CHAPTER 2

System Design Considerations

This chapter describes system design considerations for implementing a WLAN for industrial applications.

Technology Overview

This section includes considerations for choosing the right wireless technology and architecture.

Choosing the Right Wireless Technology

The first step in selecting the proper wireless technology should be assessing application and hardware requirements. A variety of wireless standards have been established in the industrial space with different characteristics and applications (see Table 2-1).

The CPwE WLAN guide is based upon established IEEE 802.11 standards that provide the following benefits for critical high-performance IACS applications:

- Widely adopted standard-based technology
- Direct transmission of Ethernet-based industrial protocols such as EtherNet/IP
- Convergence with 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
Chapter 2  System Design Considerations

Technology Overview

Choosing the Right Wireless Architecture

A wide variety of IACS applications can use wireless communication to allow equipment mobility and to replace wired Ethernet. These applications, which have different characteristics, may require different approaches to WLAN design and implementation.

When selecting the wireless architecture for an IACS application, the following factors should be considered:

- Scale of the wireless deployment (number of access points and clients: coverage area)
- Mobility requirements (plant-wide roaming, fast roaming)
- Security requirements (client authentication)
- IACS protocols to be used in the WLAN
- Existing wireless infrastructure that can be reused
- Type and capabilities of the wireless clients

Wireless Client Types

A client device can be connected to a WLAN in several ways, which are described in this section.

Integrated Wireless Adapter

Conventional wireless clients such as laptops, phones or tablets use integrated wireless adapters and antennas. However, providing an integrated wireless module for each IACS device such as a PAC or I/O chassis is not feasible for the majority of applications. Some of the limiting factors are lack of antenna options, poor RF characteristics, placement restrictions and a potentially excessive number and density of wireless nodes. Additional factors to consider are extra cost and issues associated with migration to other IACS platforms.

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

An external wireless adapter (or bridge) for each individual PAC or I/O device can solve some of the issues associated with using integrated wireless 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 terminology. It is not considered in this guide because of the single MAC address limitations and lack of other features.

Workgroup Bridge (WGB)

The ability to connect several wired clients with a single wireless bridge solves many of the previously mentioned problems. This capability is implemented in a workgroup bridge (WGB) mode, which is a type of operation supported by Stratix™ 5100 and Cisco autonomous APs.

A WGB operates in the WLAN as a single wireless client of an access point (root AP). The WGB learns MAC addresses of its wired clients on the Ethernet interface and reports them to the root AP. Multiple wired devices can be connected to the WGB using an Ethernet switch, or in linear topology, with embedded switch technology.

Note

This guide is focused on using WGBs as the main method of connecting IACS devices to a WLAN.

An example of a topology using different types of wireless clients is shown in Figure 2-1.

Figure 2-1   Wireless Client Types

Autonomous WLAN Overview

The Autonomous WLAN architecture consists of stand-alone access points that implement all of the WLAN functions: management, control, data transport and client access. An example of an autonomous access point is the Stratix 5100 AP or any Cisco AP running the autonomous Cisco IOS software.

Each autonomous AP is configured and managed individually. Limited coordination of operation exists between autonomous APs, as well as limited capability to implement scalable solutions for configuration and firmware management, client mobility, WLAN security and resilience.
Unified WLAN Overview

The Unified WLAN architecture is a Cisco solution for large scale plant-wide deployments of wireless infrastructure. In the Unified architecture, the WLAN functionality is split between lightweight access points (LWAP) and wireless LAN controllers (WLC). Most WLAN control and management functions are centralized in the WLC, and timing-critical functions of the 802.11 protocol are distributed to lightweight or "thin" APs (see Figure 2-2).

In addition to base functionality provided by LWAP and WLC, the Unified architecture includes comprehensive solutions for:

- WLAN management, end-user connectivity, and application performance visibility
- Advanced spectrum analysis, Location Based Services (LBS) and wireless Intrusion Prevention Services (wIPS)
- Design and implementation of security policy across the entire network

The spectrum analysis, LBS and wIPS features of the Unified architecture are not covered in the scope of this CPwE WLAN guide.

![Unified WLAN Functions](image)

The lightweight APs, which typically involve "zero-touch" deployment, do not require individual configuration. Configuration parameters, firmware updates, diagnostic information, and other control traffic are exchanged between LWAPs and WLCs via the Control and Provisioning of Wireless Access Points (CAPWAP) protocol. CAPWAP control messages are secured in a Datagram Transport Layer Security (DTLS) tunnel.

A Stratix 5100 AP in the WGB mode can join the Unified WLAN and communicate with LWAPs as a wireless client. However, WGBs are autonomous APs that are configured and managed separately from the lightweight APs.
Selecting the WLAN Architecture

An Autonomous WLAN architecture can be used to support stand-alone IACS applications with fixed number of clients and tightly controlled data traffic, using a dedicated set of radio channels. The limitations of the Autonomous WLAN make it unsuitable for large scale plant-wide deployments supporting wide range of clients and applications.

The Unified WLAN architecture is the only practical choice for large scale plant-wide WLAN infrastructure. Often the Unified architecture is selected because of the existing WLAN infrastructure and IT requirements. One of the main factors is centralized spectrum control and a WLAN policy that eliminates uncoordinated wireless "islands" for every application in the plant.

Both Unified and Autonomous architectures can coexist, with Autonomous WLANs deployed in some Cell/Area zones, and Unified WLAN throughout the plant.

In the mixed environment, Cisco WLCs and Cisco Prime™ Network Control System (NCS) can provide limited management features and visibility for the autonomous APs and WGBs.

When considering a WLAN architecture for a particular IACS application, use the guidelines in Table 2-2:

Table 2-2 WLAN Architecture Guidelines

<table>
<thead>
<tr>
<th>Unified WLAN Architecture</th>
<th>Autonomous WLAN Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Large number of APs (&gt;10)</td>
<td>• Small scale network (&lt;10 APs)</td>
</tr>
<tr>
<td>• Equipment that require wireless roaming</td>
<td>• Larger number of WGBs per AP (see Packet Rate Considerations, page 2-7)</td>
</tr>
<tr>
<td>• Plant-wide roaming across Cell/Area zones</td>
<td>• High performance applications that require fine tuning of QoS and radio parameters</td>
</tr>
<tr>
<td>• Existing IT practices and security policies that require Unified architecture</td>
<td>• WLAN is integrated into a stand-alone OEM machine and delivered to a plant</td>
</tr>
<tr>
<td>• WLAN is managed jointly by IT personnel and control engineers; greater level of expertise is required</td>
<td>• No roaming</td>
</tr>
<tr>
<td></td>
<td>• WLAN is managed by control engineers, lower level of expertise is required</td>
</tr>
<tr>
<td></td>
<td>• 24/7 continuous wireless operation (see WLC Redundancy and Resiliency, page 2-33)</td>
</tr>
</tbody>
</table>

Applying Wireless in IACS Applications

This section provides considerations and recommendations for using wireless media with IACS applications and EtherNet/IP protocol.

General Considerations

Table 2-3 shows IACS traffic types and Common Industrial Protocol (CIP) standards, whether they can be used with wireless media, and known constraints.

