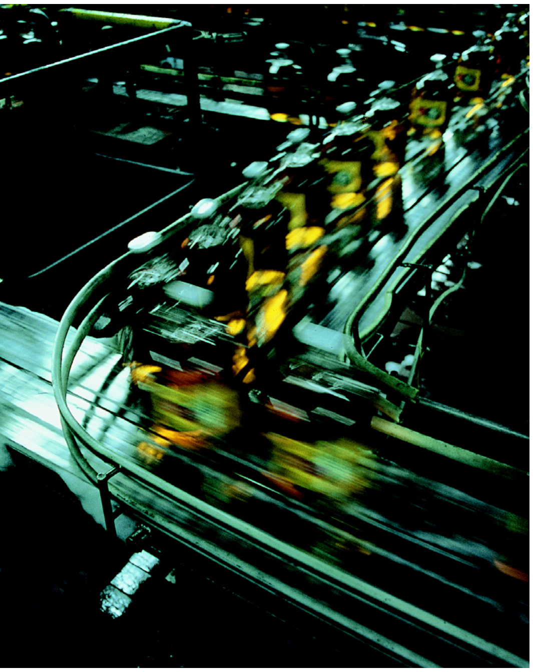


Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture

Design and Implementation Guide

November 2014

Cisco Validated Design

Document Reference Number: ENET-TD006A-EN-P

Preface

Converged Plantwide Ethernet (CPwE) is a joint system development effort between Rockwell Automation and Cisco Systems. The CPwE-WLAN design guide builds on the existing CPwE system by introducing Wireless LAN network capabilities, with emphasis on equipment connectivity. This document assumes the reader is familiar with CPwE. For more information, please refer to:

- Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
- Cisco site: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG.html

Document Organization

The CPwE WLAN Design Guide contains the following chapters and appendices:

Chapter or Appendix	Description
Chapter 1, "CPwE-WLAN System Introduction"	Provides and overview of CPwE, key concepts, system features, IACS equipment use cases, Autonomous and Unified CPwE WLAN architectures, and CPwE WLAN IACS topologies.
Chapter 2, "System Design Considerations"	Describes technology overview, how to apply wireless in IACS applications, and considerations for wireless design.
Chapter 3, "Configuring the Infrastructure"	Describes how to configure WLAN infrastructure in the CPwE system based on the design considerations of the previous chapters.
Chapter 4, "Maintaining the Infrastructure"	Describes maintenance and troubleshooting for Autonomous and Unified WLAN, and replacement of Unified Access Points, Workgroup Bridges, and Wireless LAN Controllers.
Chapter 5, "Testing the Architecture"	Describes testing Autonomous and Unified WLAN.
Appendix A, "References"	References for the CPwE architecture.
Appendix B, "CLI Configuration Examples"	Includes various configuration examples for Autonomous and Unified WLAN.

Chapter or Appendix	Description
Appendix C, "Server Infrastructure Configuration"	Includes steps for setting up DHCP, DNS, Active Directory, Root-CA and RADIUS Servers.
Appendix D, "Packet Rate Calculation Examples"	Gives two examples for quickly estimating the packet rate for the application using one of the common topologies (Fixed PAC to Wireless I/O and Fixed PAC to Wireless PAC).
Appendix E, "Test Hardware and Software"	List of hardware and software components used in testing.

CHAPTER 1

CPwE-WLAN System Introduction

Plant-wide architectures increasingly use IEEE 802.11™ 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 plant-wide WLAN requires thoughtful planning and design as well as periodic monitoring to meet expectations for bandwidth, throughput, reliability and security.

Converged Plantwide Ethernet (CPwE) WLAN for IACS applications is brought to market through a strategic alliance between Cisco Systems and Rockwell Automation. CPwE WLAN details an architecture to help with the successful 802.11 WLAN design and implementation that meets the performance requirements of IACS applications.

CPwE is the underlying architecture that provides standard network services to the applications, devices and equipment found in modern IACS applications. The CPwE architecture provides design and implementation guidance to help achieve the real-time communication, reliability and resiliency requirements of the IACS.

Converged Plantwide Ethernet WLAN

The CPwE WLAN architecture is tailored to address 802.11 wireless networking of IACS equipment and devices within the Industrial Zone of the plant. Both Unified (centralized) and Autonomous (stand-alone) WLAN architectures for IACS equipment use cases have been individually validated, allowing for architectural selection practical to a small or large-scale plant-wide deployment. The abilities of both Unified and Autonomous WLANs are defined to integrate the IACS into the broader plant-wide environment.

This CPwE WLAN Cisco® Validated Design (CVD) outlines the key requirements and design considerations to help successful design and deployment of IACS 802.11 wireless networking within plant-wide architectures:

- CPwE WLAN IACS Equipment Use Case Overview
- Review of Industrial Wireless Technologies
- Radio Frequency Design Considerations
- Autonomous WLAN Architecture Design Considerations
- Unified WLAN Architecture Design Considerations

- Important steps and considerations for WLAN implementation and configuration recommendations with IACS applications
- Maintaining and Troubleshooting the CPwE WLAN
- CPwE WLAN Test Results

CPwE WLAN IACS Equipment Use Cases

Wireless IACS equipment can be characterized by the type of mobility and operational requirements when relocating within the plant-wide architecture. Wireless IACS equipment may stay within a single Cell/Area Zone and remain associated to a single access point (AP) until powered down or disconnected. Wireless equipment may roam across the Industrial Zone and associate to multiple APs while remaining operational.

- Fixed position devices in the CPwE WLAN architecture have a permanent operational location, also known as "static." Fixed position wireless is an alternative to a wired connection for hard-to-reach and remote locations where cabling is too expensive or impossible to install. Usage areas include process control, machine condition monitoring, fixed environmental monitoring and energy industries. In the manufacturing environment, a common use case is a stand-alone OEM machine or skid that needs to be integrated into a plant-wide architecture over a wireless link.
- Nomadic equipment stays in place while operating, then moves to a new location in the shutdown state. After relocation, a new wireless connection needs to be established. Common examples are process skids, storage tanks, reactors and portable manufacturing equipment.
- Mobile (non-roaming) equipment changes position during an operation, remaining in the same coverage area within a Cell/Area Zone. Common examples are rotary platforms and turntables, Automated Storage and Retrieval Systems (ASRS), assembly systems with tracks and overhead cranes. These applications may require rapid changes in position and orientation of the wireless client relative to the AP.
- Mobile (roaming) equipment changes position during an operation by roaming across multiple coverage areas within the Industrial Zone. Common examples are automatic guided vehicles (AGVs), large ASRS, overhead cranes and train cars.

Autonomous and Unified CPwE WLAN Architectures

Two different architectures are validated in CPwE WLAN: Autonomous WLAN and Unified WLAN. With two differing architectures, CPwE WLAN allows users to make an informed architecture selection that meets both business and technical needs for scalability within the plant-wide architecture.

The benefits of the CPwE Autonomous WLAN architecture include:

- A lower initial hardware cost
- Simplified design and deployment
- More granular control of Quality of Service (QoS) for prioritization of critical IACS application network traffic

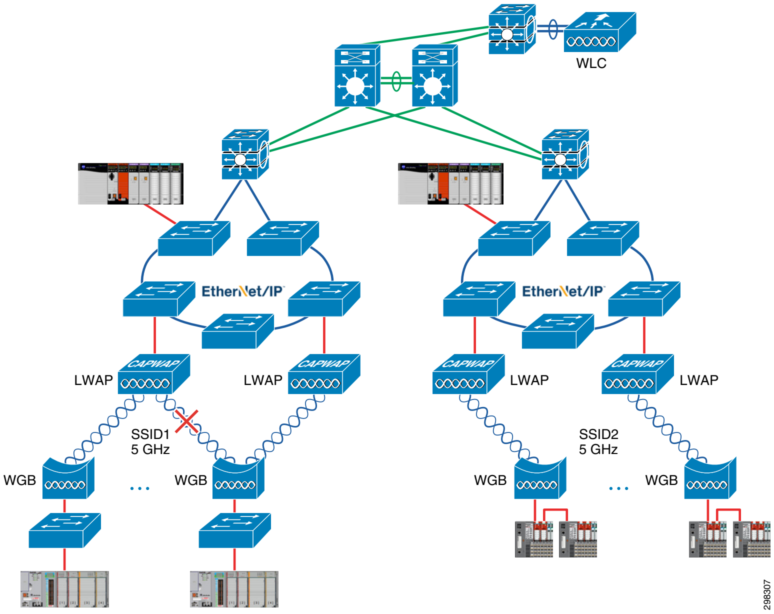
The benefits of the CPwE Unified WLAN architecture include:

- Plant-wide scalability
- Support for plant-wide mobility

- Advanced optimization and recovery mechanisms
- Enhanced security

The Unified WLAN architecture, as illustrated in Figure 1-1, has the ability to address large-scale plant-wide 802.11 wireless needs. The Unified Access architecture allows for centralized management and control of the wireless access points distributed throughout the plant. By utilizing a Wireless LAN Controller (WLC) and Lightweight Access Points (LWAP), a centralized management model is created, thus introducing security and self-healing mechanisms to the wireless architecture. The Unified WLAN architecture also introduces foundational services, including intrusion prevention and wireless guest access, for better control over devices seeking to connect to the WLAN.

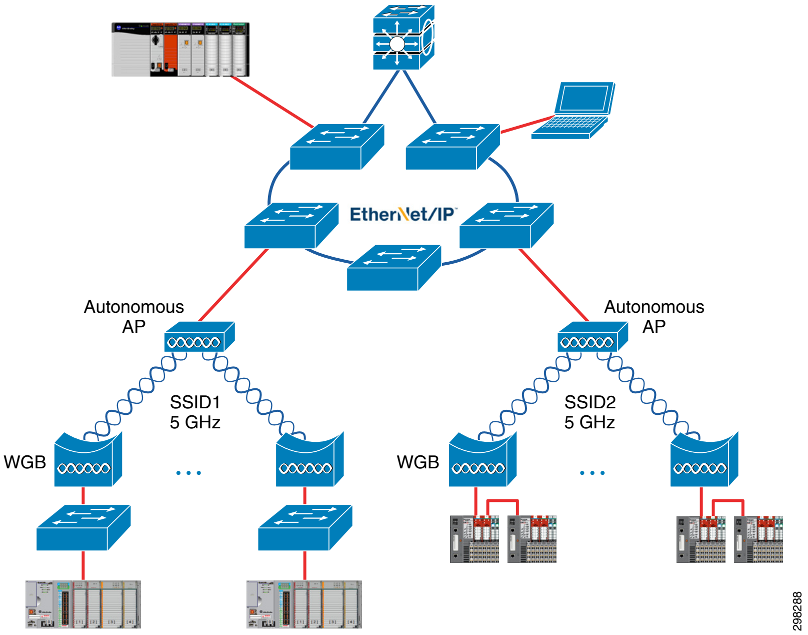
Figure 1-1 Unified WLAN



Autonomous WLAN architectures, as illustrated in Figure 1-2, do not utilize the centralized management structure found in the Unified WLAN. Each Access Point (AP) functions as its own stand-alone device, as an AP or Workgroup Bridge (WGB), without the need for a WLC. The Autonomous WLAN architecture is therefore less costly to implement, thus may be more suitable for smaller IACS applications, such as an OEM machine or skid. Autonomous WLAN APs utilized in the CPwE WLAN architecture may be later repurposed to the Unified Access architecture with additional hardware under the following conditions:

- If deployment needs change or large scale plant-wide growth requires an architectural transitioning (not covered in this CVD)
- If the OEM machine/skid is integrated into a plant-wide architecture (not covered in this CVD)

Figure 1-2 Autonomous WLAN



CPwE WLAN IACS Topologies

Several IACS WLAN topologies were tested and validated for both the Autonomous and Unified WLAN architectures. They addressed the wireless equipment use cases of fixed, nomadic, mobile (non roaming) and mobile (roaming).

