even more important for IACS applications with less tolerance to interference, latency, and jitter.

If the network architecture is to be replicated in other locations, the design should allow for the variability of parameters (e.g., the number of available wireless channels or potential radio interference on site).

The following list describes some of the more important information that needs to be obtained for every site:

- Number of exclusive wireless channels available in 2.4 GHz and 5 GHz band
- Wireless channels in use by the existing equipment and personnel
- IT policy regulating wireless spectrum in the facility
- Existing and potential sources of wireless interference in the area
- Possibility of weather, navigational, or military 5 GHz radars operating in the area
- Locations and dimensions of required signal coverage areas
- Material compositions of all the coverage areas in a site
- Any obstructions that may enter and leave the coverage areas
- If a site survey has been done and what were the criteria and equipment used
- Environmental characteristics of the site
- Installation limitations for the antennas, APs, and cabling

RF design and recommendations are covered in section 4.1 of this guide.

2.1.1.2 Network Requirements

Most industrial plants already have existing WLAN installations that cover parts or all of the facility. These wireless networks are typically managed by the IT department and are used by plant personnel to access enterprise resources or to manage plant equipment.

The new wireless IACS application can be a stand-alone deployment using an autonomous WLAN architecture, or can be integrated into existing plant-wide infrastructure, usually a WLC-based architecture. In any case, existing network requirements, limitations, IT policies, and management practices must be considered before implementation. Same as with wired network integration, early collaboration with IT personnel is critical. The following is the list of topics that should be considered:

- WLAN management method (autonomous or controller-based)
- Existing WLAN infrastructure
- Existing switch infrastructure information
  - Port capacity and speeds
- Power over Ethernet (PoE) capabilities
- Proximity to possible AP locations
- Who is responsible for managing WLAN?
  - Architecture practices
  - RF policy and channel allocation
  - Device installation and configuration
- Required WLAN security
  - Encryption type
  - Authentication methods and servers
  - Rogue detection and prevention policy
  - Interference monitoring
- IP addressing methods and DHCP information
- VLAN requirements
- Required network redundancy
  - Device level – AP, WGB, WLC, switch
  - Media redundancy – copper, fiber, port aggregation
  - Worst case failover time

2.1.1.3 Application Requirements

During the planning phase, worst case communication requirements for the application have to be determined. This information will help to decide if wireless communication is appropriate for the application, and what kind of WLAN infrastructure is needed to support it. The requirements may vary as mobile devices relocate, in which case they need to be estimated for each coverage area.

The following information should be available:
- Number and type of devices, including embedded wireless and bridged wireless
- Number of independent wireless clients per channel (e.g., WGBs or embedded adapters)
- Type of CIP protocols required by the application
- Non-CIP traffic that goes over wireless
- Packet intervals, size, and packet per second (PPS) rate for each type of traffic
  - Explicit Messaging
  - Standard Produced / Consumed
  - Standard I/O
  - Safety Produced / Consumed
  - Safety I/O
  - Motion Produced / Consumed (Virtual Axis)
- Motion I/O
- CIP Sync
- Total PPS per wireless channel
- Directional flow of the traffic per protocol
- Application timeout requirements per protocol
- Maximum tolerable latency and jitter for the application per protocol
- Handling of lost or late data packets by the application
- Time synchronization requirements
- Equipment mobility requirements (see 1.2.1) including:
  - Fixed position
  - Non-operational relocation (nomadic)
  - Operational relocation (slow movement with no roaming)
  - Rotary platforms (rapid movement and re-orientation with no roaming)
  - Roaming where connections are broken and reestablished
  - Fast roaming with no connection loss
- If multiple identical applications need to operate throughout the plant
  - Number of installations
  - Distance between each operation area

2.1.2 Packet Rate Limitations

2.1.2.1 Overview

The packet rate (number of data packets per second), as opposed to the data rate (number of bits per second), is the most important parameter limiting the bandwidth of a wireless channel. Time required to transmit each data bit can be reduced with higher 802.11n data rates (assuming that those rates are achievable between an AP and a client). However, channel access overhead in the 802.11 protocol is fixed per packet, regardless of its size. Each transmitted packet adds additional delays:

- Interframe space time
- Random backoff time to avoid collisions
- 802.11 preamble and MAC frame header transmission
- Acknowledgement (ACK) frame transmission

Figure 2-1 Wireless Transmission Cycle
Maximum theoretical packet rates (without aggregation) can be estimated by calculating these delays and transmission times for various packet sizes and QoS parameters. These numbers represent the ideal case of 100% channel utilization with packets that are uniformly distributed in time. However, the real achievable packet rate for a typical IACS application is lower due to the following:

- 802.11 control and management frames use some of the bandwidth
- Higher number of wireless nodes increases the chance of collisions and number of retries
- Data sent independently by each device with no precise timing (this contributes to collisions and additional jitter in the wireless channel)
- Asymmetry of traffic, different packet sizes and QoS priorities in the channel can negatively affect the sustainable packet rate
- There has to be a safety margin to allow for possible interference and signal degradation

Recommendations for packet rate and other application parameters are provided in section 2.2.3.

2.1.2.2 Traffic Optimization

A number of application optimization methods can be used to lower the total packet rate and improve the performance, such as:

- Rack optimized I/O connections should be used when possible.
- Produced / Consumed connection pairs between controllers are more efficient than multiple I/O connections.
- Instead of using direct wireless communication from multiple PACs, aggregate wireless traffic through a single PAC in the wired infrastructure.
- Instead of using many individual connections, Produced / Consumed data can be combined into large arrays and user-defined data types (UDT) with one or few connections.
- Different types of data can be carried in the one Produced / Consumed tag. For example, standard data can be appended to the safety Produced / Consumed data if RPI (Requested Packet Interval) is sufficient.
- The most efficient situation is transmission of one wireless packet in each direction during a cycle.

2.1.2.3 Number of Wireless Nodes

The achievable packet rate depends greatly on the number of wireless clients in the cell. The chance of collisions is higher with a greater number of clients because of random unscheduled access to the channel. In a heavily loaded channel, adding more clients affects the performance in non-linear way.

Rockwell Automation and Cisco have tested IACS application performance with up to 12 WGBs in the cell. For higher node count, total packet rate may need to be lowered.

- It is recommended not to exceed 20 wireless nodes (WGBs or embedded adapters) per AP for EtherNet/IP applications.
- Limit the number of wired clients that communicate over wireless link to 19 per WGB.
- The total number of Ethernet devices on a single VLAN (wired or wireless) should be below 200 to restrict the amount of broadcast traffic.
2.1.3 Wireless Latency and Jitter

Wireless communication causes higher latency and jitter for real-time IACS traffic when compared to wired Ethernet. However, in a channel loaded below the limit and with proper wireless QoS policy, the average latency and jitter should meet the performance requirements of typical applications. Normally only a very small percentage of real-time packets are delayed significantly enough not to be usable.

Some considerations regarding wireless latency and jitter:

- Overloading the channel will quickly lead to excessive latency and application timeouts.
- Larger number of wireless nodes increases maximum latency due to the contention for the channel access. The average latency, however, may not change significantly.
- Wireless QoS parameters have direct impact on the latency (see 4.2.2).
- Very low RPIs (faster than 5ms) may not be useful for wireless applications.
- Certain events can also cause significant delays and packet drops:
  - Wireless roaming
  - Periodic RF monitoring of channels, if enabled (see 4.1.8).

Test results for wireless latency can be found later in this guide (see Appendix A).

2.1.4 Packet Loss and Reliability

In EtherNet/IP networks, a connection timeout occurs when data packets are not received within a certain period of time, depending on the RPI, CIP protocol type, and connection multipliers. A timeout can be caused by delayed or lost packets, or both.

In 802.11-based wireless networks, data delivery cannot always be guaranteed due to collisions in the shared wireless media. Another factor is data corruption due to interference or a poor signal. If a wireless frame is not received, it will normally be retransmitted. This method provides a certain level of reliability; however it is necessary to limit the number of retries and time allowed for transmission of a single frame. Such limits prevent excessive delays for all packets in the queue.

Based on the above, some data packets are expected to be dropped in the wireless channel. The number of lost packets should be quite small if the channel load and other parameters are met. While it is not possible to create a lossless wireless communication channel, the achievable goal is to minimize a chance of the CIP connection loss to satisfy application requirements and provide the highest possible network uptime.

Below are some considerations when evaluating the reliability of wireless communication:

- Exceeding packet rate limits causes high packet loss and application timeouts.
- Systems with larger number of wireless nodes may have higher chance of timeouts.
- An application should be able to tolerate occasional packet loss. Test results show that with normal channel load, RF conditions, and recommended QoS configuration, the expected application-level packet loss is very small.
- Application parameters may need to be adjusted to avoid timeouts.
- Multicast and broadcast traffic is delivered without retries or acknowledgements, has a higher packet loss, and is much less reliable than unicast traffic (see 2.1.5).
- Changes in RF environment, interference, or unauthorized channel transmissions may decrease reliability or even completely disrupt wireless communication. This risk should always be considered for the application.
2.1.5 Unicast vs. Multicast

CIP EtherNet/IP protocols support unicast as a default method of communication, with the exception of the ControlLogix® Redundancy system and CIP Sync traffic at this time. It is recommended to use unicast EtherNet/IP connections where possible.

Table 2-1 Unicast support for Ethernet/IP

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Unicast Support / RSLogix version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard I/O</td>
<td>v18 (ControlLogix Redundancy - multicast only)</td>
</tr>
<tr>
<td>Standard Produced / Consumed</td>
<td>v16 (ControlLogix Redundancy – multicast only for consumed tags)</td>
</tr>
<tr>
<td>Safety I/O</td>
<td>v20</td>
</tr>
<tr>
<td>Safety Produced / Consumed</td>
<td>v19</td>
</tr>
<tr>
<td>CIP Sync</td>
<td>Multicast only (as of v21)</td>
</tr>
</tbody>
</table>

Although multicast delivery is supported by the 802.11n standard, its use with wireless EtherNet/IP traffic presents challenges:

- Multicast frames are not acknowledged and not repeated if lost. This can greatly increase the chance of connection timeouts.
- Additional network configuration is required to control multicast traffic (IGMP snooping and querier).

These factors are applied to multicast data delivery from the AP to wireless clients. The result can be much lower reliability of multicast EtherNet/IP traffic which is not acceptable for a critical application. Multicast can still be used with CIP Sync where packet rate is low and loss can be tolerated.

Multicast data from wireless clients to the AP is transmitted as unicast frames. This is a more reliable exchange, because acknowledgements are used. The AP then extracts the multicast payload from the unicast frame and sends the payload within a true multicast frame. The multicast frame may be, in turn, transmitted to other wireless clients downstream, if they are subscribed to the multicast group.

IGMP snooping and querier is needed to enable multicast delivery to wireless clients.
- Use unicast connections with wireless I/O or Produced / Consumed data
- Do not use ControlLogix Redundancy System with wireless communication
- Configure IGMP snooping and querier in the network infrastructure
2.2 Application Protocols

2.2.1 Overview

Table 2-2 lists various CIP protocols and their potential use with 802.11n wireless communication. The recommended topologies and performance test results for certain types of protocols can be found later in this chapter.

Table 2-2 Use of IACS protocols with 802.11n wireless

<table>
<thead>
<tr>
<th>IACS Protocol Type</th>
<th>CIP Standard</th>
<th>Use with Wireless</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information and diagnostics, process control</td>
<td>CIP Class 3 (HMI)</td>
<td>Yes</td>
<td>–</td>
</tr>
<tr>
<td>Peer to peer messaging</td>
<td>CIP Class 3 (MSG instructions)</td>
<td>Yes</td>
<td>–</td>
</tr>
<tr>
<td>Peer to Peer Control</td>
<td>CIP Class 1 Produced / Consumed</td>
<td>Yes</td>
<td>Higher latency and jitter may be an issue if an application depend on exact timing of updates</td>
</tr>
<tr>
<td>I/O Control</td>
<td>CIP Class 1 I/O</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Safety Control</td>
<td>CIP Safety</td>
<td>Yes</td>
<td>Very fast safety reaction times may not be supported (see 3.3.2)</td>
</tr>
<tr>
<td>Time Synchronization (IEEE 1588 PTP)</td>
<td>CIP Sync</td>
<td>Limited</td>
<td>Accuracy of ~150 μs can be achieved; suitable for SOE and event logging applications; (see 2.2.2.5)</td>
</tr>
<tr>
<td>Motion Control</td>
<td>CIP Motion; Produced / Consumed Virtual Axis</td>
<td>Experimental</td>
<td>Position accuracy depends on CIP Sync performance; Direct CIP Motion™ control is not feasible; Virtual Produced / Consumed axis may be possible for low performance applications</td>
</tr>
</tbody>
</table>

1 PTP support in wireless hardware is required for greater accuracy which is not available in current products

It is expected to find a mix of protocols in a typical IACS application, including some amount of non-CIP traffic for network control. As in wired networks, prioritization of traffic with QoS becomes critical where the protocols are mixed and bandwidth is limited. QoS configuration and recommendations are covered in section 4.2.2.3.

2.2.2 Protocol Characteristics

This section briefly describes characteristics of different CIP family protocols that are relevant to wireless communication.

2.2.2.1 Standard I/O

EtherNet/IP I/O packets are usually small in size (below 200 bytes) which limits the efficiency of wireless communication. 802.11 protocols allow sending up to 2304 bytes in a single wireless frame (without aggregation mechanisms).
• An RPI below 5 ms for an I/O connection may not be practical for wireless media because latency and jitter become comparable or greater than the RPI. Motion I/O is especially sensitive to latency because the loop is closed within the coarse update rate.

• Each I/O connection (direct or rack-optimized) creates a bidirectional data stream and increases the total packet rate. A system with large number of analog I/O modules or individual I/O racks may exceed the available channel bandwidth in packets per second. In such case, RPI values should be lowered or the system should be scaled down. Sometimes, the solution is to use Produced/Consumed tags over wireless and to install a PAC on the mobile equipment for I/O control.

• Standard I/O has a timeout period of 100 ms or greater, and can tolerate at least three lost packets in a row. If channel utilization is within the limits, then the latency in wireless media should not cause a standard I/O timeout.

• For low RPIs, connection timeout is not a good indication of whether the application requirements are satisfied. For example, if the RPI is set to 10 ms, some packets may be delayed more than 100 ms and the I/O connection still would not time out. However such high jitter is unlikely to meet application requirements. The degree to which lost or delayed packets can be tolerated is application-specific. The following rule has been adopted for the wireless performance testing:
- Acceptable performance is where 95% of packets arrive within 1.5x RPI;
- There should be no connection timeouts.

**2.2.2.2 Standard Produced / Consumed**

• The maximum Produced / Consumed tag size is limited to 512 bytes in the CIP specification. Application data should be aggregated into large arrays or UDTs in order to reduce the number of connections and create larger packet sizes for more efficient wireless transmission.

• As with the standard I/O, RPI below 5ms for a Produced / Consumed connection may not be practical for wireless media.

• Depending on the application, packet rate may be different for data going upstream (WGB to AP) or downstream (AP to WGB). As a result, two applications with the same total packet rate in the channel may experience different latency depending on the packet rate in each direction.

• The timeout and latency requirements for standard Produced / Consumed tags are the same as for the I/O data (see above).

**2.2.2.3 Safety I/O**

• In GuardLogix system, the default RPI is 10 ms for safety input connections and 20 ms for safety output connections (Safety Task period). The default multiplier values are x2. These values may need to be increased from defaults to account for higher latencies in the wireless media.

• All safety output tags are updated at the conclusion of safety task execution, and are sent to the network as a burst of packets. This is different from the standard I/O updates that are distributed more evenly. These patterns lead to less efficient utilization of wireless media than the standard I/O, and may lower the achievable packet rate.

• Safety I/O modules do not support rack-optimized mode and use direct connection mode only. Each module adds to the total packet rate, so a large safety I/O system may exceed the available channel bandwidth in packets per second. In such case, RPI values should be lowered or the system should be scaled down. It may be necessary to use safety Produced / Consumed tags over wireless and to install a safety PAC on the mobile equipment for I/O control.
Safety I/O has more strict requirements to the latency and packet loss than standard I/O. A safety I/O connection fault indicates that the packet has not been received (lost or delayed) within the Connection Reaction Time Limit (CRTL) which depends on the RPI and multipliers. Applications with low CRTL may not be suitable for wireless media due to potential high latencies and packet losses. On the other hand, increasing CRTL may exceed the required System Reaction Time (SRT), making the application unfeasible.

The worst-case Logix SRT values can be calculated using the Safety Estimator Tool available from the Rockwell Automation website. There are several numbers that can be used:

- No-fault Reaction Time: the worst-case performance of the system without errors or faults.
- Single-fault Reaction Time: the worst-case performance of the system when it encounters a single fault or error that would not cause the controller to fault or shutdown, but could cause a delay in performance. An example would be if a packet is corrupted and a retry is needed.
- Multiple-fault Reaction Time: the absolute worst-case delay of the system in case of a controller hard fault before a safety output would transition to a safe state.
- The decision on which number to use is based on the user’s risk assessment criteria, but the single-fault reaction time is typically used. The following rules have been for the wireless performance testing:
  - Maximum measured screw-to-screw reaction time should not exceed the theoretical single-fault SRT
  - 99.99% of the measured screw-to-screw values should not exceed the theoretical no fault SRT

### 2.2.2.4 Safety Produced / Consumed

- The maximum data size for the safety Produced / Consumed tag is 128 bytes. Safety data from several I/O modules can be aggregated into a safety produced tag for more efficient wireless communication.
- The RPI of the consumed safety tag matches the safety task period of the producing GuardLogix controller. As with safety I/O, all safety tags are updated at the end of the safety task scan. To reduce the total packet rate, safety data should be aggregated into one or few produced safety tags.
- Safety Produced / Consumed data requirements to latency and packet loss are similar to safety I/O. The multiplier values may need to be increased from default in the wireless media.
- The safety system reaction time (SRT) for the Produced / Consumed safety chain can be calculated using the Safety Estimator tool. Same criteria have been adopted for the performance testing (see safety I/O section).

### 2.2.2.5 CIP Sync

CIP Sync provides a mechanism to synchronize clocks between IACS devices on the EtherNet I/P network using IEEE 1588-2008 PTP (Precision Time Protocol). This technology supports distributed applications that require time stamping, Sequence of Events (SoE) recording, distributed motion control, and increased control coordination.

To achieve a high degree of accuracy and precision, IACS and network infrastructure devices should support PTP protocol in hardware or software, and implement QoS policy that gives highest priority to the CIP Sync traffic.

The existing wireless hardware does not support PTP. Because of that and also higher latency and significant jitter compared to wired Ethernet, the accuracy of time synchronization is limited across the wireless media.
CIP Sync generates small amount of multicast and unicast traffic in the wireless channel. The default intervals are 1 sec for sync and follow-up messages from the master clock, and 30 sec for delay requests and responses between the slave clocks and the master clock. CIP Sync protocol can tolerate some amount of packet loss and high average network latency, however large variations in network delay present challenges.

Following recommendations can be made for implementing CIP Sync applications over wireless:

- The time accuracy of 150 µs has been achieved in the test environment which indicates possible use of CIP Sync across wireless media for SoE and logging applications
- Use the latest firmware versions for Rockwell Automation components that support CIP Sync
- Place Grandmaster clock (GM) in the wired infrastructure behind the AP
- Eliminate unnecessary variable delays in the network, for example extra switch hops or unmanaged switches
- Use PTP transparent mode for switches that support PTP protocol
- Configure QoS settings with highest priority for CIP Sync traffic
- Configure IGMP snooping and querier in the network

### 2.2.3 CIP Application Recommendations

The following recommendations are based on the following assumptions:

- An application has a mix of data types and packet sizes, including standard and safety I/O or Produced / Consumed data, CIP Sync data, HMI data and messaging, RSLinx and Logix tools
- Data delivery is not coordinated between IACS devices, in other words each connection cycle is independent.
- The following recommendations are implemented as outlined in Chapter 4:
  - Wireless QoS configuration (4.2.2)
  - RF coverage requirements (4.1.5)
  - Data rate configuration (4.1.4)
- Good RF environment can be achieved with no outside interference.