Table 2-3 Use of IACS Applications with Wireless Media

<table>
<thead>
<tr>
<th>IACS Traffic 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>&lt;20% of total packet rate if combined with CIP Class 1 Standard and Safety traffic</td>
</tr>
<tr>
<td>Peer-to-peer Messaging</td>
<td>CIP Class 3 (MSG)</td>
<td>Yes</td>
<td>See above</td>
</tr>
<tr>
<td>Peer-to-peer Control</td>
<td>CIP Class 1 Produced/Consumed</td>
<td>Yes</td>
<td>Application should tolerate higher latency and jitter</td>
</tr>
<tr>
<td>I/O Control</td>
<td>CIP Class I/O</td>
<td>Yes</td>
<td>See above</td>
</tr>
</tbody>
</table>
Application Requirements

When considering wireless media for an IACS application, it is critical to know the application requirements such as traffic types and packet rates, as well as reliability and latency requirements. This information will not only be helpful in deciding if wireless media is appropriate, but also help determine what kind of WLAN infrastructure is needed to support the application.

The following information should be available:

- Number and type of devices in the WLAN (wired and wireless)
- Number of wireless clients per channel (i.e., WGBs or integrated wireless adapters)
- IACS traffic types required by the application:
  - HMI Server to Client
  - Explicit Messaging
  - Standard Produced/Consumed
  - Standard I/O
  - Safety Produced/Consumed
  - Safety I/O
  - CIP Sync
- Total expected packet rate in each wireless channel
- Requested Packet Intervals (RPI), packet size, direction of traffic and packet per second (PPS) rate for each type of IACS traffic listed above
- Information about maintenance and non-IACS traffic that may use the same wireless bandwidth:
  - Network management protocols, such as HTTPS, Secure Shell (SSH), Telnet and Simple Network Management Protocol (SNMP)
  - RSLinx®, Studio 5000®, trends
  - Voice, video and other enterprise applications
- IACS application requirements:
  - Maximum latency and jitter
  - Acceptable packet loss
  - CIP Safety Connection Reaction Time Limit (CRTL)
  - Safety System Reaction Time
- High availability requirements:
  - Minimum operation time without connection loss

Table 2-3  Use of IACS Applications with Wireless Media (continued)

<table>
<thead>
<tr>
<th>IACS Traffic Type</th>
<th>CIP Standard</th>
<th>Use with Wireless</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Control</td>
<td>CIP Safety</td>
<td>Yes</td>
<td>Very fast safety reaction times may not be supported</td>
</tr>
<tr>
<td>Time Synchronization</td>
<td>CIP Sync</td>
<td>Limited</td>
<td>Limited accuracy, may be suitable for SOE and event logging applications</td>
</tr>
<tr>
<td>Motion Control</td>
<td>CIP Motion</td>
<td>No</td>
<td>Not feasible with CIP Motion drives due to higher latency and jitter of wireless media and insufficient CIP Sync accuracy</td>
</tr>
</tbody>
</table>
Chapter 2  System Design Considerations

Applying Wireless in IACS Applications

- Maximum power cycle time
- Network and application redundancy

- Time synchronization requirements (PTP, NTP)
- Equipment mobility requirements:
  - Fixed position
  - Non-operational relocation (nomadic)
  - Mobile equipment with no roaming
  - Mobile equipment with fast roaming
- Type of movement (rotary platforms, tracks, AGV, cranes)
- If multiple identical applications need to operate throughout the plant:
  - Number of installations
  - Distance between each operation area

Packet Rate Considerations

The throughput of an IACS application sending EtherNet/IP traffic over the wireless media is more limited than for wired Ethernet communication. This is due to:

- Half-duplex communication in shared media (radio waves)
- Large amount of overhead in the wireless protocol
- Variable delays due to collision avoidance mechanism
- Retransmissions of packets lost due to collisions and interference
- EtherNet/IP traffic characteristics (small packet sizes, cyclic transmission to multiple nodes at once) which limits the effectiveness of the 802.11 wireless protocol

The main parameter for the wireless IACS application using EtherNet/IP is the **packet rate per radio channel** (number of data packets per seconds). If the packet rate exceeds the recommended number, performance and reliability issues, such as increased latency and jitter, packet loss and connection timeouts, could occur.

Based on the performance test results, the following recommendations can be made:

- Do not exceed **2,200 pps** in the wireless channel with EtherNet/IP traffic.
- The following system sizes were tested as part of this CVD to achieve the above packet rate:
  - Unified WLAN: 4 WGBs per AP
  - Autonomous WLAN: 12 WGB per AP

Today, the Autonomous WLAN has a higher degree of QoS granularity than the Unified WLAN. As such, the number of WGBs supported per autonomous AP is greater than the Unified LWAP for the equivalent IACS packet rate. To scale a Unified WLAN, add additional LWAPs to support the number of WGBs required by the IACS application.

- Reduce packet rate in environments with RF issues and interference.
- **Reserve 20% of bandwidth** for HMI and maintenance traffic such as RSLinx, programming tools and IT management.
- Take into account all communication in the channel, including non-IACS traffic and traffic from neighboring WLANs sharing the same channel.
Using the known IACS application parameters, the packet rate can be calculated using the Rockwell Automation tools (see below) and verified after deployment on the AP:

- Integrated Architecture® Builder (IAB):
  http://www.rockwellautomation.com/rockwellautomation/support/configuration.page
- EtherNet/IP Capacity Tool:

Examples of the packet rate calculations are shown in Appendix A, “References.”.

### IACS Traffic Optimization

A number of application optimization methods can be used to lower the total packet rate and improve the performance of EtherNet/IP over wireless:

- Use Rack Optimized I/O connections instead of direct connections when possible.
- Consider Produced/Consumed communication to a wireless PAC rather than multiple I/O connections over wireless.
- Configure unicast connections instead of multicast (see Unicast vs. Multicast, page 2-10).
- Aggregate wireless traffic through a single PAC instead of having multiple sources and destinations in the wired infrastructure. The most efficient scenario is transmission of one wireless packet in each direction per cycle.
- Minimize or eliminate direct communication between wireless clients (i.e., wireless PAC to wireless I/O, or wireless PAC to wireless PAC). This is not an efficient use of bandwidth since each packet is transmitted twice (upstream to the AP and downstream from the AP).
- Combine Produced/Consumed data into larger arrays and user-defined data types (UDT) using one or few connections, instead of using many individual connections of smaller size.
- Combine different types of data in one Produced/Consumed tag. For example, standard data can be appended to the safety Produced/Consumed data if the RPI is sufficient.
- Make sure that RPIs are not faster than necessary for the application.
- Disable Rack Optimized mode for Ethernet modules if no remote I/O data is being used (i.e., Produced/Consumed only). Disable unused Safety Test Output connections.
- Eliminate unnecessary CIP connections, HMI and trending traffic over the wireless connection.
- Create and enforce the policy to limit the amount of IACS maintenance traffic over the wireless:
  - Do not allow multiple instances of Studio 5000 for online edits, uploads and downloads over the same wireless channel.
  - Avoid running multiple trends and RSLinx instances.

### Non-IACS Traffic Control

An effective and strictly enforced policy should be in place to prevent excessive or unauthorized traffic over the wireless link. Some of the recommendations are listed below:

- It is recommended that a dedicated wireless channel be used for the IACS application. Sharing the channels between applications, especially under different administrative control, should be avoided.
- Strict spectrum policy must be in place to prevent unauthorized transmissions. The spectrum should be monitored for interference from neighboring WLANs and rogue APs.
• Do not allow non-WGB wireless clients (laptops, tablets or smartphones) in a WLAN dedicated to the critical EtherNet/IP communication. Use another wireless channel or wired infrastructure for maintenance traffic.

• Avoid using video streaming, large file transfers or similar applications over the same channel as the IACS control traffic.