Autonomous WLAN topologies include:

- Fixed Programmable Automation Controller (PAC) to Wireless I/O—In this topology, a fixed PAC in the wired infrastructure controls a number of I/O devices behind a wireless client—e.g., workgroup bridge (WGB).
- Fixed PAC to Wireless PAC—In this topology, a fixed PAC in the wired infrastructure communicates to a number of PACs behind WGBs.

Refer to IACS Topologies in Autonomous WLANs, page 2-15 for details.

Unified WLAN topologies include:

- Fixed PAC to Wireless I/O topology (non roaming)
- Fixed PAC to Wireless PAC topology (non roaming)
- Intra-Cell Fast Roaming—In this topology, wireless equipment roams between APs within the same Cell/Area zone
- Plant-wide Fast Roaming—In this topology, wireless equipment roams between Cell/Area zones during the operation

Refer to IACS Topologies in Unified WLANs, page 2-28 for details.

Note This release of the CPwE architecture focuses on EtherNet/IP™, which is driven by the ODVA Common Industrial Protocol (CIP). Refer to the IACS Communication Protocols section of the CPwE Design and Implementation Guide.

- Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
- Cisco site: http://www.cisco.com/en/US/docs/solutions/Verticals/CPwE/CPwE_DIG.html

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

Table 2-1 Industrial Wireless Applications and Technologies

Type of Industrial Wireless Application	Wireless Technology	Network and Hardware Characteristics	Typical Throughput	Sensitive to Latency and Packet Loss
Supervisory Control **Peer to Peer Control** **Distributed I/O Control** **Safety Control**	802.11a/g/n (CPwE WLAN)	Point-to-multipoint topology; May require roaming	Moderate to high	Yes
Mobile Operator (HMI)	802.11a/g/n (CPwE WLAN)	Integrated wireless adapters Site-wide roaming	Moderate	No
Long Haul SCADA **Remote site connectivity**	802.11a/g Cellular 3G / LTE WiMAX Proprietary FHSS	Outdoor point-to-point, point-to-multipoint, or mesh topology; Small or moderate number of nodes	Low to moderate	No
Process Instrumentation **Wireless Sensors** **Condition Based Monitoring**	ISA-100.11a WirelessHART® ZigBee® Bluetooth®	Mesh topology with large number of nodes Self-healing network, auto-provisioning Low cost and power consumption	Low	No

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)

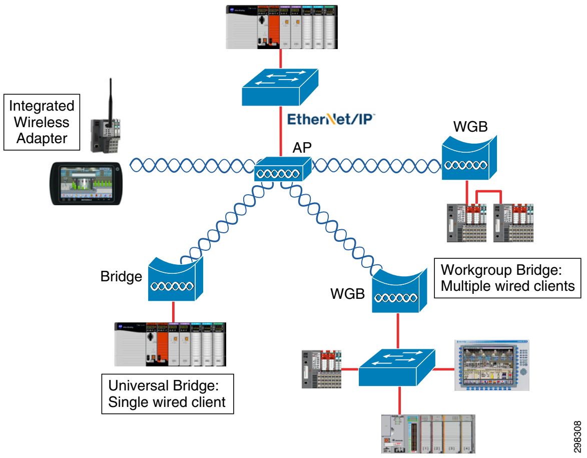
The ability to connect several wired clients with a single wireless bridge solves many of the previously mentioned problems. This capability is implemented in a workgroup bridge (WGB) mode, which is a type of operation supported by Stratix™ 5100 and Cisco autonomous APs.

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


Integrated Wireless Adapter
EtherNet/IP
AP
WGB
Bridge
WGB
Workgroup Bridge: Multiple wired clients
Universal Bridge: Single wired client
298308

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

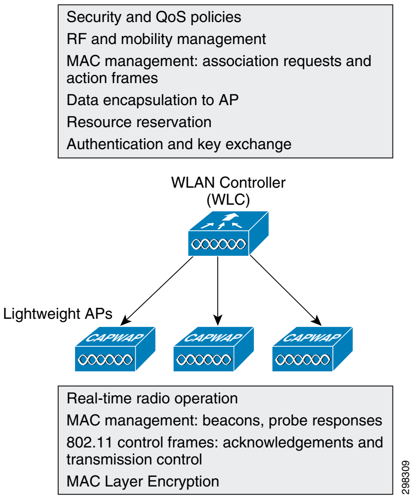
The Unified WLAN architecture is a Cisco solution for large scale plant-wide deployments of wireless infrastructure. In the Unified architecture, the WLAN functionality is split between lightweight access points (LWAP) and wireless LAN controllers (WLC). Most WLAN control and management functions are 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

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

Figure 2-2 Unified WLAN Functions


Security and QoS policies
RF and mobility management
MAC management: association requests and action frames
Data encapsulation to AP
Resource reservation
Authentication and key exchange
WLAN Controller (WLC)
Lightweight APs
CAPWAP
CAPWAP
CAPWAP
Real-time radio operation
MAC management: beacons, probe responses
802.11 control frames: acknowledgements and transmission control
MAC Layer Encryption
298309

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.

Note 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.

Note 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

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

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

IACS Traffic Type	CIP Standard	Use with Wireless	Constraints
Information and diagnostics, process control	CIP Class 3 (HMI)	Yes	<20% of total packet rate if combined with CIP Class 1 Standard and Safety traffic
Peer-to-peer Messaging	CIP Class 3 (MSG)	Yes	See above
Peer-to-peer Control	CIP Class 1 Produced/Consumed	Yes	Application should tolerate higher latency and jitter
I/O Control	CIP Class 1 I/O	Yes	See above
Safety Control	CIP Safety	Yes	Very fast safety reaction times may not be supported
Time Synchronization	CIP Sync	Limited	Limited accuracy, may be suitable for SOE and event logging applications
Motion Control	CIP Motion	No	Not feasible with CIP Motion drives due to higher latency and jitter of wireless media and insufficient CIP Sync accuracy

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
  - 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:
  http://www.rockwellautomation.com/rockwellautomation/products-technologies/integrated-architecture/tools/overview.page?

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 2-11).
- 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

Traffic Type	Unicast Support / ControlLogix Version
Standard I/O	v18 (ControlLogix Redundancy - multicast only)
Standard Produced/Consumed	v16 (ControlLogix Redundancy - multicast only for consumed tags)
Safety I/O	v20
Safety Produced/Consumed	v19
CIP Sync	Multicast only (as of v24)

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

Parameter	Value
CRTL	4 x RPI, ≥ 60 ms
RPI	≥ 15 ms
System Reaction Time (SRT) - Worst Case No Fault	≥ 200 ms (≥ 130 ms depending on the system size and RPIs)
System Reaction Time (SRT) - Worst Case Single Fault	≥ 360 ms (≥ 200 ms depending on the system size and RPIs)

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

- http://www.rockwellautomation.com/rockwellautomation/products-technologies/integrated-architecture/tools/overview.page?#/tab5

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 2-6 Site Survey Parameters

Parameter	Recommended Value
Received Signal Strength Indicator (RSSI)	Min -67 dBm
Signal-to-Noise Ratio (SNR)	Min 25 dB
Supported data rate	54 Mbps

- 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):

- Fixed Position
- Nomadic (Non-operational Relocation)
- Mobile with No Roaming

Note Autonomous WLAN architectures with roaming wireless equipment are not considered in this guide. Cisco Unified WLAN architecture is recommended to support fast roaming.

IACS Topologies in Autonomous WLANs

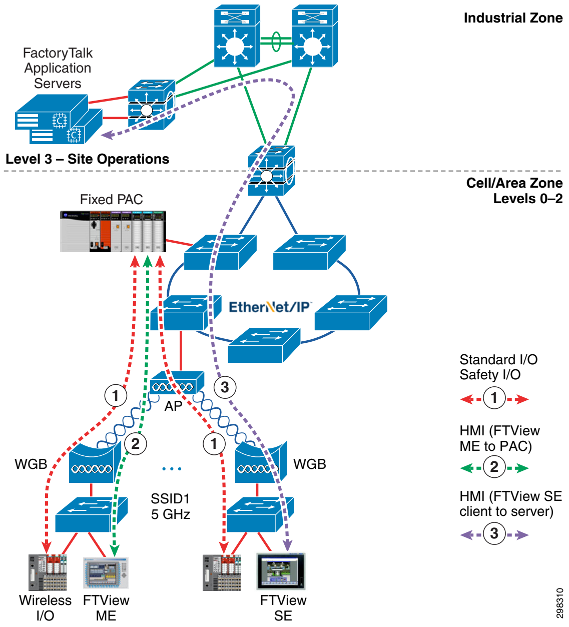
The most common topologies for wireless IACS equipment in Autonomous WLANs are discussed in the following sections.

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).

Figure 2-3 Fixed PAC to Wireless I/O Topology in Autonomous WLAN



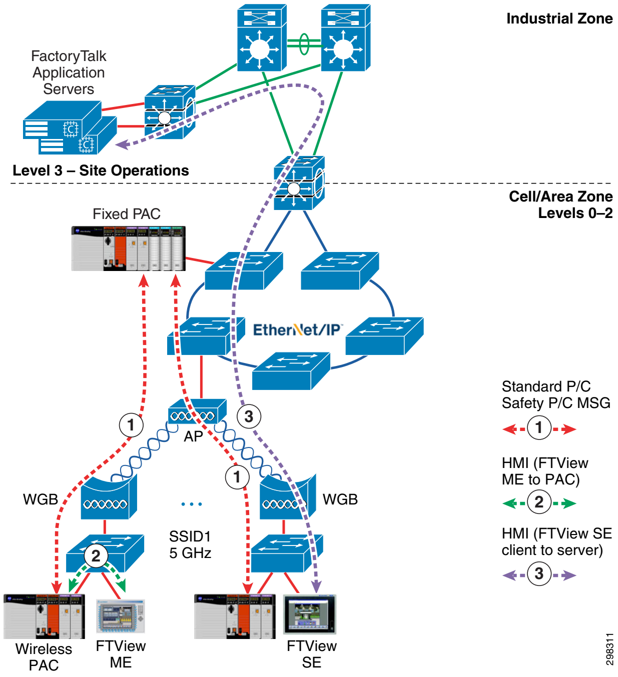
Fixed PAC to Wireless PAC Topology

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.