The following recommendations can be made for using EtherNet/IP over wireless.

- Do not exceed 2,200 pps in the wireless channel with EtherNet/IP traffic.
- Reduce packet rate in environments with RF issues and interference.
- Reserve 20% of bandwidth for HMI and maintenance traffic such as web page diagnostic, programming tools etc.
- All communication should be accounted in the total packet rate calculations, including non-CIP packets and traffic from neighboring WLAN sharing the same channel.
- Direct communication between wireless clients should be limited (see 1.2.2), since each packet is transmitted twice (upstream to the AP and downstream from the AP).
- Use rack-optimized I/O connections, large arrays and data structures, data aggregation and other programming techniques to reduce number of individual connections and packet rate.
• PAC to PAC topology with Produced / Consumed tags is preferred over PAC to I/O topology for wireless communication.

• Connection Reaction Time Limit for a CIP Safety connection over wireless should be at least:
  - 60 ms for Safety Produced / Consumed
  - 72 ms for Safety I/O

• CRTL may need to be increased further to prevent safety connection timeouts by changing Safety Timeout or Network Delay multipliers.

• For greater long-term reliability, increase CRTL to be at least x4 greater than the RPI value. This allows 3 packets in a row to be lost before the timeout.

• Safety RPI as low as 15ms can be supported (Produced / Consumed), as long as the packet rate is below the limit.

• Standard RPI of 20ms can be supported. RPIs as low as 10ms may be supported depending on the application sensitivity to jitter and delay.
3. EtherNet/IP over Wireless Performance Testing

3.1 Test Objectives

The goals of the testing were as follows:

- Characterize performance of a control system with standard and safety CIP traffic using 802.11n wireless communication.
- Determine maximum system size and wireless channel utilization with typical CIP Standard and Safety application parameters.
- Provide recommended network architectures and configurations for Rockwell Automation customers using EtherNet/IP applications with wireless networks.

The key characteristics that were tested include the following:

- Network reliability (connection timeouts and lost packets)
- Real-time network performance (latency and jitter)
- CIP Safety performance (System Reaction Time)

3.2 Test Organization

3.2.1 Test Environment

The test setup represented a “best case” RF environment:

- No outside interference or significant signal obstruction
- A vacant wireless channel in the 5 GHz band
- Default indoor omnidirectional dipole antennas
- Wireless clients (WGBs) in fixed positions
- An adequate signal level to support the highest enabled data rates

Because of the above conditions, test results represent the best achievable application performance given the channel load and the system size. There are numerous factors that can impact actual performance in the production such as moving machinery, poor antenna installation, interference and so on. Separate tests are needed to evaluate these factors which were out of scope for this version of the guide. Testing of antenna characteristics and RF propagation was also out of scope.

3.2.2 Network Infrastructure

This section describes network infrastructure that was used throughout the testing. More configuration details can be found in Appendix A.

- Access layer switches were connected to the distribution layer switch stack in the redundant star topology using Etherchannels and multi-mode 1 Gbps fiber.
- The wireless architecture consisted of a single autonomous AP and a number of workgroup bridges (WGB). Each WGB had one or several IACS devices connected to its Ethernet port in a linear topology.
- Cisco Unified (WLC-based) wireless architectures will be addressed in the future versions of this guide.
- The wireless roaming use cases and testing will be addressed in the future versions of this guide.
- A single SSID/VLAN was used to communicate to the AP, WGBs and IACS devices. Configurations with multiple SSID/VLANs will be addressed in future versions of this guide.
- Optimal QoS configuration was used as recommended in 4.2.2.3.
• WPA2-PSK authentication with AES encryption was used (see 4.2.3.1). Other types of authentication will be tested in the future.

• Unicast mode for used for all connections. CIP Sync protocol was not enabled.

3.2.3 Safety I/O Test Topology

The wireless CIP Safety I/O testing was based on the wired PAC to wireless I/O topology described in 1.2.2. In this architecture, a fixed GuardLogix PAC on the wired network communicates with a number of mobile I/O racks over the wireless connection. In addition to CIP Safety traffic, each I/O rack sends and receives standard I/O data in the rack-optimized connection.

For the purpose of this testing, the number of safety I/O modules was limited to two per EtherNet/IP adapter (one discrete safety input and one safety output module).

• Total number of safety modules is limited by the available wireless bandwidth, since each module creates a separate I/O connection and increases the packet rate.

Additional CIP Class 3 traffic was simulated in the network for a number of tests. The simulated traffic contained a mix of packet sizes at lower QoS priority which represented typical HMI and RSLogix communication.

In parallel to the safety application traffic, two ControlLogix chassis were used as a separate instrument to measure network latency in the channel in each direction.

Based on the number of I/O racks per WGB, two use cases were considered:

• Individual I/O nodes: large number of WGBs, one I/O rack per WGB
• Grouped I/O nodes: small number of WGBs, multiple I/O racks per WGB

Figure 3-1 Safety I/O Test Topology: Individual I/O Nodes
3.2.4 Safety Produced / Consumed Test Topology

The wireless CIP Produced / Consumed testing was based on the wired PAC to wireless PAC topology described in 1.2.2. In this architecture, a fixed GuardLogix PAC on the wired network communicates to a number of mobile GuardLogix PACs over the wireless connection.

Each mobile PAC produces and consumes a safety tag of the maximum size (128 bytes of data), and also a standard tag (256 bytes of data), with the total of four connections (two upstream and two downstream).

Each PAC owns standard and safety I/O in a POINT Guard I/O rack over the wired Ethernet. The architecture allows consolidating multiple safety I/O data on the wireless network into a single Produced / Consumed safety tag. This method decreases the total network load in the wireless channel and makes possible to create systems with larger number of I/O modules. For the purpose of this test, only one I/O rack was used per controller.

Two ControlLogix chassis were used as a separate instrument to measure network latency in the channel in each direction.
3.3 Test Observations

Details of the testing can be found in Appendix A:

- Test variables
- Test measurements
- Test suites
- Full test results
  - System Reaction Time
  - Connection Faults
  - Network Latency
  - Network Traffic Statistics

Next sections summarize the key findings from the tests performed.
3.3.1 Packet Rate

- Total packet rate in the channel was the most critical factor for the reliable operation of the CIP safety system without connection loss. Increasing the packet rate over the limit resulted in higher latency and eventually connection losses.

- Test system performed reliably in the lab environment with the following packet rates:

<table>
<thead>
<tr>
<th>Topology</th>
<th>I/O or P/C Packet Rate, pps</th>
<th>CIP Class 3 Packet Rate, pps</th>
<th>Total Packet Rate, pps</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP Safety I/O, 8 wireless nodes</td>
<td>2,200</td>
<td>-</td>
<td>2,200</td>
</tr>
<tr>
<td></td>
<td>1,800</td>
<td>400</td>
<td>2,200</td>
</tr>
<tr>
<td>CIP Safety I/O, 4 wireless nodes</td>
<td>2,800</td>
<td>-</td>
<td>2,800</td>
</tr>
<tr>
<td></td>
<td>2,200</td>
<td>400</td>
<td>2,600</td>
</tr>
<tr>
<td>CIP Safety P/C, 8 wireless nodes</td>
<td>2,600</td>
<td>-</td>
<td>2,600</td>
</tr>
<tr>
<td></td>
<td>2,200</td>
<td>400</td>
<td>2,600</td>
</tr>
</tbody>
</table>

- Smaller number of wireless nodes (4 vs. 8 WGBs) showed some improvement in the achievable packet rate.

- Safety Produced / Consumed topology supported comparable or somewhat higher packet rates than Safety I/O topology with the same number of WGBs. Higher data throughput as measured in Mbps was achieved with Produced / Consumed tags due to larger CIP data sizes.

3.3.2 Safety System Reaction Time

- It was demonstrated that the following Safety Reaction Times can be supported assuming Single Fault/Delay worst-case theoretical calculations and packet rate below the limit.

<table>
<thead>
<tr>
<th>Topology</th>
<th>Single Fault/Delay Safety Reaction Time (theoretical)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP Safety I/O</td>
<td>171 ms</td>
</tr>
<tr>
<td>CIP Safety P/C</td>
<td>158 ms</td>
</tr>
</tbody>
</table>

- Measured Safety Reaction Times for 99.99% of the samples was below the No-Fault worst-case theoretical values for all test cases.

- Compared to wired Ethernet baseline, less than 1% of the measured wireless SRT were larger than the maximum wired SRT. The histograms below show an example of how values were distributed for one of the test suites. The other tests showed very similar results.
3.3.3 Network Latency and RPI

- The following CIP Safety parameters were successfully tested with wireless media:

<table>
<thead>
<tr>
<th>Topology</th>
<th>Input I/O CRTL, ms</th>
<th>Output I/O CRTL, ms</th>
<th>Safety Input RPI, ms</th>
<th>Safety Output RPI, ms</th>
<th>P/C CRTL, ms</th>
<th>Safety P/C RPI, ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP Safety I/O</td>
<td>72 ms</td>
<td>90 ms</td>
<td>18 ms</td>
<td>30 ms</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>CIP Safety P/C</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>60 ms</td>
<td>15 ms</td>
</tr>
</tbody>
</table>

- Upstream latency (WGB to AP) was greater than the downstream (AP to WGB) due to the QOS parameters that prioritized AP transmissions over WGBs.

- The average wireless network latency was below 2ms for test suites with the packet rate below the limit, compared to 0.3ms for wired baseline. The average latency applies to wireless frames that are transmitted successfully without contention in the channel or other delays.
• Maximum latency for 99.99% of samples was below 10ms for test suites with the packet rate below the limit. The additional latency represents contention for channel access, retransmissions due to collisions, and output queue delays. The histogram below show an example of latency distribution for one of the test suites. The other tests showed very similar results.

Figure 3-5 Network Latency Distribution

• Maximum Safety I/O Round Trip Delay was below 35ms for test suites without I/O timeouts. This parameter is reported in the Logix properties for a safety I/O module and measured as part of CIP Safety protocol.

• Very small number of samples (less than 0.01%) had latency greater than 10ms. The absolute maximum latency measurements, however, were inconsistent between the test suites. Occurrence of standard and safety connection timeouts should be the main pass/fail test criteria.

• Additional low priority traffic in the channel (up to 20% of the total rate) did not substantially increased latency for higher priority traffic. This was expected due to the QoS configuration.
4. WLAN Design Considerations

4.1 Radio Frequency Design

4.1.1 Radio Spectrum

4.1.1.1 802.11n Frequency Bands

802.11n networks operate in unlicensed 2.400 – 2.483 GHz and 5.180 – 5.825 GHz radio spectrums, commonly known as 2.4 and 5 GHz bands. Each spectrum is sub-divided into channels with a center frequency and bandwidth. Rules for the number of available channels, allowed areas of use, and maximum transmit power vary by each country.

The 2.4 GHz band is also used by legacy 802.11b/g devices, 802.15 Wireless Personal Area Networks (WPAN) devices such as Bluetooth, WirelessHART, ISA100.11a and a variety of non-Wi-Fi consumer products. Dual-band 802.11n devices often use 2.4 GHz band by default. The 2.4 GHz band is heavily utilized and usually cannot provide interference free spectrum.

The 5 GHz band is less crowded than 2.4 GHz, and more suitable for IACS applications that require dedicated bandwidth with minimum interference. Most enterprise IT networks use 2.4 GHz band for user data while leaving 5 GHz band for specialized applications such as wireless voice. However, with increasing number of dual-band devices such as smartphones and tablets, 5 GHz band is being used more often.

5 GHz band is more heavily regulated than 2.4 GHz, and channel availability vary greatly between countries. There are also restrictions for certain channels due to radar and satellite operation. These topics are discussed in the following sections.

• 5 GHz frequency band is recommended for industrial wireless applications. Because of limited number of channels and much higher chance of interference, the 2.4 GHz band is not recommended to use for critical IACS applications, such as machine control. However, 2.4 GHz band can be used for personnel access and low throughput non-critical applications.

4.1.1.2 Regulatory Domains

Most IACS applications require exclusive use of a wireless channel to meet the performance and reliability criteria. The number of available wireless channels in the frequency band is restricted by regulatory rules of a country (for instance, FCC in the US and ETSI in Europe). These rules, specifically for the 5 GHz band, may change rapidly and should be confirmed when the new installation is planned.

It is important to remember that wireless equipment may not operate on all channels available in a particular geographic area. For example, Cisco equipment operates in 11 regulatory domains, each applied to a group of countries. Even if a country has less restrictive rules on the channel use, the domain settings in the AP may be more limited. The regulatory domain is factory set and it is not possible to add more channels even if country regulations change.

Regulatory domain rules specify not just channels, but also the maximum transmit power, allowed antennas and areas of use. Some countries fall under several regulatory domains depending on the frequency range and indoor/outdoor use.

The list of regulatory domains for Cisco equipment is shown in Table 4-2. Please note that the information provided here and in the following sections should only be used as a general guideline.

• As the rules constantly change, refer to the local regulatory authority, product documentation and the Cisco website for the most recent compliance information and channel availability in a particular country.

To verify approved equipment and to identify the regulatory domain that corresponds to a particular country, refer to the Wireless LAN Compliance Status.
### 4.1.1.3 2.4 GHz Channel Availability

There are 13 configurable channels (11 in North America and some other countries) in the 2.4 GHz band. However, the channel separation is only 5 MHz while a minimum of 20 MHz bandwidth is needed for a radio to operate without interfering with the adjacent channel. As a result, only three channels can be effectively used in the 2.4 GHz band (normally 1, 6, and 11).

- Use only channels 1, 6, and 11 in the 2.4 GHz band.
- Use of non-standard channels or more than 3 channels in 2.4 GHz band will cause adjacent channel interference and lower throughput.

![Channel Allocation in the 2.4 GHz Band](image)

### 4.1.1.4 5 GHz Channel Availability

The channels in the 5GHz band are also referred to as the UNII (Unlicensed National Information Infrastructure) channels (see Table 4-1). In contrast to 2.4 GHz, 5 GHz band has potentially more channels to choose from (16 to 21 for most regions). The number of practically usable channels is usually smaller for the following reasons:

- Dynamic Frequency Selection (DFS) requirements of the UNII-2/2e channels could make them unusable for IACS applications (see 4.1.1.6).
- Some of the UNII-2e and UNII-3 channels may not be supported by radios or not available in the domain.
- Outdoor usage may be prohibited or regulated differently for some channels (for example, UNII-1 in US and UNII-1/2 in Europe).
- Use of 40 MHz bandwidth (802.11n channel bonding) for higher throughput reduces the number of channels in half.

#### Table 4-1 Overview of 5 GHz band channels

<table>
<thead>
<tr>
<th>UNII Band</th>
<th>Channel Number (20 MHz bandwidth)</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNII-1 5.15 – 5.25 GHz</td>
<td>36, 40, 44, 48</td>
<td>Indoor only (US and Europe)</td>
</tr>
<tr>
<td>UNII-2 5.25 – 5.35 GHz</td>
<td>52, 56, 60, 64</td>
<td>DFS rules apply Indoor only (Europe)</td>
</tr>
<tr>
<td>UNII-3 5.725 – 5.825 GHz</td>
<td>149, 153, 157, 161, 165</td>
<td>Limited availability in some countries</td>
</tr>
</tbody>
</table>
The following table shows the global channel availability with and without DFS requirements. Refer to the local regulatory authority, product documentation and the Cisco Website for the most recent information.

Table 4-2 Global 5 GHz Channel Availability¹

<table>
<thead>
<tr>
<th>Regulatory Domains</th>
<th>Countries ¹</th>
<th>Available Channels (20 MHz bandwidth)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>UNII-1</td>
</tr>
<tr>
<td>A (FCC)</td>
<td>U.S., Canada, South America</td>
<td>9</td>
</tr>
<tr>
<td>E (ETSI)</td>
<td>Europe, most of Middle East and Africa, some countries in Asia</td>
<td>4</td>
</tr>
<tr>
<td>C</td>
<td>China, Indonesia, Malaysia, Pakistan</td>
<td>5</td>
</tr>
<tr>
<td>I</td>
<td>Israel, Egypt</td>
<td>4</td>
</tr>
<tr>
<td>K</td>
<td>Korea</td>
<td>9</td>
</tr>
<tr>
<td>N</td>
<td>Mexico, India, South America</td>
<td>9</td>
</tr>
<tr>
<td>Q</td>
<td>Japan</td>
<td>4</td>
</tr>
<tr>
<td>R</td>
<td>Russian Federation</td>
<td>8</td>
</tr>
<tr>
<td>S</td>
<td>Singapore</td>
<td>9</td>
</tr>
<tr>
<td>T</td>
<td>Taiwan, Brazil</td>
<td>5</td>
</tr>
<tr>
<td>Z</td>
<td>Australia, New Zealand</td>
<td>9</td>
</tr>
</tbody>
</table>

¹ Based on the indoor operating channels for the Cisco 2600 series AP

4.1.1.5 Radio Spectrum Management

Some of the wireless channels may be already utilized by the IT department, or may be reserved for future use. It is critical to start early dialogue and collaboration with the IT department and ensure availability of channels. While wireless spectrum can be shared among many corporate applications in the Enterprise Zone, it is typically not the case for the Industrial Zone. IT personnel should be educated about stricter requirements of the IACS applications.

In addition to the IT applications, other industrial equipment may operate in the unlicensed wireless spectrum. Typically, an OEM machine builder would want an exclusive use of a channel, even if not using the full bandwidth. A high level of cooperation and conformance to a common policy is required.

The proper RF spectrum policy should define the following:

- Who maintains administrative rights over the spectrum to ensure fair and efficient allocation of the bandwidth
- Who is responsible for maintaining a list of devices, their functions, frequencies assigned and reserved for future use
- List of permitted frequency bands and device types
- Procedures for testing, approving, and deploying new wireless equipment
- Responsibilities and methods of detecting and mitigating wireless interference and security attacks
- Rules regulating use of personal wireless devices

See also the following Cisco white paper, RF Spectrum Policy: Future-Proof Wireless Investment Through Better Compliance.
**4.1.1.6 DFS Channels**

Dynamic Frequency Selection (DFS) in the IEEE 802.11 standard defines operational rules in the 5GHz band to allow coexistence with certain wireless systems such as military or weather radars and satellite systems. The compliant Wi-Fi device must give priority to these systems, listening during operation and rapidly abandoning channel usage if a radar source is detected. The DFS system must also listen for a certain time before starting using a new channel.

After detecting a radar signature, the AP immediately terminates data communication and alerts clients to the loss of service and a new proposed channel. The AP randomly selects a new channel and listens for radar for a period of 60 seconds. No data or management services are provided on the new channel during this period. If no radar is present, the AP can then begin to provide service, otherwise another channel is assessed.

There are additional considerations that affect operation in the DFS channels:

- Radars do not always stay on the same frequency and may affect multiple channels
- False positive detection by an AP may happen due to other wireless interference
- If an AP switches to another DFS channel for reason other than radar detection, 60 second listening gap still applies

APs in most of the regulatory domains now comply with DFS regulations. APs randomly select between DFS channels in UNII-2/2e (Table 4-1), and these channels cannot be set manually.

60 seconds gap in communication is usually not acceptable for IACS applications. It is best to avoid using DFS channels altogether. However, the number of available non-DFS channels may not be enough for the application coverage, especially where the channels must be shared with other wireless systems.

The following recommendations can be made regarding the use of DFS channels:

- Use non-DFS channels when possible
- If DFS channels are used, thorough site survey and subsequent monitoring of DFS channels is required before and after the installation. AP logs indicate DFS events
- Particular caution should be used when operating near airports, sea ports, military bases, or large cities

**4.1.2 802.11n Characteristics**

The technical breakthrough in wireless Ethernet, the IEEE 802.11n standard makes it possible to address a broad range of manufacturing and process applications. Rockwell Automation and Cisco have tested this technology to determine its ability to meet the broad range of needs in industrial automation using standard, unmodified wireless Ethernet.