• Limit IT management and monitoring traffic, including HTTP, SNMP, Telnet, SSH, Syslog and ICMP protocols.

• Limit or eliminate unnecessary broadcast and multicast traffic in the network (ARP, client discovery protocols, IPv6 discovery or CDP).

• Prevent excessive number of probe requests from personal mobile devices. Depending on the policy, these devices should either join the existing corporate WLAN or have their Wi-Fi radios off on the plant floor.

• Limit the number of SSIDs per radio to reduce beacons.

Performance Characteristics

In addition to throughput restrictions, wireless media has other constraints to the IACS performance. Some of the considerations are discussed in this section.

Latency and Jitter

Wireless communication causes higher latency and jitter than does wired Ethernet for real-time IACS traffic. However, the average latency and jitter should meet the performance requirements of typical IACS applications if certain criteria are met (see Chapter 5, “Testing the Architecture” for test results).

• Packet rate in the channel must be below the recommended limit. Overloading the channel will lead to excessive latency and jitter due to collisions and retransmissions.

• Applying wireless QoS policy is critical to control latency and jitter.

• A very small percentage of packets can be delayed significantly enough to be unusable. The application should be able to tolerate occasional late and lost packets.

• Larger number of wireless nodes increases maximum latency due to the contention for the channel access. The average latency, however, may not change significantly.

• Very low RPIs (< 10ms) may not be appropriate for wireless applications.

Packet Loss

In 802.11-based wireless networks, data delivery cannot always be guaranteed due to collisions in the shared media, interference or poor signal quality. Some considerations regarding the packet loss are listed here.

• It is recommended to limit the number of retries and transmission time for real-time EtherNet/IP data allowing occasional packet drop. This method prevents excessive delays for all packets in the queue and delivery of "stale" data to IACS devices.

• An application should be able to tolerate occasional packet loss. Test results show that with normal channel load, optimal RF conditions and recommended QoS configuration, the observed application-level packet loss is very small (see Chapter 5, “Testing the Architecture” for test results).

• Exceeding the recommended packet rate causes high packet loss.

• Multicast and broadcast traffic is delivered without retries or acknowledgments and has much higher packet loss.
Application 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 its parameters. A timeout can be caused by excessive wireless latency or loss of several packets in a row from the same CIP connection.

Consider the following when evaluating reliability of wireless communication.

- Exceeding the recommended packet rate will eventually lead to application timeouts.
- Systems with a larger number of wireless nodes may have a higher chance of timeouts due to an increased number of collisions and retries.
- Certain parameters (for example, RPIs and safety multipliers) may need to be adjusted to prevent timeouts and improve reliability.
- Certain events can cause significant delays and packet loss in the channel, and have an effect on application reliability:
  - Wireless roaming and network convergence
  - Periodic off-channel scanning of spectrum (if enabled)
  - Periodic security re-association (session timeout)
  - Switching of a radio channel
  - Persistent interference
  - Radar presence in certain channels
  - Unauthorized channel transmissions
  - Changes in RF environment
- Redundant network infrastructure should be provided for critical wireless IACS applications to increase reliability.

Unicast vs. Multicast

EtherNet/IP protocol supports unicast as a default method of communication, with some exceptions (see Table 2-4). It is recommended to use unicast EtherNet/IP connections where possible. Although multicast delivery is supported by the 802.11n standard, its use with wireless EtherNet/IP is limited.

- Multicast frames are not acknowledged and not repeated if lost. This greatly increases the packet loss and the chance of connection timeouts.
- Use only unicast connections with wireless I/O or Produced/Consumed data.
- Do not use wireless I/O or Produced/Consumed data with the ControlLogix® Redundancy System.

Table 2-4   Unicast Support for EtherNet/IP

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Unicast Support / ControlLogix Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard I/O</td>
<td>v18</td>
</tr>
<tr>
<td></td>
<td>(ControlLogix Redundancy - multicast only)</td>
</tr>
<tr>
<td>Standard Produced/Consumed</td>
<td>v16</td>
</tr>
<tr>
<td></td>
<td>(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 v24)</td>
</tr>
</tbody>
</table>
Application Protocols

This section briefly describes characteristics and provides recommendations for various CIP protocols that are relevant to wireless communication.

Standard I/O

Standard I/O data can be sent over wireless with certain restrictions to the RPIs, number of I/O connections in the system and application sensitivity to higher latency and jitter.

- The default RPI of 20ms can be supported over wireless media. RPIs as low as 10ms may be supported depending on the application sensitivity to jitter and delay (see Autonomous WLAN Test Results, page 5-4).
- Standard I/O RPIs less than 10ms are not practical for wireless media because the maximum latency and jitter become comparable or greater than the RPI.
- Use rack-optimized I/O connections where possible to reduce the packet rate.
- A system with large number of analog I/O modules or individual I/O racks may exceed the recommended packet rate in the channel. In such a case, select larger RPIs or reduce the number of I/O connections for each AP.
- If RPI or system size cannot be changed, the solution could be to use Produced/Consumed tags over the wireless network. This can be accomplished by installing a PAC on the wireless equipment to control I/O over the wired connection.
- Standard I/O connections have a timeout period of 100 ms or greater, and can tolerate up to three lost packets in a row. If the channel packet rate is within the recommended limit, then the latency in wireless media should not cause a standard I/O timeout.
- The degree to which lost or delayed I/O packets can be tolerated is application-specific. Even when no connection timeouts exist, average and maximum latency as well as packet loss in a wireless channel have to satisfy application requirements.

Standard Produced/Consumed

Recommendations for standard Produced/Consumed data over wireless are very similar to those of I/O data.

- RPI recommendations are the same as for standard I/O data. Do not use faster RPIs than required by the application.
- Application data should be aggregated into large arrays or UDTs in order to reduce the number of connections, the packet rate, and create larger packet sizes for more efficient wireless transmission. The maximum Produced/Consumed tag size is limited to 512 bytes in the CIP specification.
- If no I/O modules exist in the remote racks (only Produced/Consumed data is passed), disable rack-optimized mode for Ethernet modules.
- In general, PAC to PAC topology with Produced/Consumed tags is preferred over PAC to I/O topology for wireless communication.
- The timeout requirements for standard Produced/Consumed tags are the same as for the I/O data.
CIP Safety

CIP Safety data can be sent reliably over wireless media if latency and packet loss is controlled. It is necessary to select CIP Safety parameters to achieve long-term reliability without "nuisance" safety timeouts. The following recommendations are based on the performance test results (see also Chapter 5, “Testing the Architecture”):

- CIP Safety connections have stricter requirements to the latency and packet loss than standard data. Safety System Reaction Time (SRT) for the application determines these requirements. Applications that need very fast reaction times may not be appropriate for wireless.

- Default CIP Safety parameters in the GuardLogix® system have to be increased for the wireless media.

- Configure CRTL to be at least x4 the RPI to prevent safety timeouts in case of network latency or packets lost in a row.

- If necessary, increase CRTL further by changing Safety Timeout or Network Delay multipliers.

- Safety I/O modules do not support rack-optimized mode and use direct connection mode. A system with large number of safety modules may exceed the recommended packet rate. In such case, select higher RPIs or reduce the number of safety I/O connections for each AP.

- It is more efficient to use safety Produced/Consumed tags over wireless and to install a safety PAC on the wireless equipment for I/O control. In this case, safety data from several I/O modules can be aggregated into one safety produced tag.