Figure 2-4 Fixed PAC to Wireless PAC Topology in Autonomous WLAN


Industrial Zone
FactoryTalk Application Servers
Level 3 – Site Operations
Cell/Area Zone Levels 0–2
Fixed PAC
EtherNet/IP
Standard P/C Safety P/C MSG
1
HMI (FTView ME to PAC)
2
HMI (FTView SE client to server)
3
AP
1
3
1
WGB
WGB
SSID1 5 GHz
2
Wireless PAC
FTView ME
FTView SE
298311

Wireless to Wireless Communication

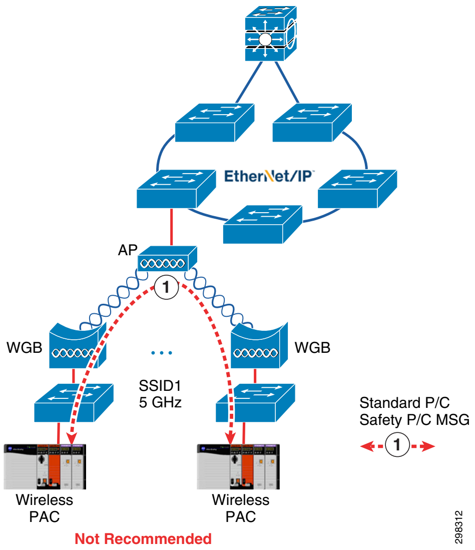
In certain applications, a wireless PAC may need to send data to another wireless PAC or a wireless I/O connected to the same AP. An example may be machine interlocking, safety status and listen-only I/O connections (see Figure 2-5).

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.

Figure 2-5 Wireless-to-Wireless Communication



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

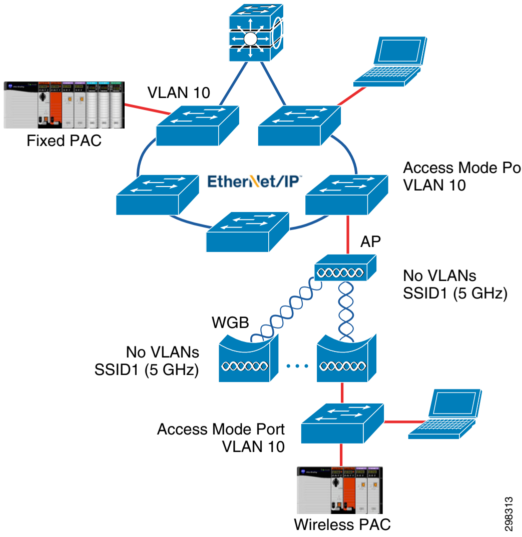
The most common case is when a single SSID is used for all traffic in the Autonomous WLAN. The data is assigned to one VLAN in the wired infrastructure (see Figure 2-6).

- 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.

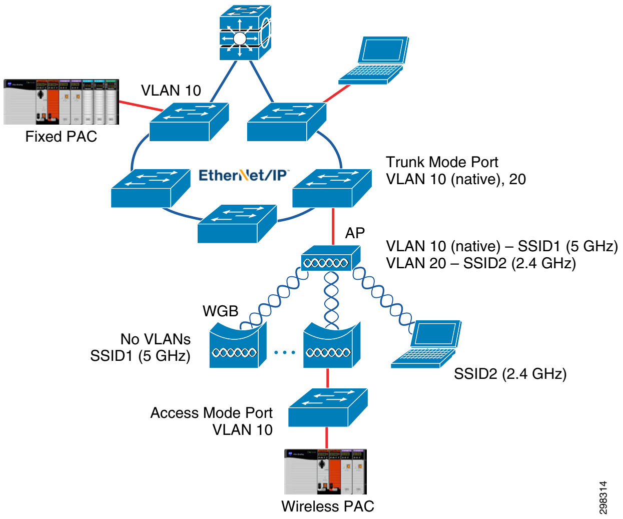
The following are recommendations for the multiple VLAN / SSID architecture implemented on a single autonomous AP (see Figure 2-7):

- 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.

Note 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

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

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.

- 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

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

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.
  - 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.

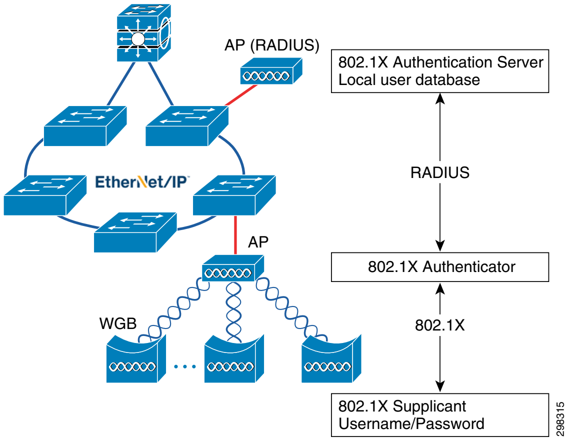
802.1X/EAP authentication method provides strong security with granular access control based on individual user credentials. However, the 802.1X method requires additional components to be available in the Autonomous WLAN:

- 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.

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.

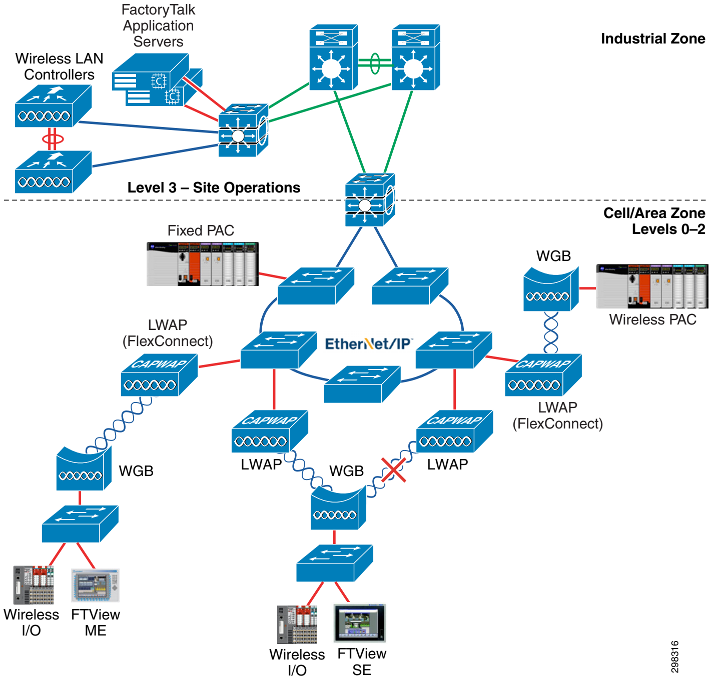
Workgroup Bridge (WGB)

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.

Figure 2-9 Unified WGB Example



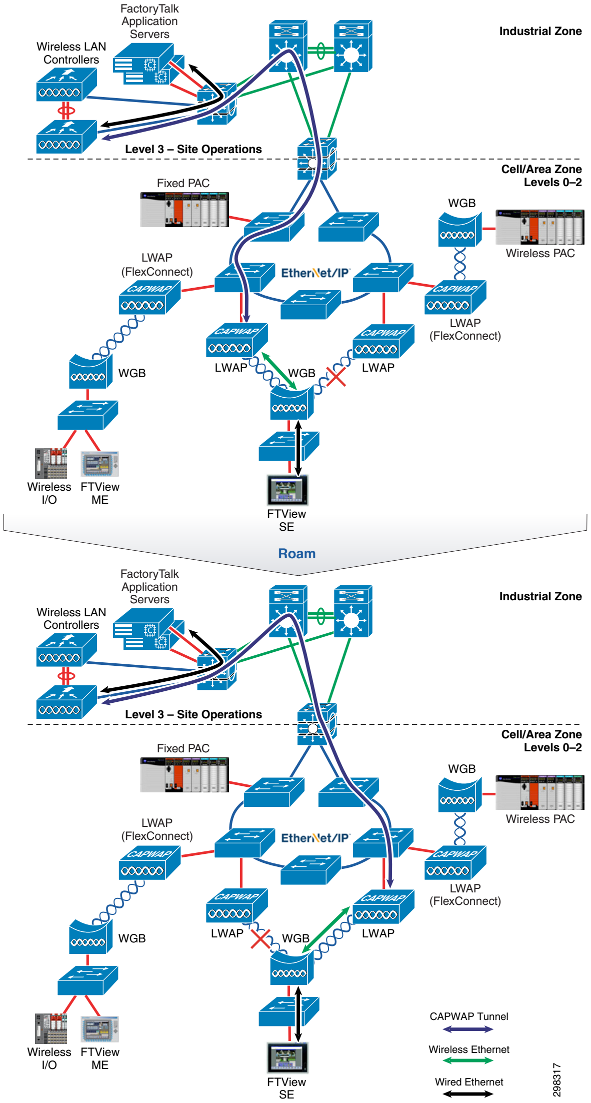
The WGB associates to an autonomous AP or LWAP on the network.

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.

Figure 2-10 WGB Roaming 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

- 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:

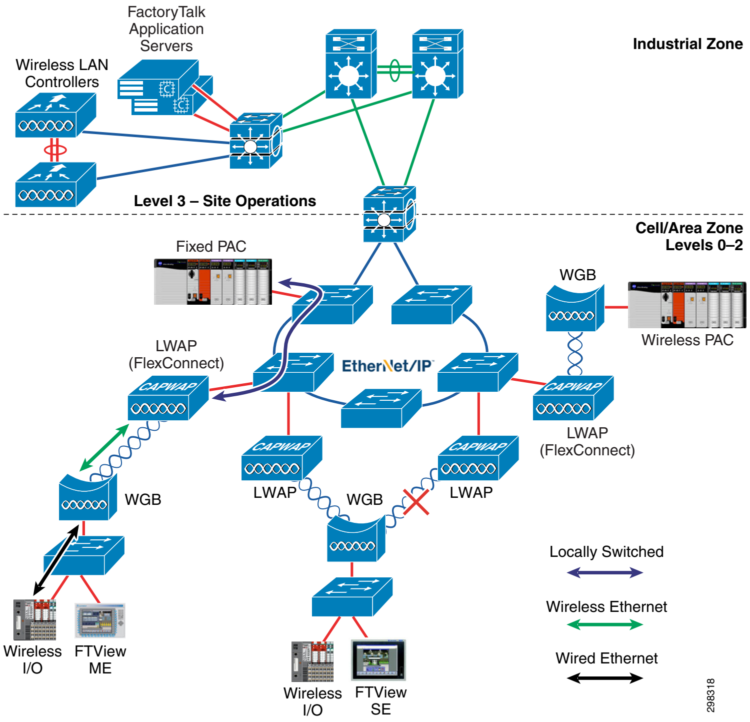
- Fixed PAC to Wireless I/O
- Fixed PAC to Wireless PAC
- Intra-Cell Fast Roaming
- Plant-wide Fast Roaming

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.