Improvements to 802.11n over previous technologies include significant performance increases, as well as the addition of new features:

- Higher transmission rates due to improved signal modulation and encoding methods
- Multiple Input Multiple Output (MIMO) technology
- Channel bonding and frame aggregation for increased throughput
- Backward compatibility with 802.11a/b/g and dual band operation (2.4 and 5 GHz)

Some of the 802.11n enhancements may not be relevant to certain types of industrial applications, or require specific configuration. Recommendations for enabling or configuring 802.11n features with IACS applications are provided in this section. More details can also be found in Appendix B.
Multiple-input multiple-output (MIMO) provides the basis of how 802.11n can raise reliability and reach data rates many times higher than 802.11a/b/g in the same radio spectrum. These benefits can be valuable in industrial settings with difficult RF environments and applications with high throughput or quality-of-service (QoS) requirements.

The most important MIMO aspects are:

- **Spatial Division Multiplexing** – the ability to send multiple signals (spatial streams) at the same time over the same channel
- **Transmit Beamforming** – the ability to use multiple transmit antennas to improve the SNR
- **MIMO Equalization** – the ability to use multiple receive antennas to improve the SNR

### 4.1.2.1 Spatial Division Multiplexing

802.11n standard specify that multiple transmitting antennas can be used to send several data streams in the same channel. This technology is called Spatial Division Multiplexing. Legacy 802.11a/b/g allows the transmission of only one spatial stream at a time. 802.11n devices can transmit up to 4 (typically 2-3) spatial streams, increasing theoretical data rate accordingly. N spatial streams require at least N transmit antennas at the transmitter and N receive antennas at the receiver.

Figure 4-2 Spatial Division Multiplexing

```plaintext
Information Is Split and Transmitted on Multiple Streams
```

Achieving the maximum data rate becomes progressively harder with two or three spatial streams because it requires high SNR and shorter distances. The most direct way to increase SNR is to place devices closer to each other, which is rarely practical. Thus it is necessary to complement spatial division multiplexing with other 802.11n technologies that improve received signal quality.

- Spatial Division Multiplexing has limited benefit for the real-time EtherNet/IP traffic. Although higher rates can reduce the transmit time of the data portion of a packet, the overall reduction is not very significant because of the short packet length and 802.11n protocol overhead (see 2.1.2.1).
- Multiple spatial streams make communication less reliable, dependent on higher SNR, and more susceptible to multipath fading. Single spatial stream is more suitable for control communication.

### 4.1.2.2 Transmit Beamforming

In typical indoor WLAN deployments, the radio signal rarely takes the direct, shortest path from the transmitter to the receiver. Most indoor environments, particularly industrial facilities, have metal surfaces that reflect a radio signal. Multiple copies of the signal may arrive at the receiver, each with a slight delay. This phenomenon is called multipath.

Legacy wireless devices transmit a single data stream over a single antenna. The multipath delay may cause a significant transformation of the signal at the receiver because of the misalignment of phase. The result is lower SNR and degraded performance.
A MIMO radio actually uses multipath as an advantage. Using transmit beamforming, it adjusts the phase of the signal sent from many antennas which maximizes the received signal strength and SNR. This feature is the most beneficial when transmitting to a single wireless client.

Figure 4-3 Transmit Beamforming

4.1.2.3 MIMO Equalization

The MIMO equalization complements transmit beamforming on the receiver side. The receiver combines the signal from multiple antennas before decoding. Redundant antennas increase the chance of receiving a good signal even if one experiences a signal fading due to multipath. To reliably receive N spatial streams, the number of receive antennas should be at least N+1. In case of a single spatial stream, the MIMO equalizer is known as Maximum Ratio Combiner (MRC).

In the multipath environment, a spatial stream follows a set of paths that may interfere in a positive or negative way at the receive antenna. If there are multiple receive antennas, it is highly unlikely that both antennas experience the destructive interference. This behavior, called spatial diversity, provides improvements to SNR just as good as with transmit beamforming.

Figure 4-4 MIMO Equalization
4.1.2.4 Channel Bonding

802.11a/g legacy networks use radio bandwidths that are 20 MHz wide. In 802.11n networks, it is possible to use 40 MHz wide channels as a simple way of doubling the data rate. With channel bonding, two adjacent 20 MHz channels are joined together, also taking advantage of the reserved bandwidth space between them, so the final data rate increase is slightly more than a double.

Figure 4-5 Channel Bonding

This technique is feasible only in the 5 GHz band since there are only three 20 MHz non-overlapping channels in the 2.4 GHz band. Even in 5 GHz band, there may be not enough free channels in the particular location because of existing use or country regulations (see 4.1.1). Therefore, the usefulness of channel bonding is limited in many cases.

Testing of 40 MHz channels with EtherNet/IP applications showed only minor improvement over 20 MHz channels. The fixed overhead of a packet is large compared to the small size of the EtherNet/IP data payload, so the higher rate has little performance advantage. In 802.11n, only large transmissions (such as file downloads) take advantage of the high bandwidth. Reduced number of channels with channel bonding is the biggest concern.

- 20 MHz channel width (no channel bonding) is recommended with IACS applications.

4.1.2.5 Frame Aggregation

Every wireless frame has fixed overhead due to the radio preamble and 802.11 MAC frame fields. As data rates increase, the time required to transmit the data frame shrinks, but the overhead “cost” remains the same, potentially becoming much greater than the packet itself at the high speeds delivered with 802.11n (see also 2.1.2).

The limitations and considerations for 802.11n frame aggregation are:

- Aggregated packets have to have the same wireless destination (WGB or embedded adapter). Very high performance can be achieved with point-to-point configurations using aggregation, and little improvement with 8-12 WGBs sharing the traffic.

- MCS data rates need to be enabled to invoke aggregation. (see 4.1.4).

- All data frames have to be ready to transmit at the same time. Because of that, some frames may be delayed in order to attempt to send a single aggregate frame. This can be a problem for scheduled periodic transmissions such as EtherNet/IP Class 1 traffic. Some aggregated packets may be discarded by the application upon the arrival.

- Test results showed that a group of wired nodes must produce at least 1000 pps to invoke consistent aggregation. At lower rates, aggregation rarely occurs. The aggregation may therefore improve performance when there are multiple Ethernet I/O racks or multiple specialty modules with direct connections behind a WGB.

For real-time control, frame aggregation can be beneficial for point-to-point type of communication, or with small number of nodes. The positive or negative effect of aggregation should be determined in the application testing.
4.1.2.6 Additional Information

For additional information about 802.11n features, see the following links:

- 802.11n Wireless Solutions page
- Industry Leading Performance with Cisco's Aironet 3600 Series Access Point
- Cisco ClientLink: Optimized Device Performance with 802.11n

4.1.3 802.11ac Standard Overview

IEEE 802.11ac is the emerging Wi-Fi technology that further improves and enhances 802.11n capabilities. Primary use cases for the 802.11ac will be very high throughput applications that exceed data rates supported by 802.11n today.

The main features of 802.11ac technology are:

- Operation in 5 GHz band only
- Support for larger channel bandwidth with channel bonding:
  - 80 MHz (first generation products)
  - 160 MHz (second generation products)
- Higher modulation rates
- Up to 8 spatial streams
- Theoretical speeds up to:
  - 1.3 Gbps (first generation products)
  - 3.5 Gbps (second generation products)
- Multi-user MIMO (multiple frames to multiple receivers): second generation only

The ability to apply 802.11ac technology to the industrial applications, particularly real-time machine control, will be determined in the future. Higher data rates do not provide any real benefits to the IACS applications while requiring more channel bandwidth. Other features, such as Multi-user MIMO technology, will be evaluated when become available.

4.1.4 Data Rates

In 802.11n wireless communication, data rates are determined by a number of variables, including modulation and coding type, channel bandwidth, and the number of spatial streams.

Higher data rates use the bandwidth more efficiently, but they also use more complex mechanisms that require better signal quality and can only be used at shorter distances. Lower data rates use simpler modulation and coding schemes that are less efficient but more reliable and allow communication at greater distances.

To improve reliability, 802.11 wireless stations use dynamic rate shifting. If excessive retransmissions occur, stations can operate at a lower data rate decreasing the SNR requirements at the receiver.

Operating data rate is not always a good measure for performance. The data rate (the number of data bits sent per second) only applies during the time that the frame is actually sent. Contention for the shared medium between stations, interference, and overhead of the protocol reduce the actual throughput to often less than 50 percent of the theoretical rate.

For details on 802.11n and legacy 802.11a/g data rates, please refer to Appendix B.
For each radio, the available data rates can be configured in one of the following states:

- Basic (also called Required or Mandatory) – Wireless clients must support this data rate in order to associate to an AP.
- Enabled – Any associated clients may communicate with the AP using that rate. However, the clients are not required to support this rate.
- Disabled – The wireless device does not transmit data at this rate.

Configuring these parameters has a direct effect on the wireless cell size, number of clients in the cell, and how certain traffic is communicated in the cell:

- At least one of the 802.11a/g basic rates needs to be configured in the 802.11n network.
- Management frames (beacons, probe responses etc.) are transmitted at the lowest basic rate.
- Multicast, broadcast, and certain control frames are transmitted at the highest basic rate.
- Clients that do not support the lowest basic data rate cannot connect to the WLAN.
- Clients with low SNR that cannot decode the lowest basic data rate cannot connect to the WLAN. Thus the lowest basic rate determines the association area and controls the number of clients in the cell.
- Lower rate clients affect the maximum throughput of the higher rate clients by taking longer to transmit packets.
- For AP to WGB communication, data rates can be defined on the AP, WGB, or both. In general, different rate configurations can be used for each WGB.

When enabling higher data rate for real-time EtherNet/IP traffic, the following needs to be considered:

- Reliable data delivery and low application latency are much more important for EtherNet/IP applications than high throughput. Small data packets and relatively low amount of traffic (for instance, compared to video and file transfer) do not allow taking full advantage of the highest data rates.
- Automation environments are commonly filled with metal objects creating multipath fading. Improved tolerance to multipath fading is not dependent on using 802.11n rates. Maximal Ratio Combining (MRC) uses multiple receivers to improve the signal even when only 802.11a rates are enabled.
- Using multiple spatial streams can actually decrease the tolerance to multipath fading. More data streams for the same number of receive antennas leads to less redundancy and lower reliability.
- The most robust configuration for EtherNet/IP traffic is one spatial stream with four receive antennas (based on the latest Cisco AP models).
- Frame aggregation requires MCS rates to be enabled. Aggregation does not happen with legacy 802.11a/g rates.

Based on the above and the results of testing, the following data rate recommendations can be made for applications:

- Use AP configuration to define data rate set. Use default rate settings on the WGBs.
- Configure 6, 12, 24, 54 Mbps data rates as basic, and disable other legacy rates.
- For applications with real-time Class 1 EtherNet/IP traffic:
  - Disable 802.11n data rates (MCS 0-23) for systems with more than 3 wireless clients (WGBs).
  - Enable MCS 0-7 rates (one spatial stream) for systems with 3 or less clients (WGBs) to be able to use frame aggregation.
- Limit CIP Sync traffic to 6 and 54 Mbps speeds only using the highest priority QoS queue.
- All available 802.11n data rates (MCS 0-23) can be enabled if the WLAN handles only Class 3 EtherNet/IP and non-IACS type of traffic.
4.1.5 Wireless Coverage

4.1.5.1 Coverage Cell Size

The size and shape of a coverage area depends on many factors:

- Frequency band
- Transmit power level
- Antenna gain and radiation pattern
- Electromagnetic environment
- Interference level from co-channel and adjacent channel
- Receiver sensitivity
- Lowest required data rate in the cell

An example of the coverage area compared to the data rate is shown in the following picture.

- The distances shown here are not exact and shown as an example only. The real distance at which the desired data rate can be supported is determined during the site survey. Changes in the environment and interference levels also dynamically increase or decrease the distance.

**Figure 4-6 Coverage Area Example**

Coverage cell size can be changed by several methods:

- Increasing or decreasing transmit power of the AP or WGB
- Changing the lowest basic data rate at which client can connect
- Changing antenna type and orientation to increase or decrease signal propagation in certain direction

The goal is to maintain the required RSSI and SNR levels throughout the area while minimizing signal propagation beyond the boundaries. *(See Appendix B for information on these parameters)*

- For EtherNet/IP applications, recommended parameters that should be maintained in the coverage area are:
  - Minimum RSSI of -67 dBm
  - Minimum SNR of 25 dB

- For CIP Sync traffic, the cell coverage area should be designed to sustain 54 Mbps data rate
4.1.5.2 Transmit Power Settings

The maximum allowable transmit power is based on these factors:
- Frequency band and particular channel due to regulatory rules
- Data rate, antenna gain, and number of transmit antennas in use

The transmit power can be set manually per AP in the autonomous mode, or configured statically or dynamically by RRM in the Unified mode.

For Cisco APs, each consecutive setting decreases the power level by half (in mW) which means 3 dBm in difference. For example, the possible settings for Cisco 2600 AP and 5 GHz radio are:

<table>
<thead>
<tr>
<th>Power Level (dBm)</th>
<th>Equivalent (mW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>23 dBm (200 mW)</td>
<td>11 dBm (12.5 mW)</td>
</tr>
<tr>
<td>20 dBm (100 mW)</td>
<td>8 dBm (6.25 mW)</td>
</tr>
<tr>
<td>17 dBm (50 mW)</td>
<td>5 dBm (3.13 mW)</td>
</tr>
<tr>
<td>14 dBm (25 mW)</td>
<td></td>
</tr>
</tbody>
</table>

Based on the regulatory restrictions, some of these settings may not be shown by the AP as available for configuration. For example, the maximum setting is limited to 14 dBm for the UNII-1 channels (36-48).

Increase in transmit power can be used in two ways:
- For a constant range, to improve SNR at a particular location and make communication possible at greater data rates.
- For a desired data rate, to increase range at which it can be reliably sustained.

Figure 4-7 Transmit Power Increase

When configuring power settings for the AP and WGBs in a cell, the following needs to be considered:
• The received signal level or the achievable range depends not only on the transmit power level but also on the antenna gain of the transmitter and receiver (see Antenna Characteristics).

• The transmit power of the AP should match the transmit power of client adapters or WGBs (if both using the same omnidirectional antennas).

• Dynamic power configuration can be used in the Unified WLAN to compensate for coverage holes or changing RF environment. For most IACS applications, static configuration is recommended.

• When changing the channel in 5 GHz band, transmit power may be automatically reduced to comply with regulations. This should be planned for when doing a site survey.

• It is not always desirable to use the maximum transmit power in the cell. Limiting transmit power creates smaller coverage cell size with less signal propagation outside the intended area and less chance for distant clients to join the AP.

4.1.5.3 Multiple Cell Coverage

In many industrial wireless applications, multiple APs are used to create continuous coverage. By changing transmit power and antenna gains, coverage cell size and AP density can be manipulated.

Figure 4-8 Transmit Power and AP Density

The following steps needs to be implemented when designing an optimal wireless coverage:

• Determine the number and locations of the wireless clients (WGBs) assuming the worst case numbers and future expansions.

• Calculate the bandwidth that each client will consume in terms of packets per second (see 2.1.1 and 2.1.2).

• Determine the number of available channels at the site and the total available bandwidth. Ideally, the channels should not be shared with any other application. The maximum packet rate per channel is discussed in 2.1.2.

• Identify redundancy requirements for coverage, i.e. if two (or more) APs should be seen from any point to provide for failures.
• Perform the site survey to estimate the number and locations of APs that can cover the production area with an adequate signal level and required level of redundancy.

The above information should help to answer the following questions:

• Is it necessary to reuse channels based on the estimated number of APs and the channel availability? The channels reuse considerations are discussed in the next section.

• What is the maximum wireless client count and packet rate per AP? If these numbers exceed the recommendations in 2.1.2, then it may be necessary to increase the AP density. Larger AP count, on the other hand, consumes more channels or requires channel reuse. Application changes may also be necessary to lower AP utilization.

Generally, smaller wireless cells with fewer clients per AP provide higher performance due to reduced media contention. Lowering transmit power can potentially help to avoid interference between the devices operating on the same channel.

4.1.5.4 Channel Allocation and Reuse

Each AP in a WLAN need to be set to a specific RF channel which the client radios will use to communicate. Wireless clients, including WGBs, do not have to be configured to use a specific channel, and usually select the best available AP to associate.

In some cases, it may be useful to specify MAC address of the AP to whom a client must associate. However, it is not a common practice.

When allocating channels, the following needs to be considered:

• Autonomous APs can be configured to select the least congested channel at startup. However, static channel assignment is recommended for better control and consistent performance.

• In the Unified architecture, a WLC can dynamically assign the channels based on the Radio Resource Management (RRM) algorithm. However, RRM is typically turned off for IACS applications (see 4.1.8). The preferred method is static allocation of channels. Dynamic channel changes during the operation will cause application timeouts.

• RRM channel allocation can still be used during the initial setup of the controller based WLAN, especially for large number of AP where channel reuse schemes needs to be implemented. The settings can be changed to static during the production.

• DFS channels in UNII-2 and UNII-2e bands cannot be set statically. Generally, these channels are not recommended for IACS applications (see 4.1.1.6).

If channels have to be reused at the site, Co-Channel Interference (CCI) is the critical factor. CCI happens when transmissions from a neighboring 802.11 wireless cell (by AP or a client) propagate into the receive range of the other cell operating on the same channel, forcing both cells to share available bandwidth.

If a wireless device can detect the transmission and decode it as a valid Wi-Fi signal, then it defers access to the channel. This applies for any 802.11 network operating in the area, regardless of SSID or other parameters. In the example below, the two wireless cells are combined into one collision domain and have to share the bandwidth:

• Transmissions from both APs and WGBs will be seen as a busy channel by the other devices that have to wait for an opportunity to transmit.

• Greater number of devices operating in the channel increases the chance of collisions and contention for the medium.

• Both AP and WGB transmissions can interfere with the neighboring cell, with a WGB at the cell edge as the worst case.
Receiver sensitivity (see RF Power Values), transmit power, and the environment determine the range at which CCI can be avoided. Since preamble of the wireless frame is always transmitted at 6 Mbps data rate, the radio sensitivity at that rate should be used. For example, for Cisco 2600 AP with omnidirectional antennas:

- Receive sensitivity at 6 Mbps (5 GHz radio) -92 dBm
- Transmit power 0 dBm
- Transmit antenna gain 4 dBi
- Receive antenna gain 4 dBi
- Attenuation needed -100 dB
- Distance with free space loss (5180 MHz) 460 meters

As seen from this example, it is hard to avoid CCI in the open space environment which is typical of many industrial sites. Attenuation is increased in the environments with walls, obstacles etc. Interference range can also be reduced by several methods:

- Lowering transmit power of APs and WGBs
- Reducing antenna gain in particular direction by changing antenna type and orientation
- Using RF attenuators or reducing sensitivity of the radios

**Recommendations**

These recommendations can be made when allocating channels for IACS applications:

- Site survey is necessary to evaluate CCI and possibility of channel reuse.
- Use static channel configuration avoiding DFS channels in 5 GHz band.
- Do not reuse the channels for wireless cells operating with high utilization and high client count, unless complete signal separation can be reliably 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.
- Channel allocation scheme should provide maximum distance separation between same channels, if possible.
- Due to some amount of ACI (Adjacent Channel Interference), neighboring cells should avoid adjacent channels, if possible (for instance, channels 36 and 40).
- Proper spectrum management policy and coordination between IT, OEM, and control engineers is critical.
4.1.5.5 Additional Resources

Click on the following guides for additional information about wireless coverage design:

- Cisco High Density Wireless LAN Design Guide
- Enterprise Mobility 7.3 Design Guide
- Cisco Aironet 1600/2600/3600 Series Access Point Deployment Guide

4.1.6 Antennas

An overview of antenna types and parameters can be found in Appendix B.

The recommendations regarding antennas in the industrial environments are as follows:

- No single type of antenna is best for all applications and locations. An accurate site survey is necessary to determine appropriate antenna type and placement.
- Make sure that antenna model, orientation and exact location during the installation actually matches what was used during the site survey.
- Follow all manufacturers’ recommendations about antenna orientation, mounting hardware, and installation procedures.
- Set the correct antenna gain in the AP/WGB configuration to make sure that transmit power conforms to regulatory restrictions.
- For APs with multiple antennas, the following is recommended:
  - Each AP antenna port should be populated with an antenna of the same model
  - All the antennas must be oriented in the same direction
  - External placement of antennas (outside a cabinet) should follow the placement of antenna ports on the AP (rectangular position and distances)
- Antennas should be mounted clear of any obstructions, particularly metal obstacles. The distance of at least two wavelengths from metal surfaces is recommended (12 cm for 5 GHz).
- Length of the antenna cable should be minimal to lower the signal loss. Low loss cables should be used for anything above 1 meter distance (typical loss is 0.35 dB/meter or better).
- Generally, the recommended height for indoor installations is 6 meters or less. Heights above 6 meters can present problems in coverage, especially directly under the antenna. In this case, the AP or the antenna should be lowered or directional antennas such as patch should be used.
- Low-gain omnidirectional antennas are typically appropriate for WGBs installed on mobile machinery.