- The performance test results show that the CIP Safety parameters listed in Table 2-5 can be supported over wireless:

Table 2-5  CIP Safety Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRTL</td>
<td>4 x RPI, ≥ 60 ms</td>
</tr>
<tr>
<td>RPI</td>
<td>≥ 15 ms</td>
</tr>
<tr>
<td>System Reaction Time (SRT) - Worst Case No Fault</td>
<td>≥ 200 ms</td>
</tr>
<tr>
<td></td>
<td>(≥ 130 ms depending on the system size and RPIs)</td>
</tr>
<tr>
<td>System Reaction Time (SRT) - Worst Case Single Fault</td>
<td>≥ 360 ms</td>
</tr>
<tr>
<td></td>
<td>(≥ 200 ms depending on the system size and RPIs)</td>
</tr>
</tbody>
</table>

Note: The worst-case Logix SRT values can be calculated using the Safety Estimator tool available from the Rockwell Automation website:


Wireless Design Considerations

This section describes design considerations and recommendations for Autonomous and Unified WLAN when applied to the IACS applications.
Radio Frequency Design

The performance of the WLAN depends greatly on the RF coverage design and selection of RF parameters such as channels, data rates and transmit power. The following sections provide an overview of RF recommendations and best practices for wireless IACS applications.

Wireless Spectrum

The main factors when allocating wireless spectrum to an IACS application are availability of the channels, bandwidth requirements of the application and existing and potential sources of interference.

- Use only 5 GHz frequency band for critical IACS applications such as I/O, peer to peer and safety control. The 2.4 GHz band is not recommended for these applications because of limited number of channels, widespread utilization of the band and much higher chance of interference.
- Use 2.4 GHz band, if necessary, for personnel access and low throughput non-critical applications on the plant floor.
- Avoid using Dynamic Frequency Selection (DFS) channels in 5 GHz band (channels 52-144) for IACS applications because of potential radar interference.
- 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.
- Determine the number of available channels and existing bandwidth utilization in each channel. It is critical to have a spectrum management policy and to coordinate spectrum allocation between IT, OEM and control engineers.
- Avoid sharing spectrum between different applications, especially under different management and with unknown bandwidth utilization. It is recommended to allocate channels exclusively to the IACS application.
- Calculate required or worst case packet rate over the wireless media for the application. Determine how many channels are necessary to cover the requirements based on the recommended packet rate limit (see Packet Rate Considerations, page 2-7).
- Perform detailed RF spectrum survey at the site. Adequate time should be spent analyzing the channels to detect intermittent interference throughout the site. Spectrum analysis is critical for IACS applications with high packet rate and low latency requirements.
- Many sources of interference are intermittent, and new sources may appear over time. It is important to proactively monitor for radio interference and rogue sources before and after the deployment. Properly defined and enforced spectrum policy on site is critical for interference prevention.

Wireless Coverage

The main goal when designing wireless coverage for an IACS application is to provide adequate signal strength for wireless clients throughout the Cell/Area zone and to be able to support the required data rate. In addition, wireless cell size should be controlled to achieve desired number of clients per AP, and to minimize co-channel interference between cells.

- Determine the maximum number and locations of the wireless clients (WGBs), including future expansions.
- Identify redundancy requirements for coverage, i.e., if two (or more) APs should be seen from any point to provide for failures.
• Perform professional site survey to determine the number and locations of the APs that can cover the area with required level of redundancy. The site survey should also determine the appropriate antenna types and verify link performance and supported data rates.

• Design the wireless coverage to maintain the parameters listed in Table 2-6 in the Cell/Area zone:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received Signal Strength Indicator (RSSI)</td>
<td>Min -67 dBm</td>
</tr>
<tr>
<td>Signal-to-Noise Ratio (SNR)</td>
<td>Min 25 dB</td>
</tr>
<tr>
<td>Supported data rate</td>
<td>54 Mbps</td>
</tr>
</tbody>
</table>

• Configure transmit power manually for each device to provide adequate coverage. The transmit power of the AP typically matches the transmit power of client adapters or WGBs.

• Change the transmit power from the maximum to reduce signal propagation outside the intended area and to minimize co-channel interference (CCI) on site.

• Use static channel allocation in the WLAN. Determine if wireless channels have to be reused based on the spectrum availability. Channel allocation scheme should provide maximum distance separation between cells using the same channels.

• Do not reuse the channels for wireless cells operating with high utilization and high client count, unless complete signal separation can be achieved.

• If a channel is reused and CCI is expected, the available bandwidth is essentially shared between the wireless cells. The total packet rate should be calculated including every application using the channel.

• If possible, use non-adjacent channels in 5 GHz band for overlapping wireless cells (for example, 36 and 44).

Radio Parameters

Certain RF parameters, such as allowed data rates and 802.11n features, should be configured differently for IACS applications using EtherNet/IP data than for a typical enterprise application. Some of the parameters are already optimized in the default Stratix 5100 configuration.

• Configure 6, 12, 24, 54 Mbps data rates as the basic (required) rates in the WLAN.

• Disable 802.11n data rates (MCS 0-23) for applications with real-time EtherNet/IP traffic (I/O, Produced/Consumed, CIP Safety). Using 802.11n data rates does not provide advantages for these types of traffic and may decrease reliability.

• 802.11n data rates (MCS 0-23) can be enabled for WLANs only with lower priority EtherNet/IP traffic (HMI, maintenance, Class 3 messaging) or non-IACS client devices and applications.

• Do not use channel bonding (40 MHz bandwidth). Use of wider channels consume the available bandwidth without improving EtherNet/IP performance.

Autonomous WLAN Design Considerations

The main use cases for an Autonomous WLAN architecture are small scale IACS applications with fixed number of clients (WGBs) in a single Cell/Area zone. The architecture can have one or several APs supporting these type of applications (refer to Chapter 1, “CPwE-WLAN System Introduction” for definitions):
Wireless Design Considerations

IACS Topologies in Autonomous WLANs

The most common topologies for wireless IACS equipment in Autonomous WLANs are discussed in the following sections.

Fixed PAC to Wireless I/O Topology

In this topology, a fixed PAC in the wired infrastructure controls a number of wireless I/O devices behind WGBs. Wired HMI clients may also be installed on the wireless equipment. This use case has the following characteristics:

- Each wireless connection may carry data for several individual CIP connections, depending on the application (see Figure 2-3):
  - Rack optimized discrete I/O connections
  - Analog or discrete direct I/O connections
  - Safety I/O connections
  - HMI client data (for instance, FactoryTalk® View ME or SE)
- More than one EtherNet/IP I/O device can be connected to a WGB (in linear topology or via a switch).
- A large number of CIP connections (EtherNet/IP adapters, analog or safety I/O modules) increases the packet rate in the channel and may exceed the limit. The solution could be to configure slower RPIs or to use more wireless channels for the application.
- Small CIP packet sizes limit the efficiency of wireless protocol (less bytes of data can be transmitted in a channel regardless of network speed).
The most common configuration for wireless IACS equipment is the topology where a fixed PAC communicates with a number of wireless PACs. This use case has the following characteristics:

- Each wireless connection may support several types of data (see Figure 2-4):
  - Produced/Consumed tags
  - Safety Produced/Consumed tags
  - Message instructions
  - HMI client data (FactoryTalk View SE client to server)
  - Maintenance and monitoring traffic (Studio 5000, RSLinx etc.)
- IACS data can be aggregated into one or a few large Produced/Consumed tags that brings down the packet rate and increases the efficiency of wireless communications.
- Each wireless PAC may have wired I/O or drives connected using a linear topology with embedded switch technology or an Ethernet switch. 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 wireless PAC.
- The second Ethernet module can be installed on the wireless PAC to segment local wired devices. The downside of the physical segmentation via the PAC backplane is that non-CIP traffic cannot reach remote devices for diagnostic or configuration purposes.
Wireless to Wireless Communication

In certain applications, a wireless PAC may need to send data to another wireless PAC or a wireless I/O connected to the same AP. An example may be machine interlocking, safety status and listen-only I/O connections (see Figure 2-5).