Figure 2-11 Fixed PAC to Wireless I/O in Unified WLAN

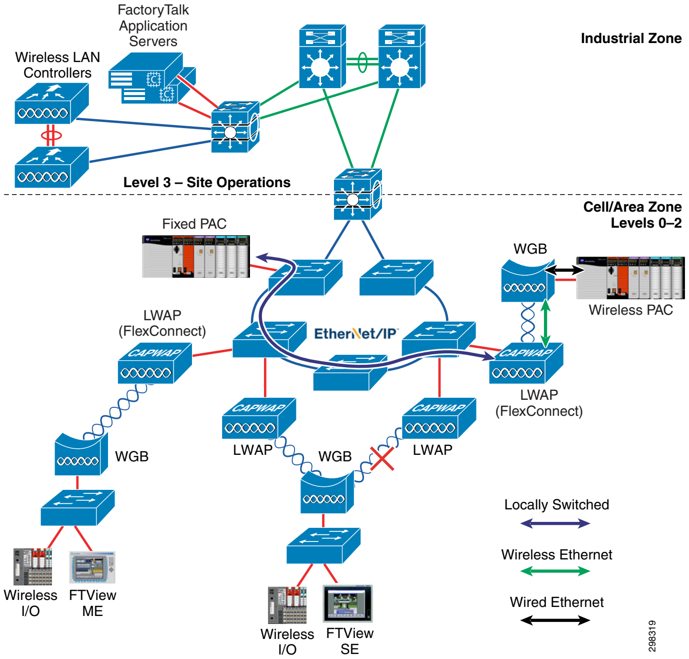


Fixed PAC to Wireless PAC

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.

Figure 2-12 Fixed PAC to Wireless PAC in Unified WLAN



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

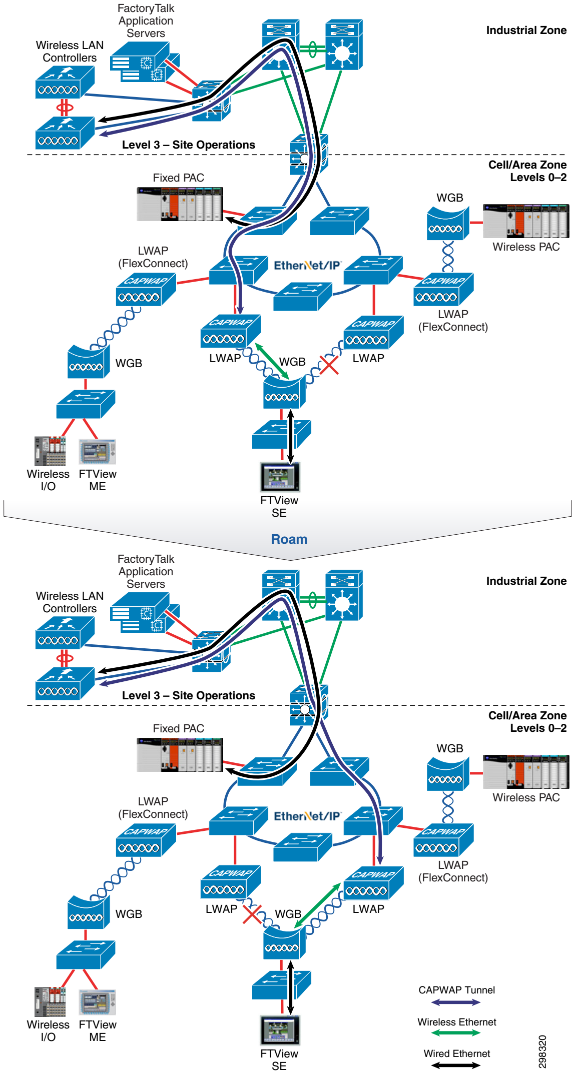
The roaming topology can be viewed as an extension of wired PAC to wireless PAC or I/O topologies described above. See Figure 2-13. This use case has the following characteristics:

- 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

Figure 2-13 Intra-Cell/Area Zone Fast Roaming in Unified WLAN



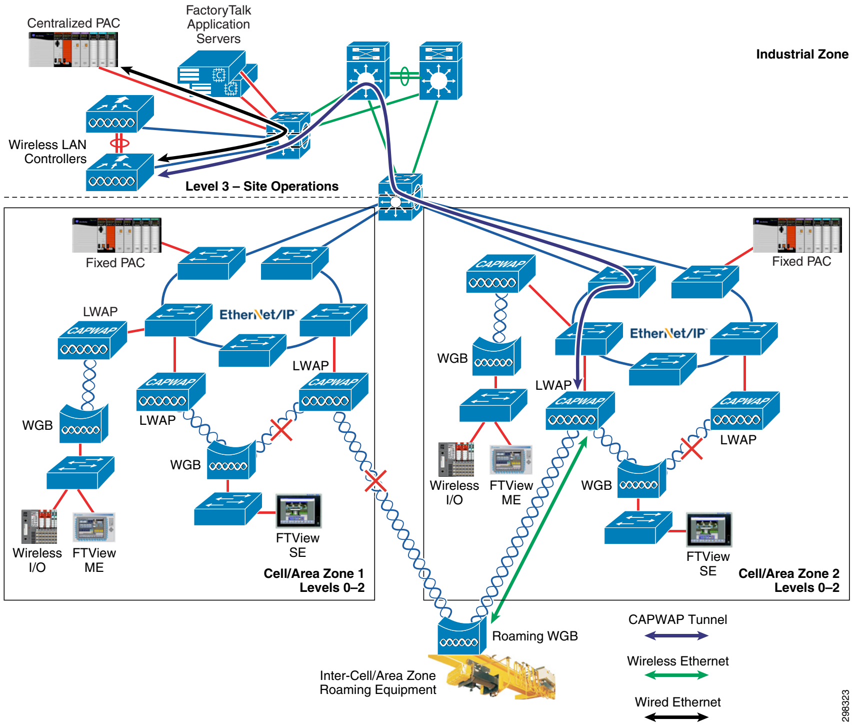
Plant-wide Cell/Area Zone Fast-Roaming

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.

Figure 2-14 Plant-wide Fast Roaming Architecture



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

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

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 2-10 SSID Requirements

Function	Example SSID Name	Notes
Intra-Cell Static WGB Connectivity	StaticWGB	Locally Switches Traffic
Intra-Cell Fast-Roaming Connectivity	IntraFast	CAPWAP for Centrally Switched
Plant-wide Fast-Roaming Connectivity	PWFast	CAPWAP for Centrally Switched

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.

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

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

- 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.

CHAPTER 3

Configuring the Infrastructure

This chapter describes how to configure WLAN infrastructure in the CPwE system based on the design considerations of the previous chapters. It covers the configuration of the Autonomous and Unified WLAN components, including APs, WLC, and switches. The included configurations have been validated during the testing effort.

Autonomous WLAN Configuration

This section describes validated configurations for the Stratix 5100 APs and IE switches that implement an Autonomous WLAN for wireless IACS equipment in the Cell/Area Zone.

The following configuration steps using the Device Manager and the CLI are covered in this section:

- Initial AP and WGB configuration
- VLAN configuration
- Security configuration
- QoS configuration
- RF configuration
- Switch configuration

Examples of the CLI configurations can also be found in Autonomous WLAN CLI Examples, page B-1.

Note This document does not provide a complete configuration guide for the Stratix 5100 and does not cover all possible scenarios where this product may be used. For more information, refer to the Stratix 5100 user manual at the following URL:

- http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um006_-en-p.pdf

Initial AP Configuration

The factory default configuration for the Stratix 5100 has the following:

- Management interface set to DHCP (no default IP address)
- No default SSID and radio interfaces are disabled
- Channel and transmit power settings are not set
- Custom QoS policy is applied to radio interfaces
- QoS and RF parameters are optimized for EtherNet/IP traffic
- HTTP and HTTPS are enabled; Telnet and SSH are disabled
- CIP is enabled on the management interface (read-only)

The following steps describe the initial AP configuration:

Step 1 Configure an IP address on the AP management interface by using one of these methods:

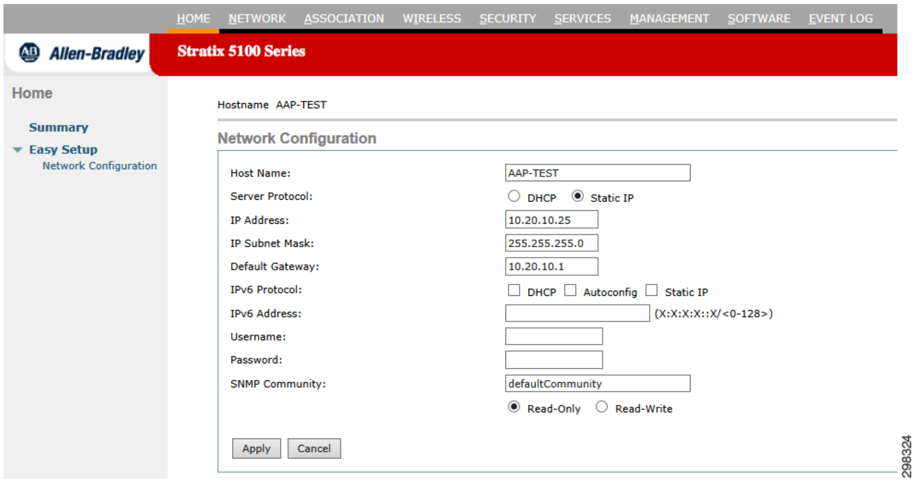
- Use a DHCP server in the infrastructure to automatically configure an IP address. The DHCP server can be configured on the access or distribution switch, or be already present in the network. To determine the assigned address, use the MAC address of the Ethernet port provided on the Stratix 5100 label.
- Use the BOOTP-DHCP Server Tool from Rockwell Automation on a PC connected directly to the AP Ethernet port.
- Configure a static IP address using the console port and CLI:

```
configure terminal
interface BVI1
ip address <ADDRESS> <MASK>
```

Step 2 Use the *Device Manager > Easy Setup > Network Configuration* page to configure basic parameters: host name, static IP address, subnet mask and default gateway as shown in Figure 3-1.

Do not change the password here (use *Security > Admin Access* page instead).

Figure 3-1 Easy Setup—Network Configuration



Hostname AAP-TEST

Network Configuration

Host Name:	AAP-TEST
Server Protocol:	○ DHCP ● Static IP
IP Address:	10.20.10.25
IP Subnet Mask:	255.255.255.0
Default Gateway:	10.20.10.1
IPv6 Protocol:	□ DHCP □ Autoconfig □ Static IP
IPv6 Address:	(X:X:X:X::X/<0-128>)
Username:	
Password:	
SNMP Community:	defaultCommunity ● Read-Only ○ Read-Write

Step 3 Configure basic parameters for the 5 GHz or 2.4 GHz radio in the *Radio Configuration* section. See Figure 3-2.

a. Configure the SSID name. It is recommended to have no more than one SSID per radio. Do not check *Broadcast SSID in Beacon*.

b. Use the *No VLAN* configuration for the initial setup. If required, VLANs can be configured and linked to SSIDs without using the Easy Setup.