Click on the following documents for additional information about antennas and installation recommendations:

- Antenna Product Portfolio for Cisco Aironet 802.11n Access Points
- Cisco Aironet Antennas and Accessories Reference Guide
- Antenna Patterns and Their Meaning
- Antenna Cabling
- Cisco Aironet 1600/2600/3600 Series Access Point Deployment Guide
4.1.7 Site Survey

A proper site survey is recommended for any WLAN installation, and absolutely critical when planning to use IACS applications in industrial facilities. There are several types of site surveys, all of which can be important steps for a successful WLAN deployment.

4.1.7.1 Pre-survey Data Collection

Before starting the site survey process, certain information has to be gathered about customer’s application and location (see also 2.1.1):

- Location and dimensions of wireless coverage areas
- Channel availability and existing wireless systems at the site
- Wireless client types and density
- Required application rates
- Roaming requirements
- AP redundancy requirements
- Detailed maps of the facility, including material compositions
- Environmental characteristics of the site, for example extreme temperatures, hosedown requirements, and intrinsic safety requirements
- Potential interference sources in the production process
- Installation limitations for the antennas, APs, and cabling

4.1.7.2 Predictive Site Survey

Predictive surveys are performed with a software program that uses information about the coverage area and RF models to predict optimal AP placements. The information may include area dimensions, type of environment, wall materials, hardware models, antenna types, roaming requirements, client density and so on.

- Predictive surveys do not include any type of field measurements, and cannot be used to make final decisions about AP quantity and locations.
- Information from the predictive survey can be used for budgetary purposes and as a starting point for a field site survey.
- Predictive surveys are useful when the deployment environment has not yet been built, or to minimize time needed on site.

An example of the predictive survey software is the Planning Tool included in the Cisco Prime NCS platform.

4.1.7.3 RF Spectrum Site Survey

An important step in the WLAN deployment is to evaluate existing RF environment and to identify non-Wi-Fi interference sources such as radars in 5 GHz and microwaves in 2.4 GHz. This information helps to select least congested channels for the application and/or mitigate interference. Specialized software and hardware tools are used for this purpose, for example Cisco Spectrum Expert sensor and software.
• RF spectrum analysis is critical for IACS applications with high bandwidth utilization and low latency requirements.
• Adequate time should be spent analyzing the channels to detect intermittent interference. This applies especially when planning to use DFS channels and looking for possible radar events (see 4.1.1.6).
• Periodic post-installation RF surveys are recommended.
• Built-in monitoring of RF spectrum is provided by CleanAir-enabled APs (see Appendix B).

4.1.7.4 Passive Site Survey

Passive survey use a software client that only listens for AP beacons and never associates to the AP. A passive survey can help to do the following:
• Estimate downlink RF coverage from an APs to a client
• Identify rogue devices (unauthorized or unknown Wi-Fi networks) on particular channels
• Quickly locate RF trouble areas

A passive survey only measures signal propagation for beacons and does not send any actual data to and from an AP. As a result, passive surveys do not provide information about data rate boundaries, retransmission and packet loss, or uplink performance.

• Passive survey should be used only as a supplemental tool. Active site survey is necessary for accurate results.

4.1.7.5 Active Site Survey

Active surveys are performed with the survey client associated to the APs. The software can evaluate uplink and downlink performance at the actual data rate needed for the application. Active surveys are recommended for new WLAN deployments because they provide the most accurate information.

A pre-installation survey is typically performed with just one AP at a time for single cell coverage (so called “AP-on-a-stick” method), or with two APs to verify adjacent cell overlap. A post-deployment survey is also recommended to verify multiple AP coverage and roaming performance. Changes in the environment or deviations from the installation plan may require a follow-up survey. For example, newly installed assembly line or pallets of product can block the signal and force changes in the AP and antenna placement.

4.1.7.6 Survey Recommendations

The following recommendations can be made for site surveys in the industrial environments:
• RF spectrum survey and active site survey types are recommended.
• A thorough RF spectrum survey should be done in all possible locations where APs and WGBs may be operating. Special attention should be paid to industrial equipment in close proximity to antennas that can cause EMI.
• Equipment used in the site survey should match exactly AP and antenna models to be installed. Correct frequency band and channel list should also be used.
• A complete walk-through of the coverage area should be performed. Accurate and properly calibrated facility maps should be used.
• A proper survey can only be done when all industrial equipment has been installed in the location. In this case, EMI interference and RF signal blockage can be detected.
• Any planned changes in the environment, such as new walls and machinery, should be taken into account. A follow-up survey may be needed after the changes.

• Considerations should be made for any moving obstacles that may block the signal, for example overhead cranes or products being assembled.

• Most IACS applications use a WGB on the mobile machinery as a wireless client. Their characteristics, such as radio parameters, antenna type and height, will be different from a laptop used during the surveys. For accurate results:
  - Simulate the expected antenna height of the client.
  - Transmit power of the AP and the client should match.
  - Verification of coverage, roaming performance, and adequate RSSI/SNR levels should be made during the post-deployment survey using an actual WGB as a client.

• When determining the wireless cell coverage, the following parameters should be used:
  - Minimum RSSI of -67 dBm
  - Minimum SNR of 25 dB

• If AP redundancy is required, at least two APs should be seen from each point at the adequate signal level.

• Common practice for a survey is to set AP power to half of the maximum. This creates smaller coverage cells but allows a margin for power increase in case of RF issues. An example would be loss of an AP when neighbor APs increase power to fill the coverage hole.

• To verify roaming coverage, the survey path should follow the expected route of the mobile equipment. The recommended cell overlap is 20% but may need to be increased depending on the equipment speed and roaming parameters.

• A minimum distance of 2 meters should be maintained between antennas of the neighboring devices (either AP to WGB or AP to AP).

For additional information about site surveys, click on the following documents:

  Site Survey Guidelines for WLAN Deployment
  Site Survey and RF Design Validation

4.1.8 Radio Resource Management

4.1.8.1 RRM Overview

Radio Resource Management (RRM) is a feature of the Unified WLAN system that allows dynamic real-time optimization of RF parameters without user intervention. RRM requires system-wide visibility and is implemented at the WLC level. The WLC gets the necessary information from the APs and creates an effective channel and power plan. The APs transmit and receive RRM neighbor data packets with information about detected radios and their signal strength, including APs from the same WLAN and rogue APs.

RRM algorithms adjust the power level of the AP to maintain the baseline signal strength with the neighboring APs. RRM also reacts to interference sources and adjusts the channel accordingly. A minimum of 4 APs is needed for RRM operation. The main parts of the RRM are:

• Dynamic Channel Assignment (DCA) – system-wide channel configuration based on the noise levels, client load, and co-channel interference
• Transmit Power Control (TPC) – dynamic power configuration to maintain coverage area without using too much power, including sending power information to clients in beacons
• Coverage Hole Detection – monitoring client SNR levels and increasing power if needed
• Rogue Detection – scanning the environment for radios sharing the spectrum that do not belong to the same WLAN

4.1.8.2 RRM Recommendations

RRM greatly simplifies management and control of large scale controller-based WLANs, and is enabled as a rule in enterprise environments. However, RRM usage with real-time IACS applications presents a problem for following reasons:
• RRM operation includes periodic off-channel scanning for 60ms by the AP during which it does not pass data traffic. This may be not acceptable for the application, or cause a connection timeout.
• Off-channel scanning can increase the roaming time when fast roaming is needed for the application.
• Dynamic channel changes can cause application timeouts.

Below are recommendations for using RRM with IACS applications:
• RRM can be used during an initial site survey to determine channels and power settings and optionally during maintenance periods to check settings.
• RRM can be used for slow applications that can tolerate gaps of 60ms, however testing is recommended. Static channel assignment is also recommended. Roaming time will be increased by 60ms as well.
• A separate AP infrastructure can be used to locate interference sources and rogue devices. These extra APs can have RRM enabled but should not be allowed to accept clients.

4.1.9 Radio Interference

4.1.9.1 Overview

In the unlicensed wireless spectrum, some level of interference is always expected. The sources of interference can be non-Wi-Fi (such as microwaves or radars), or other Wi-Fi devices (unauthorized access points, for example). It is impractical to shield a production area completely from any interference, although some level of mitigation could be achieved:
• An RF spectrum site survey can detect persistent interference at the time when the survey is done. However, many sources of interference are intermittent, and new sources may appear over time. It is important to proactively monitor for radio interference in the industrial environment, before and after the deployment.
• Even small amount of interference can severely disrupt or prevent control communication in a highly utilized Wi-Fi channel. This is true not only for persistent high duty cycle interference, but also for intermittent interference with enough duration and power to cause application timeouts.
• Properly defined and enforced spectrum policy on site is critical for interference prevention (see 4.1.1.5).

Non-Wi-Fi Interference

There is a multitude of non-Wi-Fi devices operating in the unlicensed bands. The vast majority of such interference occurs in the 2.4 GHz band. Radar interference is currently the major interference source in the 5 GHz band but only for the DFS channels (see 4.1.1.6). Some of the examples are listed below.
Table 4-3 Typical Sources of Non-Wi-Fi Interference

<table>
<thead>
<tr>
<th>2.4 GHz</th>
<th>5 GHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bluetooth devices</td>
<td>Weather and military radars (DFS channels)</td>
</tr>
<tr>
<td>Cordless phones</td>
<td>Cordless phones</td>
</tr>
<tr>
<td>Microwave ovens</td>
<td>Outdoor microwave links</td>
</tr>
<tr>
<td>Wireless video cameras</td>
<td>Harmonic interference from lower frequencies</td>
</tr>
<tr>
<td>WirelessHART</td>
<td></td>
</tr>
<tr>
<td>ISA1001Ta</td>
<td></td>
</tr>
<tr>
<td>ZigBee</td>
<td></td>
</tr>
<tr>
<td>WiMAX</td>
<td></td>
</tr>
<tr>
<td>Fluorescent lights</td>
<td></td>
</tr>
<tr>
<td>Electric motors</td>
<td></td>
</tr>
<tr>
<td>Industrial microwave heaters and dryers</td>
<td></td>
</tr>
<tr>
<td>Harmonic interference from lower frequencies</td>
<td></td>
</tr>
</tbody>
</table>

These interferers typically do not cooperate with 802.11 devices, and can cause significant loss of performance for IACS applications due to decreased SNR, increased number of retries, and lower achievable data rate.

A special source of interference could be equipment operating at lower frequencies but causing certain amount of harmonic interference in Wi-Fi bands due to the non-linear transmitter characteristics. An example would be transmissions in 1...2 GHz licensed band that may affect 5 GHz band with x3 or x5 harmonics. Such noise typically does not affect a non-critical Wi-Fi traffic but may disrupt more sensitive IACS traffic. In some cases, a spectrum survey of the non-Wi-Fi frequencies may also be needed to identify the source.

There are many spectrum analysis tools available for proactive monitoring and mitigation of interference, for example the Cisco Spectrum Expert software and sensor cards. These tools can provide detailed information about interference sources, including their type, strength, duty cycle, and location.

**Wi-Fi Interference**

Interference from Wi-Fi devices operating on the same channel can be even more destructive than non-Wi-Fi interference. That is because an AP is required to share the bandwidth with any 802.11 device on the same channel, as long as it can decode the signal as a valid Wi-Fi frame (see also 4.1.5.4 for Co-Channel Interference). The sources of interference can be:

- Unauthorized APs and ad-hoc Wi-Fi networks, including routers, smartphones, and tablets
- Legitimate APs that unintentionally use the same channel, such as in OEM equipment, corporate WLAN, or other company’s WLAN
- APs and WGBs from the same WLAN that are using the same channel without proper signal separation

**CleanAir**

CleanAir is a Cisco technology that addresses the problem of radio interference in Unified WLAN architecture. CleanAir-enabled APs are enhanced with a proprietary hardware chipset that operates in parallel with normal communication, making spectrum analysis of non-Wi-Fi energy. Information on CleanAir and considerations for its use for IACS applications can be found in Appendix B.

Click on the following documents for additional information:

- [Cisco CleanAir Technology](#)
- [Cisco Spectrum Expert User Guide](#)
4.2 WLAN Configuration

4.2.1 SSID and VLAN Segmentation

This section discusses how to configure SSIDs and VLANs in the autonomous WLAN architecture, for example for topologies described in 1.2.2.1 and 1.2.2.2.

When configuring SSID and VLAN parameters for an autonomous AP, these rules should be considered:

• A single or multiple SSIDs can be configured globally on the AP. There is no default SSID in the initial configuration.

• By default, an AP has no VLANs configured. If VLANs are used, each VLAN can be associated to only one SSID.

• Each radio interface (2.4 or 5 GHz) can be configured to serve out one or several SSIDs from the list. The same SSID can be applied to both interfaces to support clients in both frequency bands.

• A WGB, like any other wireless client, can only use one SSID at a time to communicate with the AP. Multiple SSIDs can be defined globally on a WGB, however only one SSID can be configured on a radio interface in the WGB mode.

• AP or WGB management traffic over wired or wireless interface must belong to a native VLAN.

• A WGB can only associate to a single SSID which can only be mapped to a single VLAN. VLAN tagging on the radio interfaces is not supported by WGBs in the autonomous WLAN architecture. As a result, all wireless traffic from a particular WGB must belong to a single VLAN in the network.

4.2.1.1 Single VLAN / SSID

The simplest case is when one SSID and one VLAN are used for all wireless data traffic and AP management traffic:

• In this case, APs and WGBs are not configured to use VLANs. Data and management traffic from the AP is not tagged with a VLAN ID when bridged to the wired network.

• Packets coming from the AP on the wired interface can be placed in a VLAN on a switch by associating the switch port with that VLAN (so called Access Mode).

• If there are switches behind WGBs, they can use the default VLAN 1 or any VLAN ID for access mode ports. The VLAN ID has only local significance for the WGB wired network since the VLAN information is not passed via the wireless link.
Recommendations for a single VLAN / SSID topology are:

- Same VLAN should be used for all switch ports that connect APs with a common SSID (in other words, same wireless application). This ensures Layer 2 roaming (within the same IP subnet) between the APs. Layer 3 roaming (between IP subnets) is not supported in the autonomous architecture.

- A dedicated VLAN for each wireless application is recommended, according to best practices for the Cell/Area zone VLAN segmentation.

### 4.2.1.2 Multiple VLAN / SSID

Multiple SSIDs and VLANs can be implemented in the WLAN for the following use cases:

a. AP management traffic is segmented from application data traffic to conform to best network practices or existing policies.

b. The second AP radio (2.4 GHz) is used for non-critical communication within the WLAN (engineering, monitoring and so on) on a separate SSID/VLAN.

c. Each WGB is placed into its own SSID/VLAN, for example a large process skid or an OEM machine. This is not a common use case and has limited scalability, therefore not considered in this guide.

In this scenario, each SSID is linked to a VLAN on the AP. VLAN tagging is configured on the AP and switches.
Recommendations for a topology with multiple VLAN / SSID are:

- One SSID per AP radio and per channel is normally used for IACS applications. Multiple SSID on the same channel provide logical segmentation but still have to share the same amount of bandwidth.
- Separate radio channel in 2.4 GHz band is preferred for operator and maintenance personnel access on a separate VLAN / SSID.
- A native VLAN should be used for the traffic to the AP management interface. This may be different from the native VLAN used for trunking between switches.
- WGBs should not be configured to use VLANs since they do not support VLAN tagging on the radio interfaces. WGB management traffic will be placed in the same VLAN in the wired infrastructure as the data traffic.

4.2.2 Wireless QoS

4.2.2.1 Collision Avoidance Mechanism

Because multiple wireless nodes share the medium, a channel access mechanism has to be implemented to minimize collisions. The one that used by 802.11 devices today is called used Enhanced Distributed Channel Access (EDCA). It is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) method of communication, and derived from characteristics of wireless communication that are different from full-duplex switched wired Ethernet:

- Shared media: multiple nodes share the frequency and only one can successfully transmit at a time.
- Half-duplex communication: a radio cannot transmit and receive at the same time. If the medium is identified as free, the transmitter sends a wireless frame in its entirety.
• Carrier Sense: before sending data, a node listens to determine whether anyone is transmitting or not. If the channel is busy, the node defers access. This is not always reliable because of the hidden node problem: wireless clients may be able to hear the AP, but not each other due to differences in transmit power, distance, and location.

• Multiple Access: several nodes may want to transmit at the same time. There is no centralized control or strict time scheduling for media access.

• Collision avoidance – the nodes wait a random backoff time before attempt to transmit. A collision can happen if two nodes pick the same time, or if carrier sense fails to detect busy medium. ACK frames are used to indicate a successful transmission.

• Congestion control: If a collision happens, a node exponentially increases the backoff time.

EDCA uses statistical QoS mechanism to give preferential access to certain classes of traffic by changing backoff time and other parameters.

### 4.2.2.2 EtherNet/IP Classification

Most 802.11n devices use an implementation of EDCA called Wi-Fi Multimedia (WMM). There are four Access Categories (AC) for wireless traffic in the WMM:

- AC_BK Background
- AC_BE Best Effort
- AC_VI Video
- AC_VO Voice

These categories correspond to four QoS priority queues within each wireless station. Each frame that is ready to transmit is classified and placed into one of the queues. Wireless QoS parameters are defined independently for each queue so that higher priority queues have higher chance to transmit a frame. If an internal collision occurs between the queues, the higher priority queue sends the frame and the other queues act as if a physical collision happened.

Figure 4-12 WMM QoS Queues
In case of IACS wireless applications, “Video” and “Voice” categories are not typically used to communicate the actual IP video and telephony traffic. These categories are reserved for critical types of traffic such as Class 1 EtherNet/IP and CIP Sync.

The main QoS design guidelines for wired IACS networks can be applied for wireless communication as well:

- IACS traffic should take priority over other applications in the Cell/Area zone. Non-industrial traffic should have little or no effect on the IACS application.

- Different types of IACS traffic (Time Sync, Motion, I/O, and HMI) have different requirements for latency, packet loss, and jitter. The QoS policy should differentiate service for these types of flows.

Details of the QoS classification, parameters and recommendations for wired EtherNet/IP traffic can be found in the chapter 3 of the Converged Plantwide Ethernet (CPwE) Design and implementation Guide (RA publication ENET-TD001).

EtherNet/IP packets can be classified based on these parameters:

- TCP or UDP port number
- DSCP (Differentiated Services Code Point) field in the IP packet (Layer 3 QoS)
- CoS (Class of Service) field in the Ethernet frame (Layer 2 QoS)

Most IACS devices do not mark EtherNet/IP traffic with CoS but are expected to use DSCP field according to the ODVA CIP specification. Layer 3 QoS classification has more utility since it can be implemented more easily across routed networks.

- Traffic classification based on the DSCP field is recommended for more granular QoS policy.

- Wireless QoS policy should follow the ODVA guidelines for Layer-3 QoS field (DSCP) and relative priority for various types of IACS network traffic.