In the traditional (not a mesh or ad-hoc) mode, wireless-to-wireless communication requires data to be sent upstream from the WGB to the AP and then downstream to another WGB.

- Direct communication between two wireless devices doubles the number of wireless frames and inefficiently uses the available bandwidth. Network latency will be more than twice as high.
- Wireless PAC to wireless PAC or I/O traffic should be limited and kept at low rates or removed altogether.

**Note**

Wireless-to-wireless traffic has not been tested for performance and is not covered in this guide.
SSID and VLAN Segmentation

In the WLAN architecture, a Service Set Identifier (SSID), commonly called the "network name" is used by a group of APs and wireless clients to communicate with each other using common parameters (for example, security settings). An SSID can be loosely compared to a VLAN in a wired network, and typically (but not always) a one-to-one relation exists between them.

A WLAN can have several SSIDs defined for different types of clients, for example guests, corporate users or wireless phones. In the industrial environment, different SSIDs and VLANs can be assigned for critical and non-critical IACS data, such as machine control and maintenance traffic.

**Note**

Different SSIDs on the same radio channel provide logical segmentation, but still share the same bandwidth and interfere with each other on the physical layer.

When configuring SSID and VLAN parameters for the Autonomous WLAN, this information should be considered:

- No default SSID exists in the initial Stratix 5100 configuration. One or many SSIDs must be defined globally on the AP.
- Stratix 5100 supports VLANs, but they are not configured by default. If VLANs are used, each VLAN can be associated to only one SSID.
- Each AP radio interface (2.4 or 5 GHz) can be configured with one or several SSIDs. The same SSID can be applied to both radios to support clients in both frequency bands.
- A WGB can only use one SSID at a time to communicate with the root AP. Multiple SSIDs can be defined globally on a WGB; however, only one SSID can be active on the radio interface in the WGB mode.
- 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.
- AP or WGB management traffic over wired or wireless interface must belong to a native VLAN.
Single SSID / VLAN Architecture

The most common case is when a single SSID is used for all traffic in the Autonomous WLAN. The data is assigned to one VLAN in the wired infrastructure (see Figure 2-6).

- Use a single SSID/VLAN configuration for a WLAN with a fixed set of wireless clients (WGBs) using the 5 GHz radio. This configuration is used for a single IACS application mainly for equipment control purposes.

- Other wireless clients (for example, laptops and tablets) should not connect directly to the SSID used for IACS equipment control. The maintenance and monitoring traffic to the wireless equipment should originate in the wired infrastructure.

- Do not configure VLANs on the APs and WGBs when using a single SSID. In this mode, the AP does not tag packets with a VLAN ID when sending them to the wired network.

- If necessary, assign traffic going from the AP to the wired LAN to a particular VLAN by associating the switch port with that VLAN (Access Mode port).

- Use the Access Mode on the switch port connected to the WGB.

**Note**

The switch on the wireless equipment can be configured for any VLAN, including the same VLAN as the switches on the wired network. The VLAN information, however, will not be sent over the wireless link by the WGB.

- Configure the same VLAN for all switch ports that connect autonomous APs with a common SSID, for example, for a nomadic wireless equipment that moves between the APs in a Cell/Area zone.
- Use a dedicated VLAN for each wireless application in the network, according to best practices for VLAN segmentation.

**Figure 2-6  Single SSID / VLAN Example**
Multiple SSID / VLAN Architecture

Multiple SSIDs and VLANs in the Autonomous WLAN can be used to segment the IACS control traffic from the non-critical wireless traffic, for example maintenance personnel using laptops and tablets. The maintenance traffic should also be placed on a separate wireless channel, either the 2.4 GHz radio on the same AP or a different 5 GHz channel on another AP dedicated for that purpose.

The following are recommendations for the multiple VLAN / SSID architecture implemented on a single autonomous AP (see Figure 2-7):

- Use one SSID per AP radio and per wireless channel for IACS applications. Multiple SSIDs on the same channel provide logical segmentation, but still have to share the channel bandwidth. In addition, multiple wireless beacons on the channel also consume bandwidth.

- Use 2.4 GHz radio to connect non-WGB clients on a separate VLAN / SSID. Reserve the 5 GHz radio for WGB clients and IACS control traffic.

- Create two SSIDs for IACS control and non-critical traffic and associate each with a separate VLAN on the AP. Configure VLAN tagging (trunk mode) on the AP and the switch port.

- Do not configure VLANs on the WGBs since they do not support VLAN tagging on the radio interfaces.

- Configure the VLAN used for the IACS control as a native VLAN on the radio and Ethernet interface of the AP, and on the switch trunk port that is connected to the AP.

- Configure IP addresses for the AP and WGBs in the native VLAN.

The native VLAN configured between the AP and the switch should be different from the native VLAN configured on the trunk ports between switches. Per CPwE guidelines, the inter-switch trunk native VLAN should be a dedicated VLAN that is not used for the IACS traffic.

- Use the Access Mode on the switch port connected to the WGB.

Figure 2-7  Multiple SSID / VLAN Example
Wireless QoS

Wireless networks are fundamentally different from wired Ethernet networks because of the half-duplex communication in the shared media. Quality of Service (QoS) in a WLAN plays a critical role for IACS applications with strict requirements for latency, jitter and packet loss.

The wireless QoS design guidelines for IACS applications are similar to the wired QoS guidelines:

- 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, Safety, I/O and HMI) have different requirements for latency, packet loss and jitter. The QoS policy should differentiate service for these types of flows and satisfy their performance requirements.

Traffic Classification

An autonomous AP or WGB should be able to classify IACS packets and assign a priority to each of them. Follow these recommendations for wireless EtherNet/IP traffic classification in Autonomous WLANs:

- Use the latest firmware for EtherNet/IP adapters that support QoS marking. Configure QoS on the adapters if it is not enabled by default.
- Apply the recommended QoS configuration on the industrial Ethernet switches, for example using Express Setup procedure in Stratix 5700®, Stratix 8000® and Stratix 8300® switches. Use appropriate Smartport templates for the switch interfaces.
- Use the Wi-Fi Multimedia (WMM) QoS method that is enabled by default on the Stratix 5100 and Cisco APs. The WMM uses four QoS categories for wireless traffic: Background, Best Effort, Video and Voice. Different classes of EtherNet/IP traffic should be mapped to one of these categories according to the guidelines below.

Note

In the IACS environment, "Video" and "Voice" queues are not used for the IP video and telephony traffic, but are reserved for critical types of traffic such as Class 1 EtherNet/IP and CIP Sync.

- Use the default Stratix 5100 configuration that classifies and maps the IACS traffic according to Table 2-7.