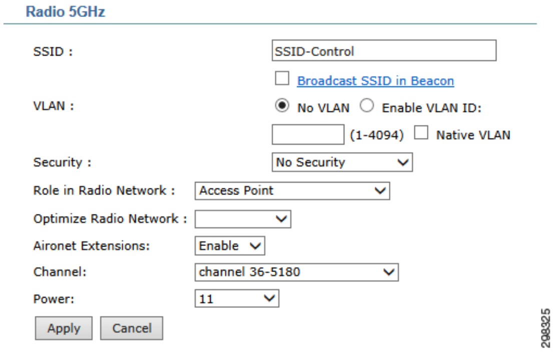
c. Do not configure security at this point (use the *No Security* option). It is recommended to use the *Security* page to configure authentication and encryption parameters.

d. Configure the role in the radio network: *Access Point* or *Workgroup Bridge*. If the WGB role is configured, use only 5 GHz radio for that role.

e. Configure static channel (AP role only) and power level on the radio using the site survey results and channel allocation scheme. It is recommended not to use the *Dynamic Frequency Selection*.

Note The Easy Setup page has certain restrictions and limited number of options to configure. It cannot be used for complete provisioning of the device in the WLAN. Refer to the Stratix 5100 User Manuals for details.

Figure 3-2 Easy Setup—Radio Configuration



Radio 5GHz

SSID : SSID-Control

□ Broadcast SSID in Beacon

VLAN : ● No VLAN ○ Enable VLAN ID:

(1-4094) □ Native VLAN

Security : No Security

Role in Radio Network : Access Point

Optimize Radio Network :

Aironet Extensions: Enable

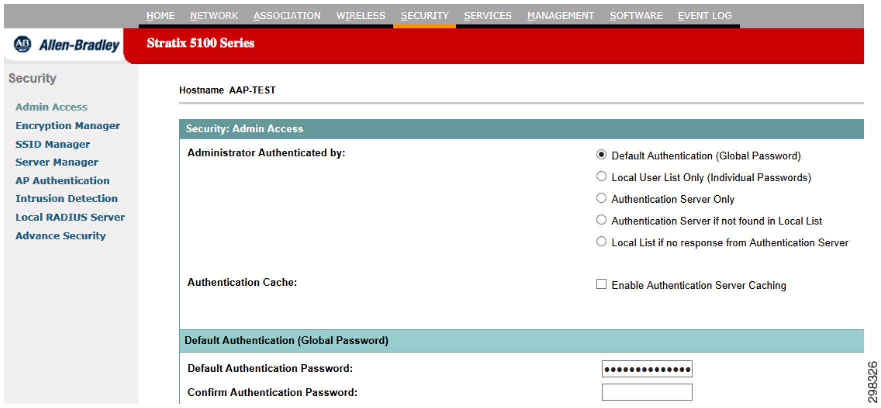
Channel: channel 36-5180

Power: 11

Step 4 Change the default authentication (global) password on the *Security-Admin Access* page. See Figure 3-3.

Note By default, a single password is used for HTTP or CLI access to the device. For information about using individual user credentials and local user lists or authentication servers, refer to the Stratix 5100 User Manual.

Figure 3-3 Security—Admin Access



Hostname AAP-TEST

Security: Admin Access

Administrator Authenticated by:

● Default Authentication (Global Password)
○ Local User List Only (Individual Passwords)
○ Authentication Server Only
○ Authentication Server if not found in Local List
○ Local List if no response from Authentication Server

Authentication Cache: □ Enable Authentication Server Caching

Default Authentication (Global Password)

Default Authentication Password: ••••••••••••••

Confirm Authentication Password:

The equivalent CLI configuration for Steps 1-4 is shown below:

```
configure terminal
hostname <NAME>
enable secret <PASSWORD>
dot11 ssid <SSID>
interface Dot11Radio1
 ssid <SSID>
 power local <VALUE>
 channel <VALUE>
 station-role {root | workgroup-bridge}
```

Step 5 If necessary, enable remote access to the AP via SSH by applying the following CLI commands:

```
configure terminal
username <USERNAME> secret <PASSWORD>
line vty 0 15
 transport input ssh
 login local
```

SSH requires individual usernames and passwords to be configured on the AP.

Note During the initial configuration, CLI commands can be entered using the console port or on the *Software - System Configuration - Show tech-support* page.

SSID and VLAN Configuration

The Easy Setup configuration or CLI example in the previous section applies to a case where only one SSID is configured with no VLANs on the AP. This is the recommended architecture for an Autonomous WLAN with a fixed set of wireless clients (WGBs) that is for equipment control purposes and a single IACS application.

In some cases, more than one SSID and VLAN should be used in the network. Design considerations and recommendations for this scenario can be found in Multiple SSID / VLAN Architecture, page 2-20.

Note VLAN configuration should be applied only in the AP role. VLANs should not be used in the WGB role because VLAN tagging is not supported over the WGB radio interfaces. Only one SSID should be configured on the WGBs.

The steps below describe how to set up two SSIDs (one per radio), each associated with a separate VLAN.

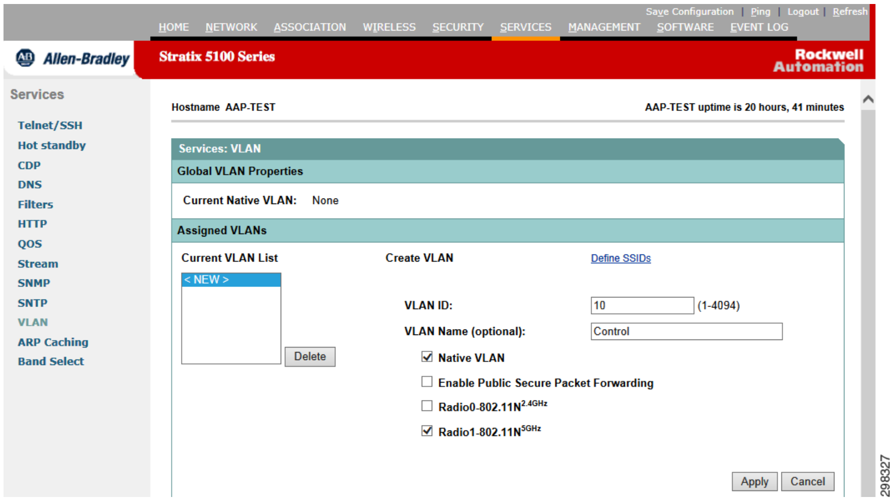
Step 1 Configure the VLAN that will be used on the 5 GHz radio (i.e., for IACS equipment control traffic to and from the WGB clients) on the *Services - VLAN* page: (See Figure 3-4.)

a. Configure the VLAN ID and name. The same VLAN ID should be configured on all infrastructure devices.

b. Make it the native VLAN. WGBs must use native VLAN for wireless traffic. Management interfaces of the AP and WGBs must belong to the native VLAN.

c. Apply to the *Radio1-802.11N 5 GHz* interface.

Figure 3-4 Services—VLAN



Hostname AAP-TEST

AAP-TEST uptime is 20 hours, 41 minutes

Services: VLAN

Global VLAN Properties

Current Native VLAN: None

Assigned VLANs

Current VLAN List: < NEW >

Create VLAN

VLAN ID: 10 (1-4094)

VLAN Name (optional): Control

☑ Native VLAN

☐ Enable Public Secure Packet Forwarding

☐ Radio0-802.11N 2.4GHz

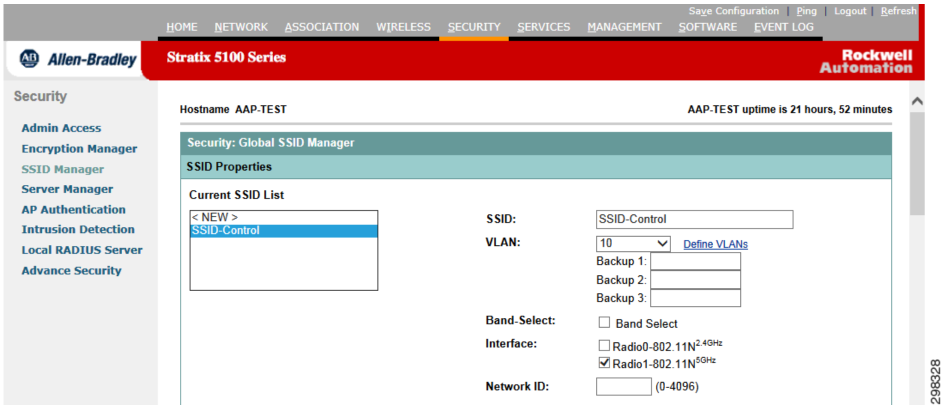
☑ Radio1-802.11N 5GHz

Step 2 Repeat Step 1 to configure the VLAN that will be used on the 2.4 GHz radio to connect non-WGB clients. Do not select the *Native VLAN* option. Apply to the *Radio0-802.11N 2.4 GHz* interface.

Step 3 Configure the SSID for the 5 GHz radio interface and associate with the corresponding VLAN on the *Security - SSID Manager* page. If an SSID has been configured previously without a VLAN attached, the old SSID has to be deleted and recreated. See Figure 3-5.

Note The default security setting is open authentication with no encryption. Configuration for SSID security is covered in the next section.

Figure 3-5 Security - SSID Manager—Properties



Hostname AAP-TEST

AAP-TEST uptime is 21 hours, 52 minutes

Security: Global SSID Manager

SSID Properties

Current SSID List

< NEW >
SSID-Control

SSID: SSID-Control

VLAN: 10 Define VLANs

Backup 1:

Backup 2:

Backup 3:

Band-Select: □ Band Select

Interface: □ Radio0-802.11N$^{2.4GHz}$
☑ Radio1-802.11N^{5GHz}

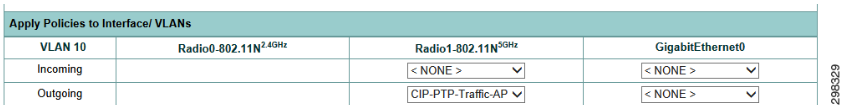
Network ID: (0-4096)

Step 4 Repeat Step 3 to create the SSID for the 2.4 GHz radio interface and link it to the corresponding VLAN.

Step 5 When a VLAN is applied to the radio interface, the default QoS policy is removed from that interface. The QoS policy needs to be reapplied to the VLAN sub-interface on the radio.

Go to the *Services - QoS* page, select the QoS policy name from the list, and apply as *Outgoing* to the VLAN / Radio. See Figure 3-6.

Figure 3-6 Services - QoS Policies



Apply Policies to Interface/ VLANs

VLAN 10	Radio0-802.11N$^{2.4GHz}$	Radio1-802.11N^{5GHz}	GigabitEthernet0
Incoming		< NONE >	< NONE >
Outgoing		CIP-PTP-Traffic-AP	< NONE >

Note If the QoS policy is not applied to the radio interface, significant performance degradation may occur for the critical EtherNet/IP data such as I/O, Produced/Consumed, and CIP Safety.