Table 4-4 shows the recommended mapping between DSCP, TCP/UDP ports, and WMM queues for different traffic classes:

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>CIP Priority</th>
<th>CIP Traffic Usage</th>
<th>DSCP (default)</th>
<th>CoS mapping</th>
<th>WMM Queue (AC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTP event</td>
<td>N/A</td>
<td>CIP Sync</td>
<td>59</td>
<td>6</td>
<td>AC_VO</td>
</tr>
<tr>
<td>PTP management</td>
<td>N/A</td>
<td>CIP Sync</td>
<td>47</td>
<td>4</td>
<td>AC_VI</td>
</tr>
<tr>
<td>CIP class 0 / 1</td>
<td>Urgent (3)</td>
<td>CIP Motion</td>
<td>55</td>
<td>4</td>
<td>AC_VI</td>
</tr>
<tr>
<td></td>
<td>Scheduled (2)</td>
<td>Safety I/O, I/O</td>
<td>47</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High (1)</td>
<td>I/O</td>
<td>43</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Low (0)</td>
<td>Not used</td>
<td>31</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>CIP class 3</td>
<td>All</td>
<td>CIP messaging</td>
<td>27</td>
<td>0</td>
<td>AC_BE</td>
</tr>
<tr>
<td>Unclassified</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

*1 Internal DSCP-to-CoS mapping in the AP and WGB

### 4.2.2.3 Wireless QoS Parameters

Default wireless QoS parameters in Cisco APs are optimized for enterprise applications that are most sensitive to latency, jitter, and packet loss, namely video and voice. Some parameters need to be adjusted for even more sensitive EtherNet/IP traffic:
• Minimum Contention Window (CW-min) determines the initial range for the backoff time.

• Maximum Contention Window (CW-max) determines the maximum range for the backoff time. In case of collisions, the contention window value is incremented from CW-min to CW-max.

• Fixed Slot Time is the time that a station must wait before starting the backoff timer.

• Transmit Opportunity (TXOP) is a guaranteed time interval during which a station can send as many frames as possible.

• Maximum Number of Retries limits the number of transmission attempts after collisions. If the number is exceeded, the wireless frame is dropped.

• Packet Timeout limits the time that a packet can be held in the AP or WGB queue.

Recommended settings for each WMM queue are shown in Table 4-5. There are two sets of parameters: for AP (downstream traffic) and WGB (upstream traffic).

Table 4-5 Wireless QoS Parameters for EtherNet/IP

<table>
<thead>
<tr>
<th>WMM Queue (AC)</th>
<th>Traffic Type</th>
<th>AP or WGB</th>
<th>Contention Window</th>
<th>Fixed Slot Time</th>
<th>TXOP</th>
<th>Max Retries</th>
<th>Packet Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>CW-min</td>
<td>CW-max</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC_VO</td>
<td>PTP events</td>
<td>AP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WGB</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AC_VI</td>
<td>CIP Class 0 / 1 PTP mgmt</td>
<td>AP</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WGB</td>
<td>7</td>
<td>7</td>
<td>3</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>AC_BE</td>
<td>CIP Class 3, non-CIP traf</td>
<td>AP</td>
<td>8</td>
<td>10</td>
<td>12</td>
<td>0</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WGB</td>
<td>8</td>
<td>10</td>
<td>12</td>
<td>0</td>
<td>16</td>
</tr>
<tr>
<td>AC_BK</td>
<td>non-CIP traffic (lowest priority)</td>
<td>AP</td>
<td>8</td>
<td>10</td>
<td>15</td>
<td>0</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WGB</td>
<td>8</td>
<td>10</td>
<td>15</td>
<td>0</td>
<td>16</td>
</tr>
</tbody>
</table>

For more information on wireless QoS, see the following guide:

Cisco Unified Wireless QoS

4.2.3 WLAN Security

4.2.3.1 Overview

The nature of wireless communication requires implementation of strong security mechanisms. Among the security risks are:

• Data interception and monitoring

• Denial of Service (DoS) attacks

• Wireless frame spoofing

WLAN security is implemented using authentication between devices and encryption of data and management traffic. The main security mechanisms for WLAN networks are:

• Wi-Fi Protected Access 2 (WPA2) – the most advanced and widely used today.

• Wi-Fi Protected Access (WPA) – only used by old firmware and hardware that cannot support WPA2.

• Wired Equivalent Privacy (WEP) and its extensions – this legacy mechanism is easily compromised and must not be used anymore.
WPA2 standard supports pre-shared key authentication or IEEE 802.1X authentication framework. It supports Advanced Encryption Standard (AES) as the most advanced and secure method of encryption.

- WPA2 security with AES encryption is the only mechanism recommended for IACS wireless applications.
- AES encryption is implemented in hardware and does not significantly affect application performance.

Additional protection against wireless security attacks is provided by:

- Wireless Intrusion Prevention System (wIPS) in the Unified WLAN architecture
- Management Frame Protection in the autonomous and Unified WLAN architectures.

4.2.3.2 WLAN Authentication

Before a wireless client can communicate through the AP, it must authenticate to it by using one of the available methods. Authentication is defined for each SSID individually, and multiple methods can exist in the same WLAN, for example to provide guest access or to support different types of clients.

After successful authentication, a secure tunnel is established between the client and the AP to generate encryption keys for wireless data frame protection.

Pre-Shared Key Authentication

This method relies on a common password configured on the autonomous AP or WLC and the client. This is the simple method that may work well in the WLAN where wireless clients are tightly controlled. An example would be a wireless application with fixed number of mobile machines using WGBs.

The limitations of the pre-shared key authentication are:

- It cannot be used to limit access only to certain clients. Anyone with knowledge of the key can authenticate to the WLAN.
- Once the key is compromised, all devices need to be reconfigured with the new key.
- Pre-shared key authentication may not be supported with some of the fast roaming methods, or may not provide the fastest roaming time.

MAC Address Authentication

This method uses the client’s MAC address as the way to authenticate. It can be useful as an additional protection against incidental connections to a WLAN where a critical application is operating and the bandwidth is limited.

- This is not a secure method by itself since MAC addresses can be spoofed. MAC address authentication should only be used with other methods such as pre shared key or 802.1x authentication.

802.1x-based Authentication

802.1X is an IEEE framework for port-based access control which has been adopted by the 802.11 standard. It relies on the Extensible Authentication Protocol (EAP) to provide authenticated access to a WLAN:

- Initially, the AP blocks all data frames from a client and only allows 802.1X-based traffic.
- The 802.1X frames carry the EAP authentication packets, which are forwarded by the AP or WLC to the authentication server, or processed locally.
The authentication server communicates with the AP or WLC (the authenticator) using a RADIUS protocol (Remote Access Dial In User Service). The RADIUS server checks the client's credentials against the user database, for example an Active Directory.

Small networks can implement local authentication by the AP or WLC rather than a dedicated RADIUS server. In this case, client credentials are defined and stored locally in the AP or WLC database.

If the EAP authentication is successful, the AP allows data traffic from the WLAN client to pass through.

**Figure 4-13 802.1X/EAP with RADIUS server**

802.1X/EAP authentication is the most secure method that provides the following advantages:
- Strong security that conforms to enterprise standards and industry regulations
- Access based on individual user credentials rather than one common password
- Granular access control based on the user's role and privileges
- Logging of individual user access
- Support of fast roaming methods

802.1X/EAP method requires more advanced configuration and often involves additional infrastructure components such as RADIUS servers. In most cases, existing IT infrastructure can be utilized.

**4.2.3.3 EAP Authentication Types**

There are several implementations of EAP available for secure wireless deployments. Regardless of the protocol, they all use 802.1X and RADIUS as their underlying transport.

Main factors affecting the choice of EAP protocol are:
- Existing authentication system and IT infrastructure that can be utilized
• Existing IT policies and regulations
• Complexity of implementation and support, particularly whether it requires use of digital certificates
• Support by the WLAN client software, authentication server, and user database platform
• Local authentication support by an autonomous AP or WLC

Some of the protocols implemented in the Cisco autonomous and Unified WLAN architectures are shown in the table below:

<table>
<thead>
<tr>
<th>EAP-FAST</th>
<th>PEAP MS-CHAPv2</th>
<th>PEAP EAP-GTC</th>
<th>EAP-TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS server certificate required?</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Client certificate required?</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Local authentication (autonomous AP)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Local authentication (WLC)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

• EAP-FAST is the recommended 802.1X-based protocol for IACS wireless networks due to reduced complexity and support for local authentication.

4.2.3.4 Management Frame Protection

The 802.11n standard uses special frame types for management and control of wireless links. Unlike data traffic which can be encrypted to provide confidentiality, these frames must be understood by all clients and therefore must be transmitted as unencrypted.

In highly secured environment, management frames must be protected from security attacks. For example, an attacker could spoof management frames from an AP to force a client to disassociate.

802.11w is the Protected Management Frames standard that is implemented in the latest Cisco autonomous and Unified code releases. It protects disassociation, deauthentication, and certain other types of frames by offering:
• Data integrity
• Data origin authenticity
• Replay detection

Certain frames, such as beacons and association probe / requests, cannot be protected, since they are transmitted before the authentication phase. Wireless IPS measures can be used to monitor and react for low level types of attacks such as beacon frame spoofing and association flood.

• The effect of enabling management frame protection (MFP) on IACS application performance has not been yet determined. It is recommended to disable MFP for EtherNet/IP applications unless required by wireless security policy.

4.2.3.5 Additional Resources

For more information on wireless security, click on the following documents:

- Cisco Unified Wireless Network Architecture – Base Security Features
- Design Zone for Mobility – Wireless Security
5. Summary of Recommendations

5.1 Application Recommendations

5.1.1 Network Topology
WLAN architectures, industrial wireless use cases and typical topologies for IACS applications are reviewed in Chapter 1.

- Workgroup bridge (WGB) is the special AP mode that can be used to connect multiple wired IACS devices to a WLAN (1.1.3.3).
- It is recommended not to exceed 20 wireless nodes (WGBs or embedded adapters) per AP for EtherNet/IP applications.
- Number of wired clients that communicate over wireless link should be limited to 19 per WGB.
- The total number of Ethernet devices on a single VLAN (wired or wireless) should be below 200 to restrict the amount of broadcast traffic.

5.1.2 Packet Rate Limitations
- Total packet rate in a wireless channel is the main factor that determines application performance (2.1.2).
- Do not exceed 2,200 pps in the wireless channel with EtherNet/IP traffic.
- Reduce packet rate in environments with RF issues and interference.
- Reserve 20% of bandwidth for HMI and maintenance traffic such as web page diagnostic, programming tools etc.
- All communication should be accounted in the total packet rate calculations, including non-CIP packets and traffic from neighboring WLAN sharing the same channel.
- Direct communication between wireless clients should be limited and kept at low rates. Wireless to wireless communication doubles the number of packets that needs to be transmitted and inefficiently uses the available bandwidth.
- A number of application optimization methods can be used to lower the total packet rate and improve the performance:
  - Use rack optimized I/O connections when possible.
  - PAC to PAC communication with Produced / Consumed tags is more efficient than PAC to I/O communication.
  - Instead of using direct wireless communication from multiple PACs, aggregate wireless traffic through a single PAC in the wired infrastructure.
  - Instead of using many individual connections, Produced / Consumed data can be combined into large arrays and user-defined data types (UDT) with one or few connections.
  - Different types of data can be carried in the one Produced / Consumed tag. For example, standard data can be appended to the safety Produced / Consumed data if RPI is sufficient.
  - The most efficient situation is transmission of one wireless packet in each direction during a cycle.
### 5.1.3 Application Parameters

- The table below lists various CIP protocols and their potential use with 802.11n wireless communication:

<table>
<thead>
<tr>
<th>IACS Protocol Type</th>
<th>CIP Standard</th>
<th>Use with Wireless</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information and diagnostics, process control</td>
<td>CIP Class 3 (HMI)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Peer to peer messaging</td>
<td>CIP Class 3 (MSG instructions)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Peer to Peer Control</td>
<td>CIP Class 1</td>
<td>Yes</td>
<td>Higher latency and jitter may be an issue if an application depend on exact timing of updates</td>
</tr>
<tr>
<td>I/O Control</td>
<td>CIP Class 1 I/O</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Safety Control</td>
<td>CIP Safety</td>
<td>Yes</td>
<td>Very fast safety reaction times may not be supported (see Summary of Results)</td>
</tr>
<tr>
<td>Time Synchronization (IEEE 1588 PTP)</td>
<td>CIP Sync</td>
<td>Limited</td>
<td>Accuracy of ~150 µs can be achieved; suitable for SOE and event logging applications; (see 2.2.2.5)</td>
</tr>
<tr>
<td>Motion Control</td>
<td>CIP Motion; Produced / Consumed Virtual Axis</td>
<td>Experimental</td>
<td>Position accuracy depends on CIP Sync performance; Direct CIP Motion control is not feasible; Virtual Produced / Consumed axis may be possible for low performance applications</td>
</tr>
</tbody>
</table>

- Use unicast connections with wireless I/O or Produced / Consumed data (2.1.5).
- Do not use ControlLogix Redundancy System with wireless communication.
- Standard RPI of 20ms can be supported. RPIs as low as 10ms may be supported depending on the application sensitivity to jitter and delay.
- Safety RPI as low as 15ms can be supported (Produced / Consumed), as long as the packet rate is below the limit.
- Connection Reaction Time Limit for a CIP Safety connection over wireless should be at least:
  - 60 ms for Safety Produced / Consumed
  - 72 ms for Safety I/O
- CRTL may need to be increased further to prevent safety connection timeouts by changing Safety Timeout or Network Delay multipliers.
- For greater long-term reliability, increase CRTL to be at least x4 greater than the RPI value. This allows 3 packets in a row to be lost before the timeout.
- CIP Sync protocol can be supported for certain applications with following considerations (2.2.2.5):
  - The time accuracy of 150 µs has been achieved in the test environment which indicates possible use of CIP Sync across wireless media for SoE and logging applications.
  - Use the latest firmware versions for RA components that support CIP Sync.
  - Place Grandmaster clock (GM) in the wired infrastructure behind the AP.
  - Eliminate unnecessary variable delays in the network, for example extra switch hops or unmanaged switches.
  - Use PTP transparent mode for switches that support PTP protocol.
  - Configure QoS settings with highest priority for CIP Sync traffic.
  - Configure IGMP snooping and querier in the network infrastructure to allow multicast traffic across wireless link.
- Direct CIP Motion control is not feasible over wireless. Virtual Produced / Consumed axis may be possible for low performance applications. Position accuracy will depend on the CIP Sync performance.
5.2 RF Design Recommendations

5.2.1 Wireless Spectrum

- 5 GHz frequency band is recommended for industrial wireless applications. Because of limited number of channels and much higher chance of interference, the 2.4 GHz band is not recommended to use for critical IACS applications, such as machine control. However, 2.4 GHz band can be used for personnel access and low throughput non-critical applications (4.1.1.1).
- Number of available channels and existing bandwidth utilization is the critical factor when implementing wireless IACS applications.
- Proper spectrum management policy and coordination between IT, OEM, ands control engineers is critical.
- As the rules constantly change, refer to the local regulatory authority, product documentation and the Cisco website for the most recent compliance information and channel availability in a particular country.
- Use only channels 1, 6, and 11 in the 2.4 GHz band. Use of non-standard channels or more than 3 channels in 2.4 GHz band will cause adjacent channel interference and lower throughput.
- Use non-DFS channels in 5 GHz band when possible (4.1.1.6).
- If DFS channels are used, thorough site survey and subsequent monitoring of DFS channels is required before and after the installation. Particular caution should be used when operating near airports, sea ports, military bases, or large cities.
- RF spectrum analysis is critical for IACS applications with high bandwidth utilization and low latency requirements. Adequate time should be spent analyzing the channels to detect intermittent interference.
- Many sources of interference are intermittent, and new sources may appear over time. It is important to proactively monitor for radio interference in the industrial environment, before and after the deployment.
- Properly defined and enforced spectrum policy on site is critical for interference prevention.

5.2.2 Wireless Coverage

- AP coverage area where desired data rate can be supported depends on many factors and can only be determined during the site survey. Changes in the environment and interference levels also dynamically change the coverage (4.1.5).
- For EtherNet/IP applications, recommended parameters that should be maintained in the coverage area are:
  - Minimum RSSI of -67 dBm
  - Minimum SNR of 25 dB
- For CIP Sync traffic, the cell coverage area should be designed to sustain 54 Mbps data rate.
- Antenna recommendations can be found in 4.1.6.
- Professional site survey is critical for WLAN implementation. Recommendations and best practices for site surveys in industrial environments can be found in 4.1.7.

5.2.3 RF Parameters

- Spatial Division Multiplexing (4.1.2.1) has limited benefit for the real-time EtherNet IP traffic. Multiple spatial streams make communication less reliable, dependent on higher SNR, and more susceptible to multipath fading. Single spatial stream is more suitable for control communication.
- 20 MHz channel width (no channel bonding) is recommended with IACS applications (4.1.2.4).
- Frame aggregation can be beneficial for point-to-point type of communication, or with small number of nodes (4.1.2.5). The positive or negative effect of aggregation should be determined in the application testing.
• Follow data rate recommendations provided in 4.1.4.
• Follow transmit power recommendations in 4.1.5.2.
• Follow channel configuration recommendations in 4.1.5.4.
• Dynamic RF configuration with RRM in Unified WLAN is not recommended (4.1.8):
  - RRM can be used during an initial site survey to determine channels and power settings and optionally during maintenance periods to check settings.
  - RRM can be used for slow applications that can tolerate gaps of 60ms, however testing is recommended.
  Static channel assignment is also recommended. Roaming time will be increased by 60ms as well.

5.3 WLAN Configuration Recommendations

5.3.1 VLAN and SSID Segmentation
• Recommendations for a single VLAN / SSID topology are (4.2.1.1):
  - Same VLAN should be used for all switch ports that connect APs with a common SSID (in other words, same wireless application). This ensures Layer 2 roaming (within the same IP subnet) between the APs. Layer 3 roaming (between IP subnets) is not supported in the autonomous architecture.
  - A dedicated VLAN for each wireless application is recommended, according to best practices for the Cell/Area zone VLAN segmentation.
• Recommendations for a topology with multiple VLAN / SSID are (4.2.1.2):
  - One SSID per AP radio and per channel is normally used for IACS applications. Multiple SSID on the same channel provide logical segmentation but still have to share the same amount of bandwidth.
  - Separate radio channel in 2.4 GHz band is preferred for operator and maintenance personnel access on a separate VLAN / SSID.
  - A native VLAN should be used for the traffic to the AP management interface. This may be different from the native VLAN used for trunking between switches.
  - WGBs should not be configured to use VLANs since they do not support VLAN tagging on the radio interfaces. WGB management traffic will be placed in the same VLAN in the wired infrastructure as the data traffic.

5.3.2 Wireless QoS
• Traffic classification based on the DSCP field is recommended for more granular QoS policy.
• Wireless QoS policy should follow the ODVA guidelines for Layer-3 QoS field (DSCP) and relative priority for various types of IACS network traffic. Recommended scheme is provided in Table 4-4.
• Wireless QoS parameters for radio interfaces should be configured as recommended in Table 4-5.
• For more information on wireless QoS, refer to 4.2.2.

5.3.3 Wireless Security
• WPA2 security with AES encryption is the only mechanism recommended for IACS wireless applications. AES encryption is implemented in hardware and does not significantly affect application performance (4.2.3.1).
• MAC address authentication is not a secure method by itself since MAC addresses can be spoofed. It should only be used with other methods such as pre-shared key or 802.1x authentication.
• WPA2-PSK is the most common method of authentication in WGB-based topologies (4.2.3.2).
• EAP-FAST is the recommended 802.1X-based protocol for IACS wireless networks due to reduced complexity and support for local authentication (4.2.3.3).
# Test Details

## Test Equipment

Table A-1 and Table A-2 list the network and IACS equipment used in the testing.