Table 2-7  Wireless QoS Classification for EtherNet/IP

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>CIP Traffic Usage</th>
<th>Port Number</th>
<th>DSCP</th>
<th>CoS</th>
<th>WMM Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTP event</td>
<td>CIP Sync</td>
<td>UDP 319</td>
<td>59</td>
<td>6</td>
<td>Voice</td>
</tr>
<tr>
<td>PTP management</td>
<td>CIP Sync</td>
<td>UDP 320</td>
<td>47</td>
<td>4</td>
<td>Video</td>
</tr>
<tr>
<td>CIP class 0 / 1</td>
<td>CIP Motion</td>
<td>UDP 2222</td>
<td>55</td>
<td>4</td>
<td>Video</td>
</tr>
<tr>
<td>Safety I/O, I/O</td>
<td>UDP 2222</td>
<td>47</td>
<td>4</td>
<td>Video</td>
<td></td>
</tr>
<tr>
<td>I/O</td>
<td>UDP 2222</td>
<td>43</td>
<td>4</td>
<td>Video</td>
<td></td>
</tr>
<tr>
<td>Not used</td>
<td>UDP 2222</td>
<td>31</td>
<td>4</td>
<td>Video</td>
<td></td>
</tr>
<tr>
<td>CIP class 3</td>
<td>CIP messaging, HMI, tools</td>
<td>TCP 44818</td>
<td>27</td>
<td>0</td>
<td>Best Effort</td>
</tr>
<tr>
<td>Unclassified</td>
<td>N/A</td>
<td>Any</td>
<td>0</td>
<td>0</td>
<td>Best Effort</td>
</tr>
</tbody>
</table>

Wireless QoS Parameters

The default WMM parameters are optimized for enterprise applications that are most sensitive to latency, jitter and packet loss, specifically video and voice. In Autonomous WLAN, some of the QoS and radio parameters can be adjusted for EtherNet/IP traffic with even higher performance requirements.
Wireless Design Considerations

- Use the default QoS configuration in the Stratix 5100 for the Autonomous WLAN. The factory configuration applies optimized QoS parameters to the radio interfaces for the outbound traffic (see Table 2-8).

  **Note**
  
  Two sets of parameters exist: for the root AP (downstream traffic) and for the WGB (upstream traffic). Downstream traffic is given a higher preference than the upstream in this configuration.

- In the Unified architecture, QoS parameters are controlled by the WLC and cannot be optimized in the same way as in the Autonomous WLAN. When using a WGB in the Unified WLAN, refer to Unified WLAN QoS, page 2-34 for configuration guidelines.

### Table 2-8 Wireless QoS Parameters for EtherNet/IP

<table>
<thead>
<tr>
<th>Device Role</th>
<th>WMM Queue</th>
<th>Traffic Type</th>
<th>CW-Min</th>
<th>CW-Max</th>
<th>Fixed Slot</th>
<th>TXOP</th>
<th>Max Retries</th>
<th>Packet Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td>Voice</td>
<td>PTP events</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1 ms</td>
</tr>
<tr>
<td>AP</td>
<td>Video</td>
<td>CIP Class 0 / 1, PTP mgmt</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>10 ms</td>
</tr>
<tr>
<td>AP</td>
<td>Best Effort</td>
<td>CIP Class 3, non-CIP traffic</td>
<td>7</td>
<td>10</td>
<td>12</td>
<td>0</td>
<td>8</td>
<td>Not used</td>
</tr>
<tr>
<td>WGB</td>
<td>Voice</td>
<td>PTP events</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1 ms</td>
</tr>
<tr>
<td>WGB</td>
<td>Video</td>
<td>CIP Class 0 / 1, PTP mgmt</td>
<td>7</td>
<td>7</td>
<td>3</td>
<td>0</td>
<td>4</td>
<td>10 ms</td>
</tr>
<tr>
<td>WGB</td>
<td>Best Effort</td>
<td>CIP Class 3, non-CIP traffic</td>
<td>7</td>
<td>10</td>
<td>12</td>
<td>0</td>
<td>8</td>
<td>Not used</td>
</tr>
</tbody>
</table>

---

**WLAN Security**

The nature of wireless communication requires implementation of strong security mechanisms. WLAN security is implemented using authentication between devices and encryption of data and management traffic. Some of the security considerations and recommendations for Autonomous WLANs are discussed in this section.

- WPA2 security with AES encryption is the only mechanism recommended for IACS wireless applications. AES encryption is implemented in hardware and does not degrade the application performance.
- WPA2 standard supports pre-shared key authentication or IEEE 802.1X authentication framework. Factors such as security policy, infrastructure support and ease of deployment determine the authentication method that should be selected.

**WLAN Authentication**

Authentication method can be defined for each SSID individually, and multiple methods can exist in the same Autonomous WLAN, for example to support different types of clients.

**Pre-Shared Key Authentication**

This method relies on a common password configured on the autonomous AP, WGB or another client device.

- Use WPA2 pre-shared key authentication for small scale Autonomous WLANs where wireless clients are tightly controlled. An example would be an IACS application with fixed number of wireless machines using WGBs.
- Be aware of the pre-shared key limitations:
  - Pre-shared key method cannot be used to limit access only to certain clients. Anyone with the knowledge of the key can authenticate to the WLAN.
  - Once the key is compromised, all devices need to be reconfigured with the new key.
Chapter 2      System Design Considerations

Wireless Design Considerations

– Pre-shared key authentication is not supported with fast roaming.

802.1X-based Authentication

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

802.1X/EAP authentication method provides strong security with granular access control based on individual user credentials. However, the 802.1X method requires additional components to be available in the Autonomous WLAN:

- Remote Access Dial-In User Service (RADIUS) authentication server
- Client credentials database, either local on the AP or external directory
- Wireless clients that support one of the EAP implementations

For an IACS application using WGBs as wireless clients, the following configuration is recommended for the Autonomous WLAN (see Figure 2-8):

- Select 802.1X authentication in the environments where pre-shared keys cannot satisfy the security requirements.
- Use EAP-FAST protocol to authenticate WGBs to the Autonomous WLAN. EAP-FAST does not require security certificates and related infrastructure.
- Configure the dedicated AP as a RADIUS server. Configure credentials for each WGB and store them locally on the RADIUS AP. This access point should not accept any wireless clients.
- An external RADIUS server with EAP-FAST support can also be used.
- If security policy requires certificates and other EAP protocols for authentication, Unified WLAN architecture is more appropriate.

Figure 2-8    802.1X Authentication with Local RADIUS

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 supporting a critical IACS application.

- MAC-based authentication is not a secure method by itself since MAC addresses can be detected over the air and spoofed. It should only be used to complement other methods such as pre-shared key or 802.1X authentication.
High Availability

High availability is a major requirement for any IACS application. In the Autonomous WLAN architecture, high availability can be achieved by using redundant network infrastructure devices and topologies, providing redundant wireless coverage and by protecting wireless spectrum from interference and unauthorized transmissions.

Design recommendations for high availability in the Autonomous WLAN are provided below.

- Use resilient network topologies and protocols in the wired infrastructure that satisfy the high availability requirements of the wireless IACS application. The examples are redundant star and ring topologies for network switches, Resilient Ethernet Protocol (REP) and Flex Links or EtherChannel.
- Select redundant network switches for the distribution layer, for example with Cisco StackWise® technology.
- Use spectrum analysis tools to proactively detect and mitigate sources of interference and unauthorized transmissions. Create and enforce wireless spectrum policy at the site.
- Monitor and regulate the amount of data that is transmitted over the wireless channel, particularly maintenance and monitoring traffic (see Packet Rate Considerations, page 2-7).
- Use redundant AP coverage for critical applications to minimize downtime. This configuration is discussed in the next section.