The equivalent CLI commands for Steps 1-5 are shown below:

```
configure terminal
dot11 vlan-name Control vlan 10
dot11 vlan-name Maintenance vlan 20
!
dot11 ssid SSID-Control
 vlan 10
 authentication open
!
dot11 ssid SSID-Maintenance
 vlan 20
 authentication open
!
interface Dot11Radio0
 ssid SSID-Maintenance
!
interface Dot11Radio0.20
 encapsulation dot1Q 20
 bridge-group 20
!
interface Dot11Radio1
 ssid SSID-Control
```

```
!
interface Dot11Radio1.10
 encapsulation dot1Q 10 native
 bridge-group 1
 service-policy output CIP-PTP-Traffic-AP
!
interface GigabitEthernet0.10
 encapsulation dot1Q 10 native
 bridge-group 1
!
interface GigabitEthernet0.20
 encapsulation dot1Q 20
 bridge-group 20
!
bridge-group 1 route ip
bridge-group 20 route ip
```

The CLI example above includes sub-interfaces that have been created on the Radio0, Radio1 and Gigabit Ethernet interfaces, each assigned to a bridge group. This is equivalent to configuring VLANs and trunking on a network switch. The sub-interfaces for the native VLAN 10 are assigned to the default bridge group 1 (not shown). The sub-interfaces for the non-native VLAN are assigned to a new bridge group.

Step 6 Configure the switch port that connects the AP as a trunk port. Configure the native VLAN on that port to match the native VLAN on the AP. See Switch Configuration, page 3-19 for more information.

Security Configuration

Based on the security design recommendations in Chapter 2, "System Design Considerations," the following WLAN security methods are discussed here:

- WPA2 with PSK authentication
- WPA2 with EAP-FAST authentication using RADIUS and local user list on the AP

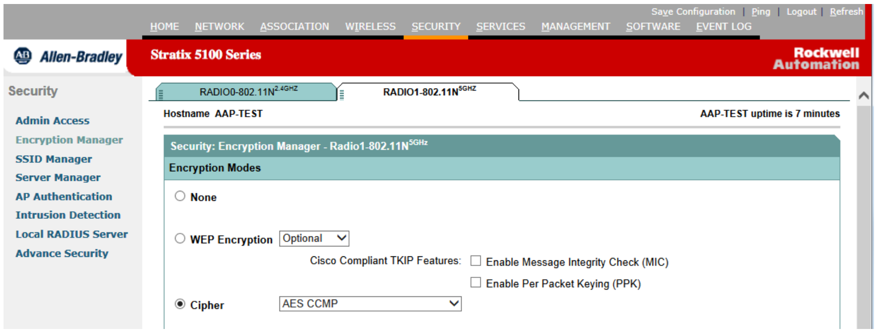
Encryption Mode

Before an authentication method can be configured for the SSID, an encryption mode should be selected on the radio. IACS networks must use AES encryption for maximum protection.

For the AP role, the configuration depends on whether VLANs are enabled on the AP (the WGB will always use the *no VLAN* option).

- If no VLANs exist, apply AES CCMP encryption mode to the 5 GHz or 2.4 GHz radio using the *Security - Encryption Manager* page. See Figure 3-7.

Figure 3-7 Security—Encryption Manager with no VLANs



Hostname AAP-TEST   AAP-TEST uptime is 7 minutes

Security: Encryption Manager - Radio1-802.11N 5GHz

Encryption Modes

○ None

○ WEP Encryption Optional

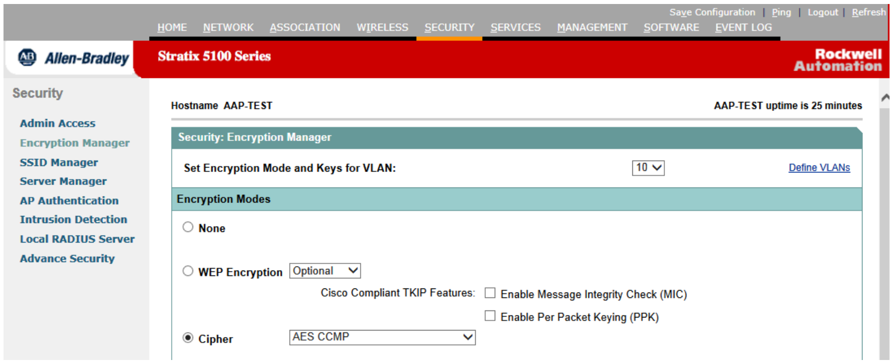
Cisco Compliant TKIP Features: □ Enable Message Integrity Check (MIC)

□ Enable Per Packet Keying (PPK)

● Cipher AES CCMP

- If VLANs are configured on the AP, the encryption mode is configured on each VLAN individually and not on the radio interface. This option does not apply to the WGB role. See Figure 3-8,

Figure 3-8 Security—Encryption Manager with VLANs



Hostname AAP-TEST   AAP-TEST uptime is 25 minutes

Security: Encryption Manager

Set Encryption Mode and Keys for VLAN: 10   Define VLANs

Encryption Modes

○ None

○ WEP Encryption Optional

Cisco Compliant TKIP Features: □ Enable Message Integrity Check (MIC)

□ Enable Per Packet Keying (PPK)

● Cipher AES CCMP

Note Do not configure *Encryption Keys* on the *Encryption Manager* page. This option only applies to the legacy WEP encryption mode that must never be used in a WLAN.

Below is the CLI to configure encryption on the 5 GHz radio without VLANs:

```
configure terminal
interface Dot11Radio1
 encryption mode ciphers aes-ccm
```

If VLANs are configured, the CLI is:

```
configure terminal
interface Dot11Radio1
 encryption vlan <VLAN ID> mode ciphers aes-ccm
```

Pre-shared Key Authentication

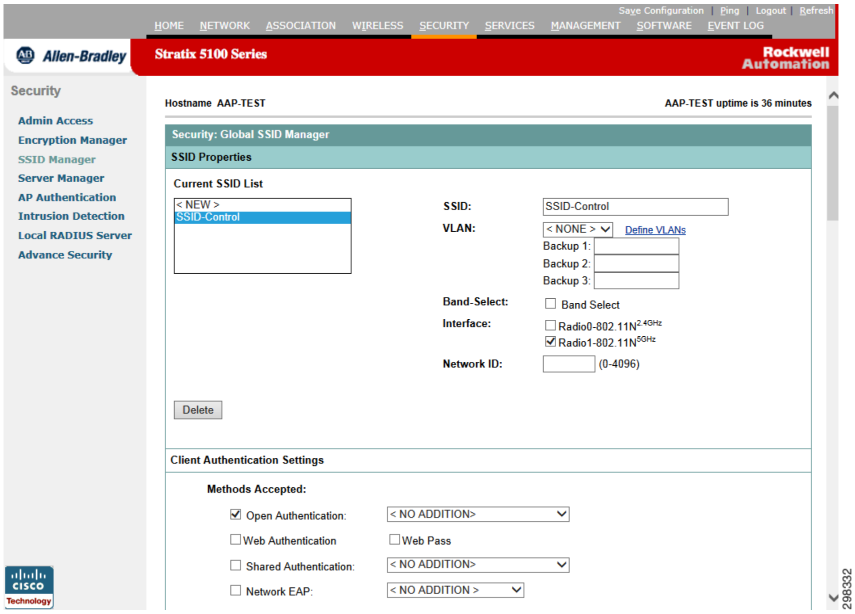
WPA2-PSK is the common security method to connect WGBs in the Autonomous WLAN. Both AP and WGBs share the common password (the PSK) that is stored in the configuration file.

Note It is important to protect configuration files and to store them in a secure location to avoid compromising the PSKs.

The WPA2-PSK configuration is the same for the AP and WGB role. The steps below assume that an SSID has already been defined on the AP or WGB and attached to the radio interface.

Step 1 Select the SSID from the list on the *Security - SSID Manager* page. Select *Open Authentication* method with *No Addition*. See Figure 3-9.

Figure 3-9 Security—SSID Manager Open Authentication



Hostname AAP-TEST
AAP-TEST uptime is 36 minutes

Security: Global SSID Manager

SSID Properties

Current SSID List: < NEW >, SSID-Control

SSID: SSID-Control

VLAN: < NONE > Define VLANs

Backup 1:
Backup 2:
Backup 3:

Band-Select: □ Band Select

Interface: □ Radio0-802.11N$^{2.4GHz}$ ☑ Radio1-802.11N^{5GHz}

Network ID: (0-4096)

Client Authentication Settings

Methods Accepted:

☑ Open Authentication: < NO ADDITION>
□ Web Authentication □ Web Pass
□ Shared Authentication: < NO ADDITION>
□ Network EAP: < NO ADDITION >

Step 2 Configure key management options on the same page. See Figure 3-10.

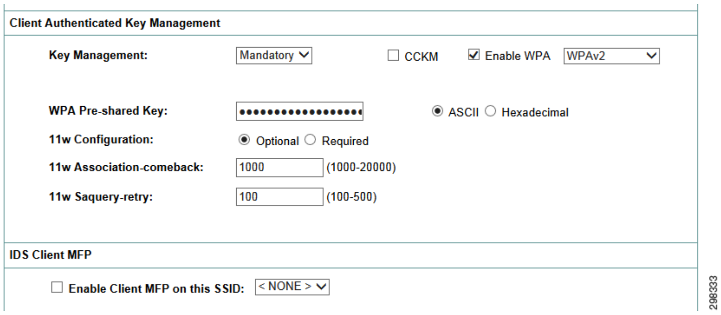
a. Make Key Management *Mandatory*.

b. Enable *WPAv2* option.

c. Enter WPA PSK in the ASCII format.

d. Disable *Client MFP* on the SSID.

Figure 3-10 Security—SSID Manager WPA2- PSK



Client Authenticated Key Management

Key Management: Mandatory □ CCKM ☑ Enable WPA WPAv2

WPA Pre-shared Key: ●●●●●●●●●●●●●●●●● ● ASCII ○ Hexadecimal

11w Configuration: ● Optional ○ Required

11w Association-comeback: 1000 (1000-20000)

11w Saquery-retry: 100 (100-500)

IDS Client MFP

□ Enable Client MFP on this SSID: < NONE >

The equivalent CLI is shown below:

```
configure terminal
dot11 ssid <SSID>
 authentication open
 authentication key-management wpa version 2
 wpa-psk ascii <PASSWORD>
       no ids mfp client
      !
      interface Dot11Radio1
       ssid <SSID>
```

EAP-FAST Authentication with Local RADIUS

EAP-FAST method can be used to provide 802.1X authentication based on the individual client credentials. This method requires more advanced configuration of the Autonomous WLAN than does the WPA2-PSK method, but can provide better protection since it does not rely on the common shared password.

The section describes configuration of the following components:

- EAP-FAST configuration on the AP (authenticator)
- EAP-FAST configuration on the WGB (wireless client)
- Local RADIUS and user list configuration on the AP (authentication server)

EAP-FAST Configuration for the AP

Step 1 Configure RADIUS server parameters on the *Security - Server Manager* page of the root AP.