### Table A-1 Network Equipment

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Software</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIR-CAP2602E-A-K9</td>
<td>Cisco 2600 autonomous AP</td>
<td>15.2(4)</td>
<td></td>
</tr>
<tr>
<td>AIR-ANT2424DW-R</td>
<td>Cisco 2.4/5GHz dipole antenna</td>
<td></td>
<td>Omnidirectional 4 dBi (5GHz)</td>
</tr>
<tr>
<td>WS-C3750X-12S</td>
<td>Cisco 3750X stackable switch</td>
<td>12.2(58)SE2</td>
<td>Distribution Layer 3 switches in the redundant stack</td>
</tr>
<tr>
<td>1783-MS10T</td>
<td>Stratix 8000 10-port managed switch</td>
<td>12.2(58)SE2</td>
<td>Access layer switches</td>
</tr>
</tbody>
</table>

### Table A-2 IACS Equipment

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Software</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1756-L73S</td>
<td>GuardLogix safety controller 12 MB</td>
<td>20.012</td>
<td>Main test equipment</td>
</tr>
<tr>
<td>1756-L7SP</td>
<td>GuardLogix safety partner</td>
<td>20.012</td>
<td></td>
</tr>
<tr>
<td>1756-EN2TR</td>
<td>ControlLogix two-port Ethernet/IP communication module</td>
<td>5.008</td>
<td></td>
</tr>
<tr>
<td>1734-AENTR</td>
<td>POINT two-port EtherNet/IP I/O Adapter module</td>
<td>3.010</td>
<td></td>
</tr>
<tr>
<td>1734-IB8S</td>
<td>POINT digital DC safety input module</td>
<td>1.001</td>
<td></td>
</tr>
<tr>
<td>1734-OB8S</td>
<td>POINT digital DC safety output module</td>
<td>1.001</td>
<td></td>
</tr>
<tr>
<td>1734-IB8</td>
<td>POINT digital DC input module</td>
<td>3.018</td>
<td>Additional equipment for network latency and System Reaction Time measurements</td>
</tr>
<tr>
<td>1734-OB8</td>
<td>POINT digital DC output module</td>
<td>3.018</td>
<td></td>
</tr>
<tr>
<td>1756-L75</td>
<td>ControlLogix controller 32 MB</td>
<td>20.011</td>
<td></td>
</tr>
<tr>
<td>1756-IB16IF</td>
<td>ControlLogix digital DC fast input module</td>
<td>1.011</td>
<td></td>
</tr>
<tr>
<td>1756-OB16IEF</td>
<td>ControlLogix digital DC fast output module</td>
<td>1.011</td>
<td></td>
</tr>
<tr>
<td>1756-IB16ISOE</td>
<td>ControlLogix SOE Input Module</td>
<td>2.009</td>
<td></td>
</tr>
</tbody>
</table>

## Configuration Details

### Radio Settings

Radio characteristics and physical layout of the test were as follows:

- Indoor omnidirectional dipole antennas were used.
- Workgroup bridges were placed at the 4...15m distance from the AP. The transmit power was set to 5 dBm or 8 dBm to maintain adequate RSSI and SNR values.
- All access points were placed at least 2m apart from each other.
- Unoccupied channel 40 (5200 MHz) and 20 MHz channel width was used during the testing. Cisco Spectrum Expert software was used to check the channel usage and duty cycle. In addition, AirPcap Nx card was used to capture possible traffic and check for beacons in the channel.
- Frame aggregation was disabled for all traffic.
- Basic rates were configured as 6, 12, 24, 54 Mbps, and rest of 802.11a rates as enabled.
- MCS data rates were disabled during the testing.
- Long guard interval (800ns) was used.
- Other parameters were kept as factory default.
WLAN Settings

- Single SSID and VLAN were used for all workgroup bridges.
- WPA2 authentication with pre-shared keys and AES-CCMP encryption was used.
- Client management frame protection (MFP) was disabled for the SSID.
- QoS configuration followed the guidelines in Table 4-4 and Table 4-5.
- Spanning Tree was disabled on radio and Ethernet interfaces of the access points. This is a recommended practice.
- Reliable Multicast delivery to WGBs was disabled on the root access point.
- CDP (Cisco Discovery Protocol) was disabled on radio interfaces.

Other Settings

- Express Setup configuration and Smartport templates were used for Stratix 8000 switches as the template. The standard Stratix QoS policy was applied to all switch ports, including Cisco 3750X.
- Communication format was set to “None” for the 1756-EN2TR modules and “Rack Optimized” for the 1734-AENTR modules.
- QoS was enabled for the EtherNet/IP modules.
- CIP Sync was disabled on the EN2TR modules.

Full Configurations

AP and WGB test configurations in CLI text format are shown below.

- These configurations are provided for reference only and must not be used “as is” without adapting for a particular IACS application and topology.
- The configurations were used with Cisco 2602 autonomous APs and IOS 15.2(4) software. Some commands may not apply for different AP models and software releases.
- Many commands are factory default and do not have to be configured during the initial setup.

This is an example of AP configuration used in the testing.

version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AAP1
!
logging rate-limit console 9
enable secret <REMOVED>
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
!
aaa session-id common
ip cef
ip domain name local
!
dot11 syslog
!
dot11 ssid <REMOVED>
  authentication open
  authentication key-management wpa version 2
  wpa-psk ascii <REMOVED>
  no ids mfp client
!
dot11 phone dot11e
dot11 guest
!
ipv6 spd queue min-threshold 98
ipv6 spd queue max-threshold 99
!
username admin privilege 15 secret <REMOVED>
!
ip ssh version 2
!
class-map match-all _class_PTP_EVENT
  match ip dscp 59
class-map match-all _class_PTP_GEN
  match ip dscp 47
class-map match-all _class_IO_HIGH
  match ip dscp 43
class-map match-all _class_IO_LOW
  match ip dscp 31
class-map match-all _class_IO_SCH
  match ip dscp 47
class-map match-all _class_IO_URG
  match ip dscp 55
class-map match-all _class_EXPLICIT
  match ip dscp 27
!
policy-map ODVA
  class _class_PTP_EVENT
    set cos 6
class _class_PTP_GEN
    set cos 4
class _class_IO_URG
  set cos 4
class _class_IO_SCH
  set cos 4
class _class_IO_HIGH
  set cos 4
class _class_IO_LOW
  set cos 4
!
bridge irb
!
interface Dot11Radio0
  no ip address
  shutdown
  antenna gain 0
  station-role root
  no cdp enable
  bridge-group 1
    bridge-group 1 subscriber-loop-control
    bridge-group 1 spanning-disabled
    bridge-group 1 block-unknown-source
    no bridge-group 1 source-learning
    no bridge-group 1 unicast-flooding
  
interface Dot11Radio1
  no ip address
  no ip route-cache
  
  encryption mode ciphers aes-ccm
  
  ssid <REMOVED>
  
  antenna gain 4
  peakdetect
  dfs band 3 block
  stbc
  no ampdu transmit priority 0
  no ampdu transmit priority 4
  no ampdu transmit priority 5
  guard-interval long
  speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 basic-54.0
  power local <REMOVED>
packet retries 16 drop-packet
packet max-retries 4 0 fail-threshold 100 500 priority 4 drop-packet
packet max-retries 0 0 fail-threshold 100 500 priority 6 drop-packet
packet timeout 10 priority 4
packet timeout 1 priority 6
packet speed 6.0 54.0 priority 6
channel <REMOVED>
station-role root access-point
dot11 qos class background local
cw-min 8
cw-max 10
fixed-slot 15
transmit-op 0
!
dot11 qos class best-effort local
cw-min 8
cw-max 10
fixed-slot 12
transmit-op 0
!
dot11 qos class video local
cw-min 0
cw-max 0
fixed-slot 2
transmit-op 0
!
dot11 qos class voice local
cw-min 0
cw-max 0
fixed-slot 0
transmit-op 0
!
dot11 qos class background cell
cw-min 8
cw-max 10
fixed-slot 15
transmit-op 0
!
dot11 qos class best-effort cell
cw-min 8
cw-max 10
fixed-slot 12
transmit-op 0
!
dot11 qos class video cell
  cw-min 7
  cw-max 7
  fixed-slot 3
  transmit-op 0
!
dot11 qos class voice cell
  cw-min 3
  cw-max 3
  fixed-slot 1
  transmit-op 0
!
no cdp enable
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
service-policy input ODVA
service-policy output ODVA
hold-queue 100 in
!
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
no keepalive
bridge-group 1
bridge-group 1 spanning-disabled
!
interface BVI1
ip address 10.20.10.21 255.255.255.0
!
ip forward-protocol nd
ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.20.10.1
!
bridge 1 route ip
!
line con 0
  logging synchronous
line vty 0 4
  logging synchronous
  transport input all
line vty 5 15
  transport input all
!
end

This is an example of WGB configuration used in the testing.
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname WGB02
!
logging rate-limit console 9
enable secret <REMOVED>
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
!
aaa session-id common
ip cef
ip domain name local
!
dot11 syslog
!
dot11 ssid <REMOVED>
  authentication open
  authentication key-management wpa version 2
  wpa-psk ascii <REMOVED>
no ids mfp client
!
dot11 guest
!
username admin privilege 15 secret <REMOVED>
!
ip ssh version 2
!
class-map match-all _class_PTP_EVENT
  match ip dscp 59
class-map match-all _class_PTP_GEN
  match ip dscp 47
class-map match-all _class_IO_HIGH
  match ip dscp 43
class-map match-all _class_IO_LOW
  match ip dscp 31
class-map match-all _class_IO_SCH
  match ip dscp 47
class-map match-all _class_IO_URG
  match ip dscp 55
class-map match-all _class_EXPLICIT
  match ip dscp 27
!
policy-map ODVA
  class _class_PTP_EVENT
    set cos 6
  class _class_PTP_GEN
    set cos 4
  class _class_IO_URG
    set cos 4
  class _class_IO_SCH
    set cos 4
  class _class_IO_HIGH
    set cos 4
  class _class_IO_LOW
    set cos 4
!
bridge irb
!
interface Dot11Radio0
no ip address
shutdown
antenna gain 0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding

! interface Dot11Radio1
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid <REMOVED>
!
antenna gain 4
peakdetect
stbc
no ampdu transmit priority 0
no ampdu transmit priority 4
no ampdu transmit priority 5
guard-interval long
power local <REMOVED>
packet retries 16 drop-packet
packet max-retries 4 0 fail-threshold 100 500 priority 4 drop-packet
packet max-retries 0 0 fail-threshold 100 500 priority 6 drop-packet
packet speed 6.0 54.0 priority 6
station-role workgroup-bridge
no cdp enable
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
service-policy input ODVA
service-policy output ODVA

interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
no keepalive
bridge-group 1
bridge-group 1 spanning-disabled

interface BVI1
ip address 10.20.10.32 255.255.255.0

ip forward-protocol nd
ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.20.10.1

bridge 1 route ip
bridge 1 aging-time 3600

line con 0
logging synchronous
line vty 0 4
logging synchronous
transport input all

end
**Test Measurements**

The key parameters that were measured for each test suite. To establish a point of reference, System Reaction Time and Network Latency data were also measured using a wired connection.

The key difference in measurements between the I/O and Produced / Consumed tests was how the System Reaction Time was measured. In the Produced / Consumed safety chain, the SRT was measured twice: from a wired safety input to a wireless safety output, and from a wireless safety input to a wired safety output.

**Table A-3 Safety I/O Test Measurements**

<table>
<thead>
<tr>
<th>Test Data</th>
<th>Data Source</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Reaction Time</td>
<td>Test application (1756-L73S)</td>
<td>Measured screw-to-screw time from wireless safety input to wireless safety output</td>
</tr>
<tr>
<td>I/O connection faults</td>
<td></td>
<td>For all I/O modules in the test, including safety and rack optimized connections</td>
</tr>
<tr>
<td>Maximum observed network delay (round-trip)</td>
<td>Safety I/O module properties – Safety tab</td>
<td>For all Safety I/O modules in the test; measures round-trip delay between the PAC and I/O</td>
</tr>
<tr>
<td>Network latency and % of lost packets (AP to WGB)</td>
<td>Test application (1756-L75)</td>
<td>Measured screw-to-screw time from local input module to remote output module</td>
</tr>
<tr>
<td>Wireless interface statistics</td>
<td>All access points</td>
<td>–</td>
</tr>
<tr>
<td>Traffic flow statistics</td>
<td>Wireshark captures</td>
<td>–</td>
</tr>
</tbody>
</table>

**Table A-4 Safety Produced / Consumed Test Measurements**

<table>
<thead>
<tr>
<th>Test Data</th>
<th>Data Source</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Reaction Time</td>
<td>Test application (1756-L73S)</td>
<td>Measured screw-to-screw time: 1. From wired safety input to wireless safety output (downstream); 2. From wireless safety input to wired safety output (upstream).</td>
</tr>
<tr>
<td>Produced / Consumed connection faults</td>
<td></td>
<td>For all connections, including standard and safety</td>
</tr>
<tr>
<td>Network latency and % of lost packets (AP to WGB)</td>
<td>Test application (1756-L75)</td>
<td>Measured screw-to-screw time from local input module to remote output module</td>
</tr>
<tr>
<td>Wireless interface statistics</td>
<td>All access points</td>
<td>–</td>
</tr>
<tr>
<td>Traffic flow statistics</td>
<td>Wireshark captures</td>
<td>–</td>
</tr>
</tbody>
</table>
Test Variables

Tables below summarize application parameters that were selected for the testing. Default GuardLogix safety and standard parameters and RPI values were used as a starting point. These parameters were then adjusted to create desirable total packet rate in the channel.

For a given safety input RPI and safety task period, timeout multipliers were adjusted to change the CRTL numbers. The main goal was to achieve the reliable long-term communication without safety connection faults. The test results were then compared against the other application requirements (SRT and latency).

In all test suites, safety task scan time was increased to 8 ms by using simulated ladder logic.

Table A-5 Safety I/O Test Variables

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Options</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td># of WGBs</td>
<td>4, 8</td>
<td>–</td>
</tr>
<tr>
<td># of POINT I/O chassis per WGB</td>
<td>1, 2, 3</td>
<td>1 I/O rack x 8 WGBs, 3 I/O racks x 4 WGBs, 2 I/O racks x 4 WGBs</td>
</tr>
<tr>
<td># of safety modules per rack</td>
<td>2</td>
<td>1734-IB8S, 1734-OB8S</td>
</tr>
<tr>
<td># of discrete modules per rack</td>
<td>2</td>
<td>1734-IB8, 1734-OB8</td>
</tr>
<tr>
<td>Safety Input RPI</td>
<td>12 ms, 18 ms, 24 ms</td>
<td>–</td>
</tr>
<tr>
<td>Safety Task Period (same as Safety Output RPI)</td>
<td>20 ms, 30 ms, 40 ms</td>
<td>–</td>
</tr>
<tr>
<td>Standard I/O RPI</td>
<td>20 ms, 40 ms</td>
<td>Rack optimized connection</td>
</tr>
<tr>
<td>Safety Timeout Multipliers</td>
<td>x2, x4</td>
<td>–</td>
</tr>
<tr>
<td>Network Delay Multipliers</td>
<td>200%</td>
<td>Both input and output safety connections</td>
</tr>
<tr>
<td>Safety Task Scan Time</td>
<td>8 ms</td>
<td>Simulated ladder logic</td>
</tr>
<tr>
<td>Safety Task Watchdog</td>
<td>11 ms</td>
<td>–</td>
</tr>
</tbody>
</table>

Table A-6 Safety Produced / Consumed Test Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Options</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td># of WGBs</td>
<td>8</td>
<td>–</td>
</tr>
<tr>
<td># of PACs per WGB</td>
<td>1</td>
<td>–</td>
</tr>
<tr>
<td>Safety Task Period (same as Safety P/C RPI)</td>
<td>15 ms, 20 ms</td>
<td>–</td>
</tr>
<tr>
<td>Standard P/C RPI</td>
<td>8 ms, 10 ms</td>
<td>Same for producer and consumer</td>
</tr>
<tr>
<td>P/C Timeout Multipliers</td>
<td>x2</td>
<td>–</td>
</tr>
<tr>
<td>P/C Network Delay Multipliers</td>
<td>200%</td>
<td>–</td>
</tr>
<tr>
<td>Safety I/O Input RPI (wired)</td>
<td>12 ms</td>
<td>Wired connection</td>
</tr>
<tr>
<td>Safety I/O Output RPI (wired)</td>
<td>15 ms, 20 ms</td>
<td>Wired connection</td>
</tr>
<tr>
<td>Safety Task Scan Time</td>
<td>8 ms</td>
<td>Simulated ladder logic</td>
</tr>
<tr>
<td>Safety Task Watchdog</td>
<td>11 ms</td>
<td>–</td>
</tr>
</tbody>
</table>
Test Suites

Below are the test suites for Safety I/O and Safety Produced / Consumed topologies. The main characteristics for a test suite are the number of wireless nodes (WGBs) and the total packet rate in the wireless channel. These parameters determine the overall performance of the wireless network.

The calculated packet rate below does not include network and CIP control packets, such as ARP, TCP etc., and additional latency test traffic. The actual network load, as determined by the interface statistics on the AP and WGBs, was 5-10% higher.

A number of tests were performed with simulated CIP Class 3 traffic using IXIA packet generator hardware and the following parameters:

- 400 pps (~20% of the total channel load)
- TCP/IP port 44818, QoS DSCP 27
- Ethernet frame sizes:
  - 64 bytes (15%), 128 bytes (40%), 256 bytes (20%), 512 bytes (25%)

Generated packet mix was selected by observing the actual traffic generated by a PanelView™ HMI and RSLogix 5000 online with the PAC.

### Table A-7 Safety I/O Test Suites

<table>
<thead>
<tr>
<th>Test suite</th>
<th>Std. and Safety I/O Packet rate, pps</th>
<th>IXIA Packet rate, pps</th>
<th># of WGBs</th>
<th>Std. I/O RPI, ms</th>
<th>Safety Input RPI, ms</th>
<th>Safety Task Period, ms</th>
<th>Timeout mult.</th>
<th>CRTL, ms</th>
<th>System Reaction Time (Theoretical), ms</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IO-8x1-A1</td>
<td>2,933</td>
<td>-</td>
<td>8</td>
<td>1</td>
<td>20</td>
<td>12</td>
<td>20</td>
<td>2</td>
<td>48 60 89 125</td>
</tr>
<tr>
<td>IO-8x1-A2</td>
<td>2,933</td>
<td>-</td>
<td>8</td>
<td>1</td>
<td>20</td>
<td>12</td>
<td>20</td>
<td>4</td>
<td>72 100 89 165</td>
</tr>
<tr>
<td>IO-8x1-B1</td>
<td>2,222</td>
<td>-</td>
<td>8</td>
<td>1</td>
<td>20</td>
<td>18</td>
<td>18</td>
<td>2</td>
<td>72 90 117 171</td>
</tr>
<tr>
<td>IO-8x1-C1</td>
<td>1,822</td>
<td>-</td>
<td>8</td>
<td>1</td>
<td>40</td>
<td>18</td>
<td>30</td>
<td>2</td>
<td>72 90 117 171</td>
</tr>
<tr>
<td>IO-8x1-X1</td>
<td>1,822</td>
<td>400</td>
<td>8</td>
<td>1</td>
<td>40</td>
<td>18</td>
<td>30</td>
<td>2</td>
<td>72 90 117 171</td>
</tr>
<tr>
<td>IO-4x3-A1</td>
<td>3,333</td>
<td>-</td>
<td>4</td>
<td>3</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>2</td>
<td>72 90 117 171</td>
</tr>
<tr>
<td>IO-4x3-A2</td>
<td>3,333</td>
<td>-</td>
<td>4</td>
<td>3</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>4</td>
<td>108 150 117 231</td>
</tr>
<tr>
<td>IO-4x3-B1</td>
<td>2,800</td>
<td>-</td>
<td>4</td>
<td>3</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>2</td>
<td>72 90 117 217</td>
</tr>
<tr>
<td>IO-4x2-A1</td>
<td>2,222</td>
<td>-</td>
<td>4</td>
<td>2</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>2</td>
<td>72 90 117 171</td>
</tr>
<tr>
<td>IO-4x2-X1</td>
<td>2,222</td>
<td>400</td>
<td>4</td>
<td>2</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>2</td>
<td>72 90 117 171</td>
</tr>
</tbody>
</table>

### Table A-8 Safety Produced / Consumed Test Suites

<table>
<thead>
<tr>
<th>Test suite</th>
<th>Std. and Safety P/C Packet rate, pps</th>
<th>IXIA Packet rate, pps</th>
<th># of WGBs</th>
<th>Std. P/C RPI, ms</th>
<th>Safety Task Period, ms</th>
<th>Timeout mult.</th>
<th>P/C CRTL, ms</th>
<th>SRT no fault (calc.)</th>
<th>SRT single fault (calc.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC-8x1-A1</td>
<td>2,400</td>
<td>-</td>
<td>8</td>
<td>10</td>
<td>20</td>
<td>2</td>
<td>80</td>
<td>140</td>
<td>188</td>
</tr>
<tr>
<td>PC-8x1-B1</td>
<td>2,667</td>
<td>-</td>
<td>8</td>
<td>10</td>
<td>15</td>
<td>2</td>
<td>60</td>
<td>125</td>
<td>158</td>
</tr>
<tr>
<td>PC-8x1-X1</td>
<td>2,133</td>
<td>400</td>
<td>8</td>
<td>15</td>
<td>15</td>
<td>2</td>
<td>60</td>
<td>125</td>
<td>158</td>
</tr>
<tr>
<td>PC-8x1-C1</td>
<td>3,067</td>
<td>-</td>
<td>8</td>
<td>8</td>
<td>15</td>
<td>2</td>
<td>60</td>
<td>125</td>
<td>158</td>
</tr>
</tbody>
</table>
Summary of Results

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Minimum Number of Samples / Test Run Time(^1)</th>
<th>Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety I/O System Reaction Time</td>
<td>1,000,000</td>
<td>Table A-9</td>
</tr>
<tr>
<td>Safety I/O Connection Faults</td>
<td>7 days</td>
<td>Table A-9</td>
</tr>
<tr>
<td>Safety P/C System Reaction Time</td>
<td>1,000,000</td>
<td>Table A-10</td>
</tr>
<tr>
<td>Safety P/C Connection Faults</td>
<td>7 days</td>
<td>Table A-10</td>
</tr>
<tr>
<td>Safety I/O Network Latency</td>
<td>6,000,000</td>
<td>Table A-11</td>
</tr>
<tr>
<td>Safety P/C Network Latency</td>
<td>6,000,000</td>
<td>Table A-12</td>
</tr>
<tr>
<td>Network Traffic Statistics</td>
<td>–</td>
<td>Table A-13</td>
</tr>
</tbody>
</table>

\(^1\) Run time was increased to 14 days for selected cases to verify no connection loss

The results include data for the wired baseline (with 8 I/O racks or 8 consumers).