Redundant AP Coverage

Additional access points can be used in the WLAN to provide redundant wireless coverage for the equipment. Such configuration can minimize downtime if the primary AP is down or if the signal from the AP is severely degraded.

- Redundant APs can operate in the same or different channels. If wireless spectrum is available, select different channels for better protection from interference.
- Design RF coverage in the area to receive adequate signal from both APs (see Table 2-6).
- Connect redundant APs to different network switches in a resilient topology. Use redundant Power over Ethernet (PoE) sources, if available.
- If redundant APs are connected to the switch stack with PoE ports, use different stack members for the APs.
- Do not place redundant APs right next to each other (minimum 2 meters between antennas is recommended).
- Make sure that primary and backup AP configurations match. Use the same SSID, VLAN and IP subnet.
- Please be aware that association to the backup AP may take up to 30 seconds if the primary AP is lost (powered down). It will cause I/O and Produced/Consumed connections to timeout.
- The WGBs can also roam to the backup AP if the signal strength becomes poor. In this case, configure WGBs for roaming criteria (see Workgroup Bridge Configuration, page 3-18).
- If the application requires faster recovery time, consider Unified WLAN architecture with fast roaming support.

Unified Wireless Design Considerations

This section provides design considerations for using Cisco Unified WLAN architectures with IACS applications in the large plant-wide environment.
Chapter 2      System Design Considerations

Unified WLAN Overview

This section provides an overview of the Unified WLAN.

Access Point (AP)

An access point (AP) is a device that allows wireless devices to connect to a wired network. In the Unified architecture, the access points are configured, managed and controlled through the Wireless LAN Controller (WLC).

FlexConnect AP Mode

FlexConnect is a wireless solution for branch office and remote office deployments. It enables customers to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect APs can switch client data traffic and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller. In the connected mode, the FlexConnect AP can also perform local authentication.

In the Cell/Area Zone (Level 0 - 2), the use of FlexConnect configurations on the wireless APs will provide the shortest path connectivity between the WGB/AP-attached equipment and the wired equipment within the Cell/Area Zone (Level 0 - 2).

Some of the APs utilized in the Unified Access architecture will have FlexConnect enabled so that local switching will occur for all intra-cell traffic. This will help meet latency requirements.

Workgroup Bridge (WGB)

A workgroup bridge (WGB) provides a wireless infrastructure connection for Ethernet-enabled devices. Devices that do not have a wireless client adapter to connect to the wireless network can be connected to the WGB through the Ethernet port. The WGB associates to the root AP through the wireless interface. In this way, wired clients get access to the wireless network.

It is also possible to implement the WGB functionality with the use of a normal AP. You can configure APs as WGBs. In WGB mode, the unit associates to another AP as a client. The unit provides a network connection for the devices that are connected to its Ethernet port.

In the CPwE example, it provides wireless connectivity for a group of IACS devices: HMIs, I/O, controllers and drives that are attached to a local switch which in turn is attached to the wireless WGB. See Figure 2-9.
Wireless Design Considerations

Figure 2-9 Unified WGB Example

The WGB associates to an autonomous AP or LWAP on the network.

In the Unified CPwE WLAN, scaling out the WGB will include up to 19 devices behind a single WGB.

WGB Roaming Mode

In CPwE WLAN, WGB roaming is a requirement for the wireless equipment. In these use cases, the WGB scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, too many lost beacons or a high frame-loss percentage. These criteria can be selected in the WGB configuration. A WGB configured as a mobile station searches for a new parent association and roams to a new parent before it loses its current association. Figure 2-10 provides a WGB roaming use case example.
Wireless LAN Controller (WLC)

The Wireless LAN Controller (WLC) is a highly scalable and flexible platform that enables system-wide services for mission-critical wireless networking in medium- to large-sized industrial environments. The WLC should provide the following:

- Support for RF visibility and protection
- The ability to simultaneously manage up to 500 APs
- Sub-second stateful failover of all access points and clients from the primary to the hot-standby controller
- Larger mobility domain for more simultaneous client associations
- Intelligent RF control plane for self-configuration, self-healing and self-optimization
- Efficient roaming that improves application performance as required by IACS applications, whether within a Cell/Area Zone (Levels 0-2) or between multiple Cell/Area Zones
Wireless Design Considerations

- Full Control and Provisioning of Wireless Access Points (CAPWAP) access-point-to-controller encryption
- Support for rogue access point detection and denial-of-service attack detection

IACS Topologies in Unified WLANs

The topologies for deploying Unified WLAN with IACS applications are as follows:

- Fixed PAC to Wireless I/O
- Fixed PAC to Wireless PAC
- Intra-Cell Fast Roaming
- Plant-wide Fast Roaming

Fixed PAC to Wireless I/O

In this topology, a fixed PAC communicates with a number of wireless I/O devices behind WGBs in the same Cell/Area Zone. See Figure 2-11. This use case has the following characteristics:

- Each wireless connection 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
  - HMI client data (for instance, FactoryTalk View ME or SE)
- More than one EtherNet/IP I/O device can be connected to a WGB (in linear topology or via a switch).
- Large connection counts increase the packet rate in the channel and limit the scale of this topology.
Fixed PAC to Wireless PAC

In this topology, a fixed PAC communicates with one or more wireless PACs behind WGBs (peer-to-peer communication). See Figure 2-12. This use case has the following characteristics:

- Each wireless connection may support several types of data:
  - Produced/Consumed tags
  - Safety Produced/Consumed tags
  - Message instructions
  - HMI client data (FactoryTalk View SE client to server)
  - Maintenance and monitoring traffic (Studio 5000, RSLinx, etc.)
- IACS data can be aggregated into one or a few large Produced/Consumed tags that bring down the packet rate and increase the efficiency of wireless communications.
Each wireless PAC may have wired I/O or drives connected using a linear topology with embedded switch technology or an Ethernet switch. 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 wireless PAC.

Wired I/O and other devices can also be connected via the second Ethernet module in the PAC chassis. The advantage of the second Ethernet module on the wireless PAC is reduction of 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 web pages or configure the switch.

Intra-Cell/Area Zone Fast Roaming Topology

The roaming topology can be viewed as an extension of wired PAC to wireless PAC or I/O topologies described above. See Figure 2-13. This use case has the following characteristics:

- Wireless equipment moves within the same Cell/Area Zone during the operation.
- Coverage areas must overlap to allow for seamless roaming.
- Wireless infrastructure supports fast secure roaming with convergence delay that does not cause IACS application connection timeouts.
- LWAPs in centralized switching mode are used for fast roaming.
- Combining locally-switched (FlexConnect) and centrally-switched traffic on the same AP is not supported. If FlexConnect APs are used in a Cell/Area zone to support a non-roaming application, separate APs in centralized switching mode should be installed to support fast roaming, or the existing APs should be converted to the centralized mode.

Unified WLAN Architecture provides the best solution for the following reasons:

- Proven and tested fast roaming mechanisms
- Better support for IACS application coverage with large number of APs
Plant-wide Cell/Area Zone Fast-Roaming

Another important use case for plant-floor wireless communication is Inter-Cell/Area Zone Plant-wide roaming shared equipment:

- Mobile shared equipment such as overhead cranes for moving large objects between Cells/Area zones during the IACS process.