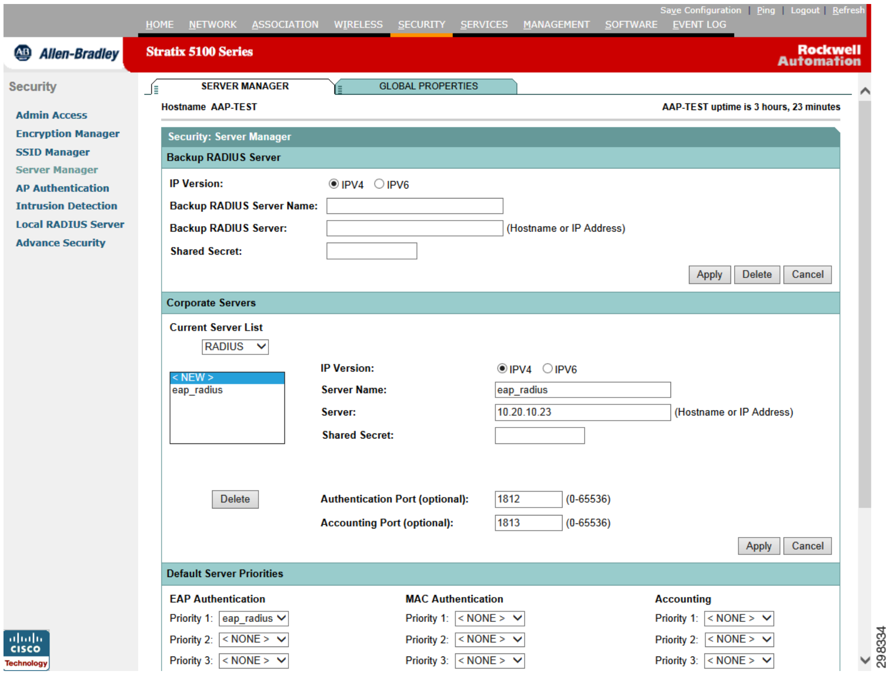
a. Configure server name and IP address. The RADIUS server could be another AP configured for local RADIUS authentication, or any RADIUS server that supports EAP-FAST protocol.

b. Configure the shared key that the AP will use to authenticate to the RADIUS server.

c. Configure authentication port as 1812 and accounting port as 1813.

d. Apply the settings, then select the server name as *Priority 1* for the *EAP Authentication*.

Figure 3-11 Security - Server Manager—RADIUS



Hostname AAP-TEST

AAP-TEST uptime is 3 hours, 23 minutes

Security: Server Manager

Backup RADIUS Server

IP Version: ● IPV4 ○ IPV6

Backup RADIUS Server Name:

Backup RADIUS Server: (Hostname or IP Address)

Shared Secret:

Corporate Servers

Current Server List: RADIUS

< NEW >
eap_radius

IP Version: ● IPV4 ○ IPV6

Server Name: eap_radius

Server: 10.20.10.23 (Hostname or IP Address)

Shared Secret:

Authentication Port (optional): 1812 (0-65536)

Accounting Port (optional): 1813 (0-65536)

Default Server Priorities

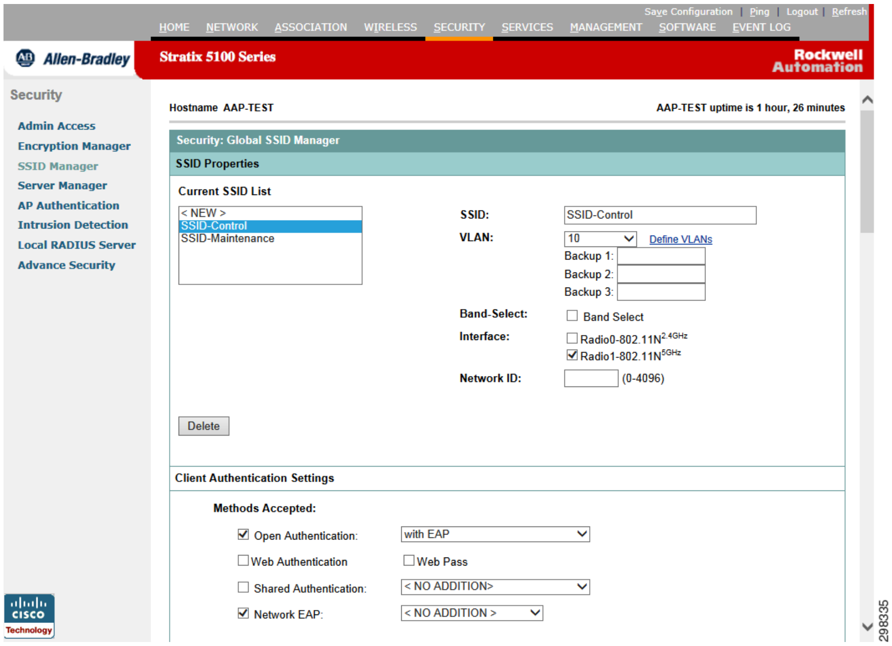
EAP Authentication	MAC Authentication	Accounting
Priority 1: eap_radius	Priority 1: < NONE >	Priority 1: < NONE >
Priority 2: < NONE >	Priority 2: < NONE >	Priority 2: < NONE >
Priority 3: < NONE >	Priority 3: < NONE >	Priority 3: < NONE >

Step 2 Select the SSID from the list on the *Security - SSID Manager* page:

a. Select *Open Authentication* with *EAP*.

b. Select *Network EAP* with *No Addition*.

Figure 3-12 Security—SSID Manager EAP Authentication



Hostname AAP-TEST AAP-TEST uptime is 1 hour, 26 minutes

Security: Global SSID Manager

SSID Properties

Current SSID List: < NEW >, SSID-Control, SSID-Maintenance

SSID: SSID-Control

VLAN: 10 Define VLANs

Backup 1:
Backup 2:
Backup 3:

Band-Select: □ Band Select

Interface: □ Radio0-802.11N 2.4GHz ☑ Radio1-802.11N 5GHz

Network ID: (0-4096)

Client Authentication Settings

Methods Accepted:

☑ Open Authentication: with EAP

□ Web Authentication □ Web Pass

□ Shared Authentication: < NO ADDITION>

☑ Network EAP: < NO ADDITION >

Step 3 Configure key management options on the same page:

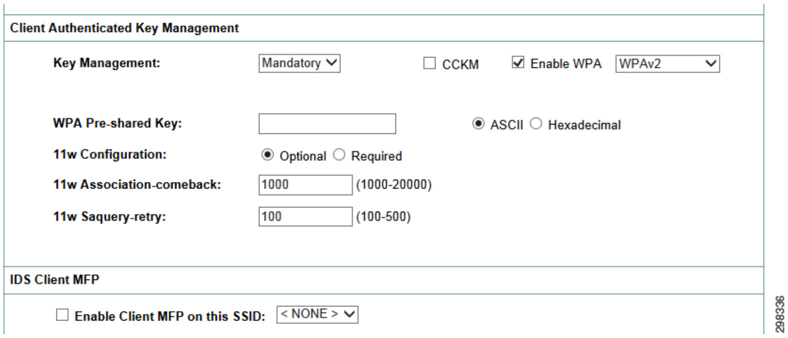
a. Select *Key Management* as *Mandatory*.

b. Enable *WPAv2* option.

c. Leave pre-shared key field as blank.

d. Disable *Client MFP* on the SSID.

Figure 3-13 Security—SSID Manager WPA2 with EAP



Client Authenticated Key Management

Key Management: Mandatory □ CCKM ☑ Enable WPA WPAv2

WPA Pre-shared Key: ● ASCII ○ Hexadecimal

11w Configuration: ● Optional ○ Required

11w Association-comeback: 1000 (1000-20000)

11w Saquery-retry: 100 (100-500)

IDS Client MFP

□ Enable Client MFP on this SSID: < NONE >

The following example shows the CLI configuration to configure EAP-FAST authentication on the root AP. This is equivalent to the Steps 1-3 above.

```
configure terminal
aaa new-model
!
```

```
aaa group server radius rad_eap
 server name eap_radius
!
aaa authentication login eap_methods group rad_eap
!
dot11 ssid <SSID>
 authentication open eap eap_methods
 authentication network-eap eap_methods
 authentication key-management wpa version 2
 no ids mfp client
!
ip radius source-interface BVI1
!
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
!
radius server eap_radius
 address ipv4 <IP ADDRESS> auth-port 1812 acct-port 1813
 key <SHARED KEY>
```

EAP-FAST Configuration for the WGB

The following steps should be completed for each WGB in the WLAN.

Step 1 Configure WGB credentials and authentication method on the *Security - AP Authentication* page.

a. Configure *Credentials Name.*

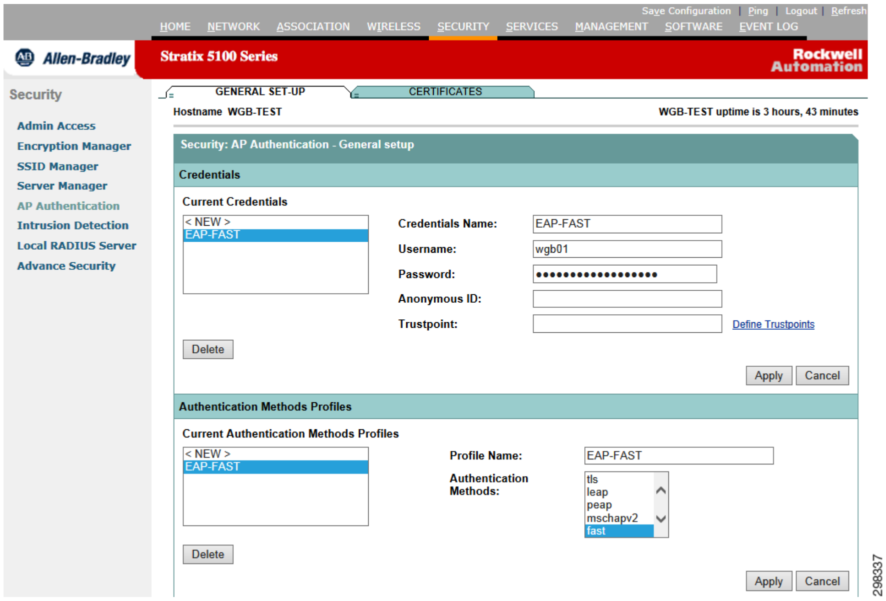
b. Configure *Username* and *Password* for the WGB. The same credentials should be defined in the user directory or local list on the RADIUS server.

Note It is important to protect configuration files by storing them in a secure location to avoid compromising the WGB credentials.

c. Configure *Profile Name* for the authentication methods.

d. Select *fast* in the list of methods.