Table A-9 Safety I/O SRT and Faults

<table>
<thead>
<tr>
<th>Test Suite</th>
<th>I/O Packet Rate, pps</th>
<th>CIP Class 3 Rate, pps</th>
<th>Total Packet Rate, pps</th>
<th>Std. I/O RPI, ms</th>
<th>Safety Input RPI, ms</th>
<th>Safety Task Period, ms</th>
<th>Input CRTL, ms</th>
<th>System Reaction Time (Theoretical), ms</th>
<th>System Reaction Time (Observed), ms</th>
<th>Safety I/O Faults</th>
<th>Test Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>IO-8x1-A1</td>
<td>2,933</td>
<td>-</td>
<td>2,933</td>
<td>20</td>
<td>12</td>
<td>20</td>
<td>48</td>
<td>89</td>
<td>125</td>
<td>45</td>
<td>Yes</td>
</tr>
<tr>
<td>IO-8x1-A2</td>
<td>2,933</td>
<td>-</td>
<td>2,933</td>
<td>20</td>
<td>12</td>
<td>20</td>
<td>72</td>
<td>89</td>
<td>165</td>
<td>45</td>
<td>Yes</td>
</tr>
<tr>
<td>IO-8x1-B1</td>
<td>2,222</td>
<td>-</td>
<td>2,222</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>72</td>
<td>117</td>
<td>171</td>
<td>52</td>
<td>No</td>
</tr>
<tr>
<td>IO-8x1-C1</td>
<td>1,822</td>
<td>-</td>
<td>2,222</td>
<td>40</td>
<td>18</td>
<td>30</td>
<td>72</td>
<td>117</td>
<td>171</td>
<td>52</td>
<td>No</td>
</tr>
<tr>
<td>IO-8x1-X1</td>
<td>1,822</td>
<td>400</td>
<td>2,222</td>
<td>40</td>
<td>18</td>
<td>30</td>
<td>72</td>
<td>117</td>
<td>171</td>
<td>53</td>
<td>No</td>
</tr>
<tr>
<td>IO-4x3-A1</td>
<td>3,333</td>
<td>-</td>
<td>3,333</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>72</td>
<td>117</td>
<td>171</td>
<td>54</td>
<td>Yes</td>
</tr>
<tr>
<td>IO-4x3-A2</td>
<td>3,333</td>
<td>-</td>
<td>3,333</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>72</td>
<td>117</td>
<td>171</td>
<td>54</td>
<td>Yes</td>
</tr>
<tr>
<td>IO-4x3-B1</td>
<td>2,800</td>
<td>-</td>
<td>2,800</td>
<td>20</td>
<td>24</td>
<td>40</td>
<td>96</td>
<td>117</td>
<td>171</td>
<td>54</td>
<td>Yes</td>
</tr>
<tr>
<td>IO-4x2-A1</td>
<td>2,222</td>
<td>-</td>
<td>2,222</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>72</td>
<td>117</td>
<td>171</td>
<td>53</td>
<td>No</td>
</tr>
<tr>
<td>IO-4x2-X1</td>
<td>2,222</td>
<td>400</td>
<td>2,622</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>72</td>
<td>117</td>
<td>171</td>
<td>53</td>
<td>No</td>
</tr>
<tr>
<td>IO-8-wired</td>
<td>2,222</td>
<td>-</td>
<td>2,222</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>72</td>
<td>117</td>
<td>171</td>
<td>51</td>
<td>No</td>
</tr>
</tbody>
</table>
### Table A-10 Safety Produced / Consumed SRT and Faults

<table>
<thead>
<tr>
<th>Test Suite</th>
<th>I/O Packet Rate, pps</th>
<th>CIP Class 3 Rate, pps</th>
<th>Std. P/C Rate, RPI, ms</th>
<th>Safety P/C Rate, RPI, ms</th>
<th>P/C CRTL, ms</th>
<th>System Reaction Time (Theoretical), ms</th>
<th>System Reaction Time (Observed), ms</th>
<th>Safety I/O Faults</th>
<th>Test Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC-8x1-A1</td>
<td>2,400</td>
<td>-</td>
<td>10</td>
<td>20</td>
<td>80</td>
<td>140</td>
<td>188</td>
<td>66</td>
<td>No Pass</td>
</tr>
<tr>
<td>PC-8x1-B1</td>
<td>2,667</td>
<td>-</td>
<td>10</td>
<td>15</td>
<td>60</td>
<td>125</td>
<td>158</td>
<td>58</td>
<td>No Pass</td>
</tr>
<tr>
<td>PC-8x1-X1</td>
<td>2,133</td>
<td>400</td>
<td>15</td>
<td>15</td>
<td>60</td>
<td>125</td>
<td>158</td>
<td>58</td>
<td>No Pass</td>
</tr>
<tr>
<td>PC-8x1-C1</td>
<td>3,067</td>
<td>-</td>
<td>8</td>
<td>15</td>
<td>60</td>
<td>125</td>
<td>158</td>
<td>58</td>
<td>Yes Fail</td>
</tr>
<tr>
<td>PC-8-wired</td>
<td>2,667</td>
<td>-</td>
<td>10</td>
<td>15</td>
<td>60</td>
<td>125</td>
<td>158</td>
<td>56</td>
<td>No n/a</td>
</tr>
</tbody>
</table>

1 Largest between measurements in downstream and upstream direction

### Table A-11 Safety I/O Latency

<table>
<thead>
<tr>
<th>Test Suite</th>
<th>I/O Packet Rate, pps</th>
<th>CIP Class 3 Rate, pps</th>
<th>Total Packet Rate, RPI, ms</th>
<th>Safety Input RPI, ms</th>
<th>Safety Task Period, ms</th>
<th>Input CRTL, ms</th>
<th>Measured Network Latency AP to WGB / WGB to AP, ms</th>
<th>Max. Safety I/O Round Trip Delay, ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>IO-8x1-A1</td>
<td>2,933</td>
<td>-</td>
<td>2,933</td>
<td>20</td>
<td>12</td>
<td>20</td>
<td>48</td>
<td>0.8 / 15</td>
</tr>
<tr>
<td>IO-8x1-A2</td>
<td>2,933</td>
<td>-</td>
<td>2,933</td>
<td>20</td>
<td>12</td>
<td>20</td>
<td>72</td>
<td>0.7 / 12</td>
</tr>
<tr>
<td>IO-8x1-B1</td>
<td>2,222</td>
<td>-</td>
<td>2,222</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>72</td>
<td>0.7 / 10</td>
</tr>
<tr>
<td>IO-8x1-C1</td>
<td>1,822</td>
<td>400</td>
<td>2,222</td>
<td>40</td>
<td>18</td>
<td>30</td>
<td>72</td>
<td>0.7 / 12</td>
</tr>
<tr>
<td>IO-8x1-X1</td>
<td>1,822</td>
<td>400</td>
<td>2,222</td>
<td>40</td>
<td>18</td>
<td>30</td>
<td>72</td>
<td>0.7 / 12</td>
</tr>
<tr>
<td>IO-4x3-A1</td>
<td>3,333</td>
<td>-</td>
<td>3,333</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>72</td>
<td>0.8 / 24</td>
</tr>
<tr>
<td>IO-4x3-A2</td>
<td>3,333</td>
<td>-</td>
<td>3,333</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>72</td>
<td>0.8 / 24</td>
</tr>
<tr>
<td>IO-4x3-B1</td>
<td>2,800</td>
<td>-</td>
<td>2,800</td>
<td>20</td>
<td>24</td>
<td>40</td>
<td>96</td>
<td>0.8 / 18</td>
</tr>
<tr>
<td>IO-4x2-A1</td>
<td>2,222</td>
<td>-</td>
<td>2,222</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>72</td>
<td>0.7 / 13</td>
</tr>
<tr>
<td>IO-4x2-B1</td>
<td>2,222</td>
<td>400</td>
<td>2,622</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>72</td>
<td>0.8 / 15</td>
</tr>
<tr>
<td>IO-8-wired</td>
<td>2,222</td>
<td>-</td>
<td>2,222</td>
<td>20</td>
<td>18</td>
<td>30</td>
<td>72</td>
<td>0.3</td>
</tr>
</tbody>
</table>

1 As reported by Safety I/O modules in GuardLogix

### Table A-12 Safety Produced / Consumed Latency

<table>
<thead>
<tr>
<th>Test Suite</th>
<th>P/C Packet Rate, pps</th>
<th>CIP Class 3 Rate, pps</th>
<th>Std. P/C Rate, RPI, ms</th>
<th>Safety P/C Rate, RPI, ms</th>
<th>P/C CRTL, ms</th>
<th>Measured Network Latency AP to WGB / WGB to AP, ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC-8x1-A1</td>
<td>2,400</td>
<td>-</td>
<td>10</td>
<td>20</td>
<td>80</td>
<td>0.7 / 15</td>
</tr>
<tr>
<td>PC-8x1-B1</td>
<td>2,667</td>
<td>-</td>
<td>10</td>
<td>15</td>
<td>60</td>
<td>0.7 / 16</td>
</tr>
<tr>
<td>PC-8x1-X1</td>
<td>2,133</td>
<td>400</td>
<td>15</td>
<td>15</td>
<td>60</td>
<td>0.7 / 15</td>
</tr>
<tr>
<td>PC-8x1-C1</td>
<td>3,067</td>
<td>-</td>
<td>8</td>
<td>15</td>
<td>60</td>
<td>0.7 / 19</td>
</tr>
<tr>
<td>PC-8-wired</td>
<td>2,667</td>
<td>-</td>
<td>10</td>
<td>15</td>
<td>60</td>
<td>0.3</td>
</tr>
</tbody>
</table>

1 As reported by Safety I/O modules in GuardLogix
### Table A-13 Network Traffic Statistics

<table>
<thead>
<tr>
<th>Test Suite</th>
<th>I/O or P/C Packet rate, pps</th>
<th>CIP Class 3 Rate, pps</th>
<th>Safety Input RPI</th>
<th>Safety Output RPI, ms</th>
<th>Std I/O or P/C RPI</th>
<th>Avg. Rate, pps(^1)</th>
<th>Avg. Rate, Mbps(^1)</th>
<th>Avg. Packet Size, bytes</th>
<th>AP Packet Retries</th>
<th>WGB Packets Retries</th>
<th>AP CRC Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>IO-8x1-A1</td>
<td>2.933</td>
<td>-</td>
<td>12</td>
<td>20</td>
<td>-</td>
<td>20</td>
<td>3.095</td>
<td>1.84</td>
<td>75</td>
<td>0.6%</td>
<td>3.3%</td>
</tr>
<tr>
<td>IO-8x1-B1</td>
<td>2.222</td>
<td>-</td>
<td>18</td>
<td>30</td>
<td>-</td>
<td>20</td>
<td>2.375</td>
<td>1.48</td>
<td>78</td>
<td>0.6%</td>
<td>2.7%</td>
</tr>
<tr>
<td>IO-8x1-C1</td>
<td>1.822</td>
<td>-</td>
<td>18</td>
<td>30</td>
<td>-</td>
<td>40</td>
<td>1.977</td>
<td>1.24</td>
<td>78</td>
<td>0.3%</td>
<td>1.9%</td>
</tr>
<tr>
<td>IO-8x1-X1</td>
<td>1.822</td>
<td>400</td>
<td>18</td>
<td>30</td>
<td>-</td>
<td>40</td>
<td>2.376</td>
<td>2.00</td>
<td>105</td>
<td>0.6%</td>
<td>2.2%</td>
</tr>
<tr>
<td>IO-4x3-A1</td>
<td>3.333</td>
<td>-</td>
<td>18</td>
<td>30</td>
<td>-</td>
<td>20</td>
<td>3.518</td>
<td>2.16</td>
<td>77</td>
<td>0.8%</td>
<td>3.4%</td>
</tr>
<tr>
<td>IO-4x3-B1</td>
<td>2.800</td>
<td>-</td>
<td>24</td>
<td>40</td>
<td>-</td>
<td>20</td>
<td>3.002</td>
<td>1.91</td>
<td>77</td>
<td>0.7%</td>
<td>2.8%</td>
</tr>
<tr>
<td>IO-4x2-A1</td>
<td>2.200</td>
<td>-</td>
<td>18</td>
<td>30</td>
<td>-</td>
<td>20</td>
<td>2.377</td>
<td>1.48</td>
<td>78</td>
<td>0.6%</td>
<td>2.2%</td>
</tr>
<tr>
<td>IO-4x2-X1</td>
<td>2.200</td>
<td>400</td>
<td>18</td>
<td>30</td>
<td>-</td>
<td>20</td>
<td>2.776</td>
<td>2.23</td>
<td>101</td>
<td>0.8%</td>
<td>2.4%</td>
</tr>
<tr>
<td>PC-8x1-A1</td>
<td>2.400</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>15</td>
<td>10</td>
<td>2.660</td>
<td>6.36</td>
<td>299</td>
<td>1.0%</td>
<td>2.8%</td>
</tr>
<tr>
<td>PC-8x1-B1</td>
<td>2.667</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>15</td>
<td>10</td>
<td>2.929</td>
<td>7.03</td>
<td>300</td>
<td>0.9%</td>
<td>3.0%</td>
</tr>
<tr>
<td>PC-8x1-X1</td>
<td>2.133</td>
<td>400</td>
<td>-</td>
<td>-</td>
<td>15</td>
<td>15</td>
<td>2.723</td>
<td>6.38</td>
<td>293</td>
<td>0.8%</td>
<td>2.7%</td>
</tr>
<tr>
<td>PC-8x1-C1</td>
<td>3.067</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>15</td>
<td>8</td>
<td>3.326</td>
<td>8.04</td>
<td>302</td>
<td>11%</td>
<td>4.4%</td>
</tr>
</tbody>
</table>

\(^1\) Including CIP Class 3, network control and test traffic
WLAN Reference Information

RF Power Values
Radio transmitter power is measured in milliwatts (mW) or more commonly in logarithmic form using decibels as compared to 1 mW (dBm):

- Power [dBm] = 10 * log10 (Power [mW])

When comparing power levels, these general rules can be used:

<table>
<thead>
<tr>
<th>Increase or decrease in dB</th>
<th>Transmit power changes by the factor of</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 dB</td>
<td>2</td>
</tr>
<tr>
<td>10 dB</td>
<td>10</td>
</tr>
<tr>
<td>20 dB</td>
<td>100</td>
</tr>
</tbody>
</table>

Some of the approximate dBm to mW values are shown below:

<table>
<thead>
<tr>
<th>dBm</th>
<th>mW</th>
<th>dBm</th>
<th>mW</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>14</td>
<td>25</td>
</tr>
<tr>
<td>2</td>
<td>156</td>
<td>17</td>
<td>50</td>
</tr>
<tr>
<td>5</td>
<td>313</td>
<td>20</td>
<td>100</td>
</tr>
<tr>
<td>8</td>
<td>625</td>
<td>23</td>
<td>200</td>
</tr>
<tr>
<td>11</td>
<td>125</td>
<td>30</td>
<td>1000</td>
</tr>
</tbody>
</table>

Power gain rating of antennas is measured in dBi which is the ratio of power compared to the theoretical isotropic antenna that transmit equal power density in all directions. Real world antennas distribute more power in some directions than the others. The rating of an antenna in dBi is the gain in the direction of the maximum radiation (see Antenna Characteristics).

The maximum energy coming from a radio system is measured as Effective Isotropic Radiated Power (EIRP), which is a sum of the dB values of the various components:

- EIRP [dBm] = Transmitter Power [dBm] – Cable Loss [dB] + Antenna Gain [dBi]

EIRP is the value that regulatory agencies, such as the FCC or ETSI, use to determine and measure power limits.
Receiver Sensitivity

Receiver sensitivity is the minimum received power level (in dBm or mW) that is necessary for the receiver to accurately decode a signal. Receiver sensitivity has negative dBm values (i.e. it is a fraction of 1 mW).

Receiver sensitivity depends on the AP model and radio type, frequency band, and data rate. Packets that are transmitted at the lower data rate can be decoded at the lower power level and therefore at the greater distance. As an example, some of the values for the Cisco 2600 series AP are shown below.

Table B-1 Receiver sensitivity (Cisco 2600 AP)

<table>
<thead>
<tr>
<th>Radio Type / Band</th>
<th>Receiver Sensitivity / Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a 5 GHz</td>
<td>-92 dBm / 6 Mbps</td>
</tr>
<tr>
<td></td>
<td>-89 dBm / 24 Mbps</td>
</tr>
<tr>
<td></td>
<td>-79 dBm / 54 Mbps</td>
</tr>
<tr>
<td>802.11n 5 GHz</td>
<td>-92 dBm / 6.5 Mbps</td>
</tr>
<tr>
<td>20 MHz channels</td>
<td>-75 dBm / 65 Mbps</td>
</tr>
<tr>
<td></td>
<td>-74 dBm / 130 Mbps</td>
</tr>
<tr>
<td></td>
<td>-73 dBm / 195 Mbps</td>
</tr>
</tbody>
</table>

RF Signal Propagation

Several factors impact the ability of the radio wave to carry data to the destination, such as attenuation, noise, reflection and multipath propagation, and interference.

Attenuation

As a radio signal propagates through the air, it experiences a decrease in amplitude referred to as attenuation. For example, a power level at the transmitter antenna might be 20 dBm (100 mW) while the receiver might get the signal at -60 dBm (0.000001 mW), the \(10^8\) (100,000,000) times decrease.

Most attenuation results from the Free Space Loss which is the exponential decrease of the amplitude as the signal propagates farther away from the antenna. For example, if you double the distance, the amplitude of the radio wave at that location will be one-quarter of its initial value.

- The rule of thumb for the free space loss:
  - Double distance = -6 dB
  - Triple distance = -10 dB

The attenuation also increases with higher frequencies, thus 5 GHz signal propagates less in the open space than 2.4 GHz. As an example, free space loss at 100 meters would be 86 dB for 5 GHz and 80 dB for 2.4 GHz (the 6 dB difference means \(x^4\) change in the amplitude).

In addition to the free space loss, different construction materials, machinery, liquids, atmospheric conditions, etc., absorb the RF signal causing attenuation. For example, the signal loss can be in the range of 3-5 dB for drywalls and 10-30 dB for brick or concrete walls. In practice, only the actual site survey results can give an accurate picture of the RF signal propagation in the particular location.
Reflection and Multipath

In addition to absorption, the signal can be reflected off the obstacles, particularly from metal surfaces. Some radio waves take different paths when propagating from source to destination which is called multipath propagation. Some of the signal will arrive with delay to the receiver which can negatively impact the transmission. Several features of the 802.11n technology are designed to reduce or even take advantage of the multipath effects (see 4.1.2).