Mobile shared equipment such as overhead cranes, which can contain PACs, I/O, sensors, motors, and so on, can communicate with the AP using either 2.4 GHz or 5 GHz radio. It should operate within specifically designated SSID / VLAN which spans multiple zones, separate from the Cell/Area Zone SSID / VLANs mentioned in the above section. This traffic will flow from the overhead crane to the controller through the use of a CAPWAP tunnel as displayed in Figure 2-14. This type of traffic should be prioritized based upon the Industrial protocol required for operation for its corresponding QoS configuration.
Unified WLAN Requirements

This section describes the United WLAN requirements.

Scale, Configuration and Resiliency

This version of the CPwE solution architecture focuses on basic wireless concepts. Rather than focusing on full-range and scalability testing, this solution architecture focuses on defining and testing core concepts that are applicable to a full range of IACS application sizes.

Scaling of the cell/area zone within a wireless environment, the number of devices supported should adhere to the requirements shown in Table 2-9:

Table 2-9  Unified WLAN Equipment Requirements

<table>
<thead>
<tr>
<th>Node Type</th>
<th>Function</th>
<th>Number</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Point to support Cell/Area</td>
<td>Intra-Cell static WGB traffic</td>
<td>1 minimum</td>
<td>Two are required for redundant AP support</td>
</tr>
<tr>
<td>Static WGB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Point to support Roaming</td>
<td>Intra-Cell Fast-Roaming, Plant-wide Equipment</td>
<td>2 minimum</td>
<td>Required for roaming connectivity and redundancy</td>
</tr>
<tr>
<td>Roaming</td>
<td>Fast-Roaming</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workgroup Bridge (WGB)</td>
<td>Maximum of 10 associated to 1 AP</td>
<td></td>
<td>Static and Roaming</td>
</tr>
<tr>
<td>Ethernet Switches</td>
<td>Behind a Workgroup Bridge</td>
<td>1 maximum</td>
<td>Static and Roaming</td>
</tr>
<tr>
<td>Clients</td>
<td>Clients attached to switches behind a Workgroup Bridge</td>
<td>19 maximum</td>
<td>Static and Roaming</td>
</tr>
</tbody>
</table>
SSID Requirements

Depending on the use case (static, intra-cell or plant-wide roaming), up to three SSIDs may be required to provide full coverage of the requirements. The use of three SSIDs provides for segmentation of traffic based on function. Table 2-10 provides a breakdown of the SSID by function and SSID name.

<table>
<thead>
<tr>
<th>Function</th>
<th>Example SSID Name</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra-Cell Static WGB Connectivity</td>
<td>StaticWGB</td>
<td>Locally Switches Traffic</td>
</tr>
<tr>
<td>Intra-Cell Fast-Roaming Connectivity</td>
<td>IntraFast</td>
<td>CAPWAP for Centrally Switched</td>
</tr>
<tr>
<td>Plant-wide Fast-Roaming Connectivity</td>
<td>PWFast</td>
<td>CAPWAP for Centrally Switched</td>
</tr>
</tbody>
</table>

Network Resiliency and Redundancy

High availability is a major requirement for any IACS application. In the Unified WLAN architecture, high availability can be achieved by using redundant network infrastructure devices and topologies, providing redundant wireless coverage and by protecting the wireless spectrum from interference and unauthorized transmissions.

The following are design recommendations for high availability in the Unified WLAN:

- Use resilient network topologies and protocols in the wired infrastructure that satisfy the high availability requirements of the wireless IACS application, for example, redundant star and ring topologies for network switches, REP and EtherChannel.
- Use redundant network switches for the distribution layer, such as the Cisco Catalyst® 3750X, which utilizes StackWise technology.
- Use spectrum analysis tools to proactively detect and mitigate sources of interference and unauthorized transmissions. Create and enforce a wireless spectrum policy at the site.
- Monitor and regulate the amount of data that is transmitted over the wireless channel, particularly maintenance and monitoring traffic.
- Use overlapping redundant AP coverage for critical applications to minimize downtime. This configuration is discussed in the next section.

WLC Redundancy and Resiliency

The WLC provides redundancy through the use of an active / hot-standby configuration. To provide the backup/failure performance, it is recommended that the controller be connected via a 2x GE port aggregate link (EtherChannel) which provides physical connectivity between the WLC pair.

Configuration of the redundant wireless LAN controllers is accomplished through use of an aggregate link pair directly connecting the controllers.

Note

When operating an IACS network utilizing a Unified Wireless architecture, due to security functionality of the WLC, the system will initiate a re-authentication process every 24 hours. This automated re-authentication process will force a sub-second network re-convergence for the wireless-attached devices, followed by an automated self-recovery. This re-authentication process could result in IACS application timeouts.
Wireless Design Considerations

Note

For IACS applications that require 24 hour continuous operation, Cisco and Rockwell Automation recommend Autonomous WLAN architecture at this time.

Wireless Access Point Redundancy

Wireless Access Point redundancy in a Unified Access deployment is provided by installing multiple APs that provide overlapping coverage of all required areas within the Cell/Area Zone Level 0 - 2. Based on RSSI, the WGB will associate with the best connection within the Cell/Area Zone.

Unified WLAN Security

This section describes Unified WLAN Security requirements.

Fast Roaming Security Requirements

Fast roaming requires using Cisco Centralized Key Management (CCKM) since PSK authentication cannot provide fast roaming. EAP-TLS is the recommended authentication method for plant-wide WLAN security. EAP-TLS requires RADIUS and certificate services deployed in the infrastructure. The RADIUS server will be located in the Industrial Zone Level 3.

Note

Other security methods include local RADIUS authentication on the WLC and using username/password credentials for WGBs instead of certificates. These methods have not been considered for the CPwE WLAN guide.

In CPwE, the use of local EAP certificates is supported on the controller. When using Stratix 5100 as a WGB, importing the vendor-specific certificate must be completed prior to implementing the Stratix 5100 in the solution.

Static/Nomadic Security Requirements

It is recommended in the Unified WLAN solution that the non-roaming applications use the same security configuration as fast roaming applications (i.e., EAP-TLS). This simplifies deployment and removes confusion over which devices and SSIDs are configured for which security mode.

Unified WLAN QoS

This section describes QoS parameters for Unified WLAN.

Wireless QoS Parameters

In a Unified wireless deployment, QoS settings for the LWAP is configured on the WLC and pushed down to the LWAPs for consistency and ease of configuration. The default wireless QoS parameters in Cisco APs are optimized for applications that are most sensitive to latency, jitter and packet loss, such as voice and video or as in the CPwE context, IACS applications.
The four levels of QoS are described in Table 2-11:

Table 2-11  Unified Wireless QoS Settings

<table>
<thead>
<tr>
<th>QoS Levels</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platinum (Voice)</td>
<td>Ensures a high quality of service over wireless time sensitive applications</td>
</tr>
<tr>
<td>Gold (Video)</td>
<td>Supports high quality of service for applications that are not time sensitive, but require better than average/normal performance</td>
</tr>
<tr>
<td>Silver (Best Effort)</td>
<td>Supports best effort traffic, such as normal user traffic</td>
</tr>
<tr>
<td>Bronze (Background)</td>
<td>Provides lowest bandwidth capability for traffic such as guest services</td>
</tr>
</tbody>
</table>

- It is recommended to use the Platinum QoS Level for all WLANs as this provides the best performance. The WLAN QoS level sets the maximum threshold for the data traversing the WLC. The IACS traffic will be assigned the appropriate wireless QoS category (Best Effort, Video, Voice) based on the QoS marking in the data packets.
- It is recommended to configure "Voice and Video Optimized" QoS profile on the WLC because it provides the optimal configuration of the radio parameters for the IACS traffic.