Diffusion and diffraction of waves around objects also change signal characteristics. These effects relate to the wavelength of the radio (6-12 cm for Wi-Fi networks). Shifts by a portion of this distance may already cause changes in reception.

RSSI and Signal-to-Noise Ratio

The receiver’s ability to decode the signal is impacted by the presence of interfering radio signals or noise. The communication can be improved by either moving the antennas closer together, increasing the transmit power, or reducing the surrounding noise.

An average noise of –95 dBm (referred to as noise floor) always exists in the atmosphere. In addition to that, other frequency emitting devices and neighboring wireless networks may increase the average noise level to –90 dBm and even higher. An important WLAN characteristic is the signal-to-noise (SNR) ratio, expressed in dB, which is the received signal power (in dBm) minus the noise power (in dBm) at the particular point.

Figure B-1 Signal to Noise Ratio Example

The signal power is usually indicated by Received Signal Strength Indicator (RSSI) parameter reported by the AP.

Even if the signal level is above the receiver sensitivity, the SNR must be high enough to be able to distinguish the signal from the noise. Higher data rates, especially high throughput 802.11n rates, require higher SNR.

• For 802.11n networks in the industrial environments, the minimum SNR at the receiver should be at least 25 dB to provide a safety margin and minimize retransmissions.
Legacy 802.11a/g Rates

The IEEE 802.11a/g standards use orthogonal frequency-division multiplexing (OFDM) with different modulation techniques to deliver 6 to 54 Mbps speeds using only a single transmitter (spatial stream).

Table B-2 802.11a/g Data Rates

<table>
<thead>
<tr>
<th>Data Rate, Mbps</th>
<th>Modulation and Coding Rate</th>
<th>Data Rate, Mbps</th>
<th>Modulation and Coding Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>BPSK 1/2</td>
<td>24</td>
<td>16-QAM 1/2</td>
</tr>
<tr>
<td>9</td>
<td>BPSK 3/4</td>
<td>36</td>
<td>16-QAM 3/4</td>
</tr>
<tr>
<td>12</td>
<td>QPSK 1/2</td>
<td>48</td>
<td>64-QAM 2/3</td>
</tr>
<tr>
<td>18</td>
<td>QPSK 3/4</td>
<td>54</td>
<td>64-QAM 3/4</td>
</tr>
</tbody>
</table>

802.11n Data Rates

The 802.11n standard improves OFDM modulation with increased efficiency and encoding rate. These changes increase the data rate to a maximum of 65 Mbps for a single spatial stream (using 20 MHz channels and long guard interval). Multiple data streams using Spatial Division Multiplexing increase the maximum data rate accordingly.

The number of spatial streams, modulation type, and coding rate define the Modulation Coding Scheme (MCS) index for each 802.11n data rate. The available MCS rates are shown below.

Table B-3 802.11a/g Data Rates¹

<table>
<thead>
<tr>
<th>MCS Index</th>
<th>Spatial Streams</th>
<th>Data Rate, Mbps</th>
<th>MCS Index</th>
<th>Spatial Streams</th>
<th>Data Rate, Mbps</th>
<th>MCS Index</th>
<th>Spatial Streams</th>
<th>Data Rate, Mbps</th>
<th>MCS Index</th>
<th>Spatial Streams</th>
<th>Data Rate, Mbps</th>
<th>Modulation and Coding Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>6.5</td>
<td>8</td>
<td>2</td>
<td>13</td>
<td>16</td>
<td>3</td>
<td>24</td>
<td>4</td>
<td>26</td>
<td>BPSK 1/2</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>13</td>
<td>9</td>
<td>2</td>
<td>26</td>
<td>17</td>
<td>3</td>
<td>25</td>
<td>4</td>
<td>52</td>
<td>QPSK 1/2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>19.5</td>
<td>10</td>
<td>2</td>
<td>39</td>
<td>18</td>
<td>3</td>
<td>26</td>
<td>4</td>
<td>78</td>
<td>QPSK 3/4</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>26</td>
<td>11</td>
<td>2</td>
<td>52</td>
<td>19</td>
<td>3</td>
<td>27</td>
<td>4</td>
<td>104</td>
<td>16-QAM 1/2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>39</td>
<td>12</td>
<td>2</td>
<td>78</td>
<td>20</td>
<td>3</td>
<td>28</td>
<td>4</td>
<td>156</td>
<td>16-QAM 3/4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>52</td>
<td>13</td>
<td>2</td>
<td>104</td>
<td>21</td>
<td>3</td>
<td>29</td>
<td>4</td>
<td>208</td>
<td>64-QAM 2/3</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>58.5</td>
<td>14</td>
<td>2</td>
<td>117</td>
<td>22</td>
<td>3</td>
<td>30</td>
<td>4</td>
<td>234</td>
<td>64-QAM 3/4</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>65</td>
<td>15</td>
<td>2</td>
<td>130</td>
<td>23</td>
<td>3</td>
<td>31</td>
<td>4</td>
<td>260</td>
<td>64-QAM 5/6</td>
<td></td>
</tr>
</tbody>
</table>

¹ 20 MHz channel, 800 ns guard interval
Antenna characteristics

Two fundamental properties of a wireless antenna are power gain and radiation pattern.

The antenna gain is the ratio of the power increase relative to a reference antenna. The gain is compared to an ideal isotropic antenna that radiates energy equally in all directions. A real physical antenna is able to transmit and receive more energy in a certain direction, and less in the other.

Antenna gain is expressed in logarithmic units (dBi) and assumed to be the gain in the direction of the maximum radiation. For example, the gain of 4 dBi means 2.5 times increase in radiated power. It is important to understand that an antenna with gain does not create more power but only changes the way the power is distributed in three-dimensional space. A useful analogy is the reflector in a flashlight that intensifies the light beam in a particular direction.

The radiation pattern shows the radiation properties of the antenna in space. The actual pattern is three-dimensional since any antenna radiates or receives energy in all directions. Commonly this pattern is described with two two-dimensional patterns called the principal plane patterns:

- Azimuth plane or “horizontal” pattern measured in the X-Y plane (see the picture below)
- Elevation plane or “vertical” pattern measured in the Y-Z plane

Here the terms “horizontal” and “vertical” assume that the antenna is mounted in the correct orientation for its use. The patterns are usually normalized to the maximum gain of the antenna which is subtracted from the measured values. In this case, the 0 dB line on a plot corresponds to the peak gain.

Radiation patterns provided by vendors are “best case” lab patterns. They do not take into account environmental factors, for example when an antenna is placed near metal objects.
Antennas are also selected based on the following:

- Frequency band: 2.4 GHz only, 5 GHz only, or dual-band
- Single-element antennas (one per antenna port of the AP), or MIMO antennas with multiple elements in a single enclosure
- Type of mounting (ceiling, wall, mast)
- Area of use (indoor or outdoor)

Antenna Types

Omnidirectional Antennas

Omnidirectional antennas radiate energy equally in all directions in the azimuth plane (toward the horizon if oriented vertically). The elevation plane pattern shows maximum energy radiating out into the intended coverage area, with minimum energy directly under the antenna.

The basic low-gain omnidirectional antenna is a dipole (see an example below) that is attached directly to the port on the AP. This is a default AP antenna that may be used for installations where there are no metal enclosures or obstacles around the AP. The gain of dipole antennas in 5 GHz band is 4 dBi which should be sufficient for most indoor applications.

- A dipole antenna should be vertically oriented towards the floor or ground. For correct operation, all antennas on the AP and WGBs should be oriented in the same way. If an AP has to be installed on a vertical surface, special mounting brackets should be used to provide orientation.
- Dipole (and other low-gain omnidirectional antennas) may not provide adequate coverage when installed high above the ground. Site survey is necessary to determine the appropriate antenna type.
When dipole antennas are not appropriate, other types of omnidirectional antennas are used:

- MIMO omnidirectional antennas have several radiating elements in a single enclosure, and are connected to multiple antenna ports. The gain and radiating patterns are similar to the dipole antennas. They have a variety of mounting options (ceiling, pole, wall etc.). As with all types of antennas, correct orientation is critical to provide intended coverage and MIMO operation.

- High-gain omnidirectional antennas are typically used outdoors for large area point-to-multipoint connections. They are attached directly to the AP or mounted on a mast. The indoor use in industrial environments is limited:
  - Higher gain creates undesirable signal propagation in all directions and makes channel reuse very difficult.
  - Zones with poor signal ("nulls") can be created directly underneath and behind the antenna due to high gain radiation patterns.
**Directional Antennas**

Directional antennas radiate their energy out in a particular direction. They are used to cover difficult areas (aisles, corridors, high ceilings) as well as for point-to-point links. Directional antennas may be useful to limit the signal propagation beyond the intended area. Some of the common types and their patterns are shown below.

![Directional Antenna Examples](image)

**CleanAir**

CleanAir is a Cisco technology that addresses the problem of radio interference in Unified WLAN architecture. CleanAir-enabled APs are enhanced with a proprietary hardware chipset that operates in parallel with normal communication, making spectrum analysis of non-Wi-Fi energy. The CleanAir hardware does not impede wireless performance and has no effect on the Wi-Fi client traffic.

The information obtained from APs is used to identify and locate a potential interference source, and to avoid the interference to maintain an adequate service level. Parts of the CleanAir operation are:

- The APs identify potential interference sources in the wireless channel, and forward the information to the controller. Non-Wi-Fi sources are classified (i.e. microwave, cordless phone, Bluetooth etc.) based on known signatures.
- Regular lightweight APs (Local mode) provide reports only for the operating channel while continuing to serve clients. Monitor mode lightweight APs (listen only) provide reports for all monitored channels.
- The controller collects and process spectrum data, and displays interference reports. The channel reports take into account not just non-Wi-Fi energy, but also the amount of adjacent and co-channel interference from neighboring APs.
- If the interference is above configured threshold, RRM is used to select a new channel using DCA (see 4.1.8). In the event of significant interference, the channel can be switched immediately.

While Cisco CleanAir technology helps to detect and avoid interference, there are considerations and limitations of its use with industrial applications:

- CleanAir feature is available only for Cisco lightweight access points. Autonomous APs currently do not support CleanAir since most of the benefits can only be realized in the Unified architecture.
- It was verified that CleanAir does not itself interfere with the industrial applications There is no difference in performance when deploying CleanAir APs in Local mode.
- Most IACS applications in Unified architecture require RRM to be turned off (see 4.1.8). In this case, CleanAir functionality is limited.
• CleanAir APs can be used in Monitor mode overlaying non-CleanAir AP infrastructure. APs in monitor mode do not pass user data traffic and do not participate in RRM. Correlating interference device detections from multiple access points is limited.

• Monitor mode APs provide reports for all configured channels. They can also be used for other functionality, such as rogue detection and mitigation, and wireless intrusion prevention system (WIPS). They also can be temporarily assigned the normal role (Local mode) if a primary AP fails.

Recommendations for Unified Architecture:

• If RRM features can be turned on, CleanAir access points can be used in Local mode. Do not mix CleanAir and non-CleanAir APs in the same coverage area.

• If an application requires RRM to be turned off (majority of use cases), and monitoring for wireless interference is necessary, use CleanAir access points in Monitor mode as an overlay deployment. Use non-CleanAir access points for user traffic. The typical ratio of Monitor to Local APs recommended by Cisco is no more than 1:5.

Recommendations for Autonomous Architecture:

• For plant-wide proactive monitoring, use separate Unified infrastructure with CleanAir APs in Monitor mode. For on-demand monitoring in a single location, use stand-alone spectrum analysis products such as Cisco Spectrum Expert.

WLAN Diagnostics

This section describes some of the important metrics and diagnostic information that can be used to monitor and troubleshoot a WLAN. There are several methods to obtain the information from an AP or WGB:

• Web interface diagnostics (radio interface status and statistics, association data, log messages)

• Command Line Interface (CLI) using “show” and “debug” command output

• SNMP (Simple Network Management Protocol) diagnostics using an SNMP server software

• System logging using a Syslog server software

In the Cisco Unified architecture, WLAN monitoring and diagnostic information is consolidated in the WLCs or NCS Prime software.

Radio Interface Information

Table B4 lists the important radio interface data that should be used for monitoring and diagnostics. It is critical to determine a baseline for the normal WLAN operation in production environment. During troubleshooting, the parameters can be compared to the baseline values.

For example, some level of CRC errors and packet retries is expected in any WLAN. However, sudden increases or fluctuations of these numbers may indicate unexpected traffic or interference in the channel.
<table>
<thead>
<tr>
<th>Category</th>
<th>Parameter</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio Status –</td>
<td><strong>Hardware Status (up/down)</strong></td>
<td></td>
</tr>
<tr>
<td>Configuration</td>
<td><strong>Software Status (enabled/disabled)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Operational Rates</strong></td>
<td>All allowed rates</td>
</tr>
<tr>
<td></td>
<td><strong>Basic Rates</strong></td>
<td>All basic rates should be supported on a client or WGB (4.1.4)</td>
</tr>
<tr>
<td></td>
<td><strong>Active Radio Channel</strong></td>
<td>If using DFS channels in the 5 GHz band, changes in the active channel may indicate a DFS event due to radar interference (4.1.1.6)</td>
</tr>
<tr>
<td></td>
<td><strong>Channel Width</strong></td>
<td>20 MHz should be selected for IACS applications (4.1.2.4)</td>
</tr>
<tr>
<td></td>
<td><strong>Transmitter Power (dBm)</strong></td>
<td>Normally (Tx power + antenna gain) should match between an AP and a WGB</td>
</tr>
<tr>
<td></td>
<td><strong>Antenna Gain</strong></td>
<td>Antenna gain should be configured manually based on the specifications</td>
</tr>
<tr>
<td></td>
<td><strong>Role in Network (Root AP / WGB)</strong></td>
<td></td>
</tr>
<tr>
<td>Radio Status –</td>
<td><strong>Input Rate (bps, pps)</strong></td>
<td>Compare to baseline and known application load to detect unexpected traffic through the AP/WGB</td>
</tr>
<tr>
<td>Statistics</td>
<td><strong>Output Rate (bps, pps)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Input Errors</strong></td>
<td>Normally should be no input errors (not the same as CRC errors)</td>
</tr>
<tr>
<td></td>
<td><strong>Output Errors</strong></td>
<td>Changes from baseline show excessive retries and packet drop</td>
</tr>
<tr>
<td>Radio Detailed</td>
<td><strong>Kbytes Sent</strong></td>
<td>Compare to baseline – check for unexpected multicast traffic</td>
</tr>
<tr>
<td>Status –</td>
<td><strong>Unicast Packets Sent</strong></td>
<td></td>
</tr>
<tr>
<td>Transmit Statistics</td>
<td><strong>Multicast Packets Sent</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Broadcast Packets Sent by Host</strong></td>
<td>Compare to baseline; most broadcast from the AP should be beacons (100ms default period)</td>
</tr>
<tr>
<td></td>
<td><strong>Beacons Packets Sent</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>RTS Transmitted</strong></td>
<td>Normally RTS/CTS is disabled and should not be seen</td>
</tr>
<tr>
<td></td>
<td><strong>CTS Not Received</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Retries</strong></td>
<td>Retries need to be compared to the baseline for the application. Normally should be less than 5% of transmitted packets. High levels indicate channel congestion or RF issues.</td>
</tr>
<tr>
<td></td>
<td><strong>Packets with One Retry</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Packets with &gt;1 Retry</strong></td>
<td></td>
</tr>
<tr>
<td>Radio Detailed</td>
<td><strong>Kbytes Received</strong></td>
<td>Compare to baseline – check for unexpected multicast, broadcast, and beacon traffic</td>
</tr>
<tr>
<td>Status –</td>
<td><strong>Unicast Packets Received</strong></td>
<td></td>
</tr>
<tr>
<td>Receive Statistics</td>
<td><strong>Multicast Packets Received</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Broadcast Packets Received</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Broadcast Packets to Host</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Beacon Packets Received</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>CRC Errors</strong></td>
<td>CRC errors need to be compared to the baseline for the application. Normally should be less than 10% of received packets. High levels indicate channel congestion or RF issues.</td>
</tr>
<tr>
<td>Radio Detailed</td>
<td><strong>Rx Packets / Bytes per each data rate used</strong></td>
<td>All beacons are transmitted at the lowest basic rate. Majority of the data packets should be transmitted and received at the highest enabled rate. Excessive packet counts at other rates indicate poor RF conditions and high level of retries.</td>
</tr>
<tr>
<td>Status –</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rate Statistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Total and Last 5 sec)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Radio Association Parameters

Table B-5 shows useful information about devices associated to the AP. Main parameters that need to be monitored for each client are the data rate, signal strength, and signal to noise values. In IACS applications with fixed number of clients, any unexpected association entries should be noted.

Table B-5 Radio Association Parameters

<table>
<thead>
<tr>
<th>Category</th>
<th>Parameter</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP/WGB Information and Status (Device Types: AP-parent or WGB)</td>
<td>IP Address</td>
<td>Management IP address and radio MAC address</td>
</tr>
<tr>
<td></td>
<td>MAC Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSID</td>
<td>Security settings</td>
</tr>
<tr>
<td></td>
<td>Key Mgmt / Encryption</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Current Rate (Mbps)</td>
<td>Should be highest enabled rate in normal RF conditions</td>
</tr>
<tr>
<td></td>
<td>Signal Strength (dBm)</td>
<td>Compare to baseline; at least -67 dBm is recommended for IACS traffic</td>
</tr>
<tr>
<td></td>
<td>Signal to Noise (dB)</td>
<td>Compare to baseline; at least 25 dB is recommended for IACS traffic</td>
</tr>
<tr>
<td></td>
<td>Connected For (sec)</td>
<td>Check for recent disassociation events</td>
</tr>
<tr>
<td>AP/WGB Receive/Transmit Statistics</td>
<td>Input and Output Rate</td>
<td>Compare to baseline and other clients, for example if</td>
</tr>
<tr>
<td></td>
<td>Data Retries</td>
<td>equal packet rate is expected for each WGB</td>
</tr>
<tr>
<td>Wired Client Information (Device Type: WGB-client)</td>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MAC Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Parent MAC Address</td>
<td></td>
</tr>
</tbody>
</table>

System Logging and Debug Information

System log messages and debug messages can provide valuable information for in-depth troubleshooting of the system. Some considerations for their use are provided here:

• Logging to local buffer and to the syslog server can be used. Sufficient buffer size should be used to avoid overwriting of messages.

• Timestamps with millisecond accuracy should be enabled for analysis and correlation of events. NTP (Network Time Protocol) infrastructure is needed to keep the common clock between devices. In absence of NTP, system uptime format can be used as local reference.

• Severity level “Notification” is recommended for normal syslog operation. More detailed levels can be enabled on demand.

• Enabling debug commands on the AP/WGB can severely impact performance and disrupt the data traffic. In some cases, rebooting the AP is required. Debugging level should only be used by tech support during troubleshooting, and not to be left on during the normal operation.

• Detailed information for technical support can be obtained via web interface or CLI as a text file. It is recommended to keep a baseline copy of this information for each device.

This chapter summarizes recommendations found in chapters 1-4 of this guide. More detailed technical information and context for these recommendations can be found in specific sections referenced below.
To learn more about how Cisco and Rockwell Automation can help you, please visit:
[www.rockwellautomation.com/partners/cisco.html](http://www.rockwellautomation.com/partners/cisco.html)

Cisco is the worldwide leader in networking that transforms how people connect, communicate and collaborate. Information about Cisco can be found at [www.cisco.com](http://www.cisco.com).
For ongoing news, please go to [http://newsroom.cisco.com](http://newsroom.cisco.com). Cisco equipment in Europe is supplied by Cisco Systems International BV, a wholly owned subsidiary of Cisco Systems, Inc.

[www.cisco.com](http://www.cisco.com)

**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Europe Headquarters**
Cisco Systems International BV
Amsterdam, The Netherlands

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](http://www.cisco.com/go/offices).

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration: Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, QuickStudy, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2014 Cisco Systems, Inc. and Rockwell Automation, Inc. All rights reserved.