Figure 3-14 Security—AP Authentication



Hostname WGB-TEST

WGB-TEST uptime is 3 hours, 43 minutes

Security: AP Authentication - General setup

Credentials

Current Credentials: < NEW >, EAP-FAST

Credentials Name: EAP-FAST

Username: wgb01

Password: ●●●●●●●●●●●●●●●●●

Anonymous ID:

Trustpoint:

Authentication Methods Profiles

Current Authentication Methods Profiles: < NEW >, EAP-FAST

Profile Name: EAP-FAST

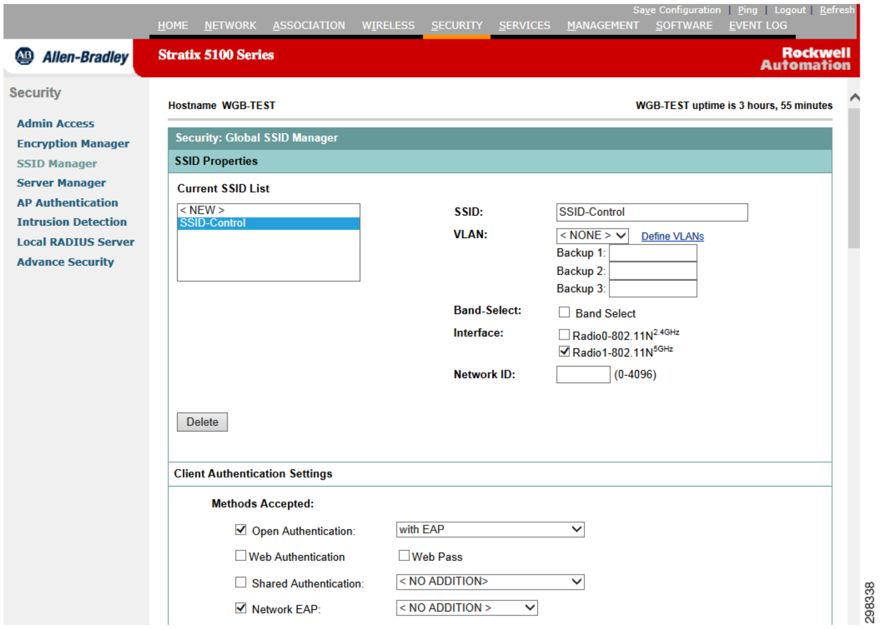
Authentication Methods: tls, leap, peap, mschapv2, fast

Step 2 Select the SSID from the list on the *Security - SSID Manager* page:

a. Select *Open Authentication* with *EAP*.

b. Select *Network EAP* with *No Addition*.

Figure 3-15 Security—SSID Manager-EAP for WGB



Hostname WGB-TEST

WGB-TEST uptime is 3 hours, 55 minutes

Security: Global SSID Manager

SSID Properties

Current SSID List: < NEW >, SSID-Control

SSID: SSID-Control

VLAN: < NONE >

Backup 1:

Backup 2:

Backup 3:

Band-Select: □ Band Select

Interface: □ Radio0-802.11N$^{2.4GHz}$ ☑ Radio1-802.11N^{5GHz}

Network ID: (0-4096)

Client Authentication Settings

Methods Accepted:

☑ Open Authentication: with EAP

□ Web Authentication □ Web Pass

□ Shared Authentication: < NO ADDITION>

☑ Network EAP: < NO ADDITION >

Step 3 Configure other options on the same page:

a. Select *Key Management* as *Mandatory*.

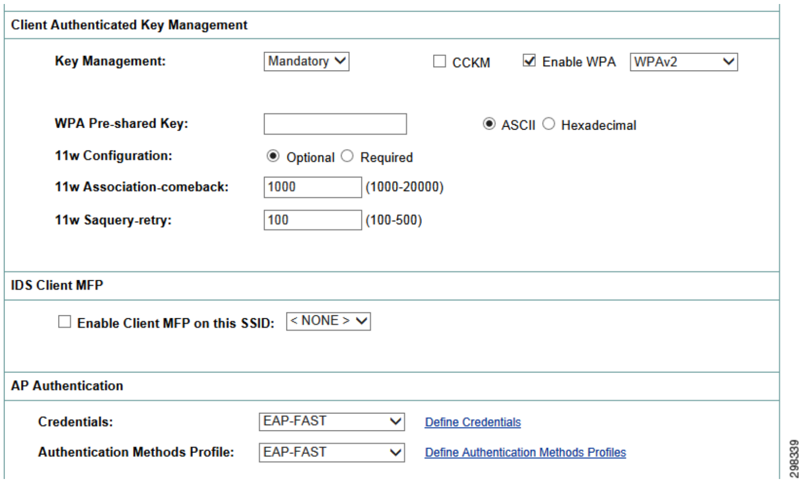
b. Enable *WPAv2* option.

c. Leave pre-shared key field as blank.

d. Disable *Client MFP* on the SSID.

e. Select *Credentials* and *Authentication Methods Profile* names from the list.

Figure 3-16 Security—SSID Manager-WGB Authentication



Client Authenticated Key Management

Key Management: Mandatory ☐ CCKM ☑ Enable WPA WPAv2

WPA Pre-shared Key: ● ASCII ○ Hexadecimal

11w Configuration: ● Optional ○ Required

11w Association-comeback: 1000 (1000-20000)

11w Saquery-retry: 100 (100-500)

IDS Client MFP

☐ Enable Client MFP on this SSID: < NONE >

AP Authentication

Credentials: EAP-FAST Define Credentials

Authentication Methods Profile: EAP-FAST Define Authentication Methods Profiles

The following example shows the CLI configuration to configure EAP-FAST authentication on the WGB. This is equivalent to the steps 1-3 above.

```
dot11 ssid <SSID>
 authentication open eap eap_methods
 authentication network-eap eap_methods
 authentication key-management wpa version 2
 dot1x credentials EAP-FAST
 dot1x eap profile EAP-FAST
 no ids mfp client
!
eap profile EAP-FAST
 method fast
!
dot1x credentials EAP-FAST
 username <USERNAME>
 password <PASSWORD>
```

Local RADIUS Authentication for EAP-FAST

A small Autonomous WLAN can use an AP as a RADIUS server to authenticate EAP-FAST clients using the local list of users. Such AP should not be used for client traffic. The steps below describe local RADIUS configuration on the AP.

Step 1 Dedicate one AP in the WLAN just as a RADIUS server. Do not configure SSIDs or enable radio interfaces.

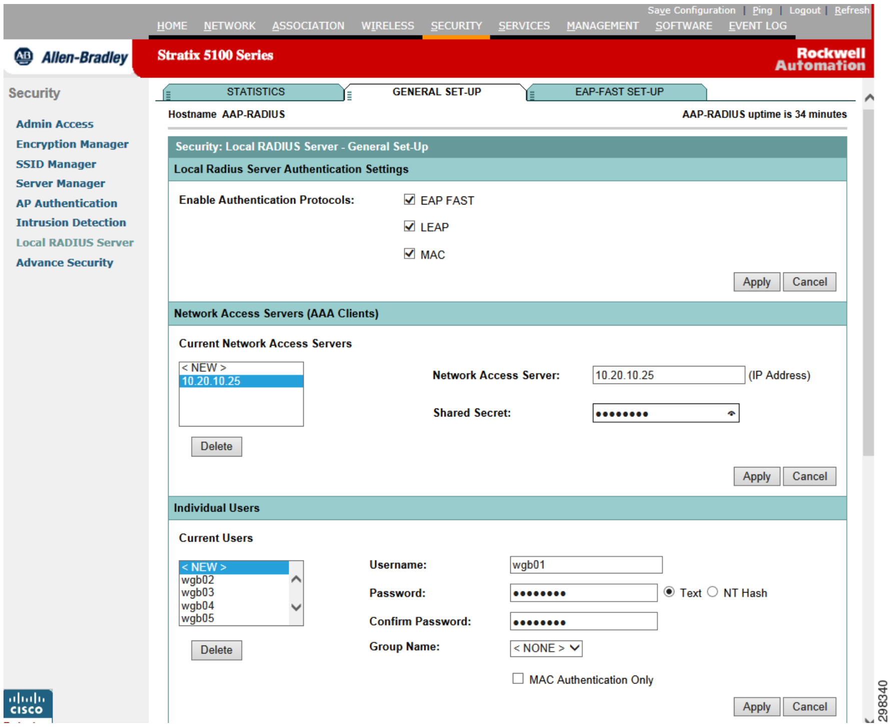
Step 2 Configure parameters on the *Security - Local RADIUS Server* page:

a. Select *EAP FAST* as the authentication method.

b. In the *Network Access Servers (AAA Clients)* section, configure IP addresses of every AP that use the RADIUS server and the shared keys for authentication.

c. In the *Individual Users* section, configure usernames and passwords for every WGB that use EAP-FAST authentication.

Figure 3-17 Security—Local RADIUS Server



Hostname AAP-RADIUS   AAP-RADIUS uptime is 34 minutes

Security: Local RADIUS Server - General Set-Up

Local Radius Server Authentication Settings

Enable Authentication Protocols: ☑ EAP FAST ☑ LEAP ☑ MAC

Network Access Servers (AAA Clients)

Current Network Access Servers: < NEW >, 10.20.10.25

Network Access Server: 10.20.10.25 (IP Address)

Shared Secret: ••••••••

Individual Users

Current Users: < NEW >, wgb02, wgb03, wgb04, wgb05

Username: wgb01

Password: •••••••• ● Text ○ NT Hash

Confirm Password: ••••••••

Group Name: < NONE >

□ MAC Authentication Only

Step 3 Disable "Service Password-Encryption" mode on the RADIUS AP using the CLI command:

```
no service password-encryption
```

Note CLI commands can be entered using the console port, Telnet, SSH, or on the *Software - System Configuration - Show tech-support* page.

This is an example of the CLI configuration for the local RADIUS on the AP:

```
configure terminal
no service password-encryption
radius-server local radius-server local
 nas 10.20.10.25 key <SHARED KEY>
 user wgb01 password <PASSWORD>
 user wgb02 password <PASSWORD>
 user wgb03 password <PASSWORD>
```

QoS Configuration

The default Stratix 5100 configuration includes QoS settings that are optimized for EtherNet/IP traffic (see Wireless QoS, page 2-21). These settings have a direct impact on latency, jitter and packet loss of the high priority IACS traffic.

- It is recommended to not modify the default QoS parameters unless directed by technical support. These settings can be found on the *Services - QoS* page.
- In the WGB role, certain QoS parameters are controlled by the root AP. The *Access Category* parameters in the WGB configuration do not take effect and the *Client Access Category* parameters in the root AP are applied during the association.

- If VLANs are configured on the AP, the default QoS policy is removed from the interfaces. The policy has to be reapplied to the sub-interface that corresponds to the native VLAN on the radio (see SSID and VLAN Configuration, page 3-4).
- The Stratix 5100 configuration classifies traffic based on the DSCP field in the data packet. The EtherNet/IP devices have to support QoS and to correctly mark the traffic according to the ODVA specifications.

The default CLI configuration for the AP provided here as a reference.

```
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 CIP-PTP-Traffic-AP
 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
!
interface Dot11Radio1
 packet retries 8 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
  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 7
    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 7
   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
!
service-policy output CIP-PTP-Traffic-AP
```

Radio Configuration

This section describes parameters that need to be configured on the radio interfaces prior to deployment. It is recommended to leave other radio settings as default unless directed by the technical support.

Step 1 Navigate to the *Network - Network Interface - Radio0/1 - Settings* page. Configure device role as *Access Point* or *Workgroup Bridge* (if not configured on the *Easy Setup* page previously). See Figure 3-18.

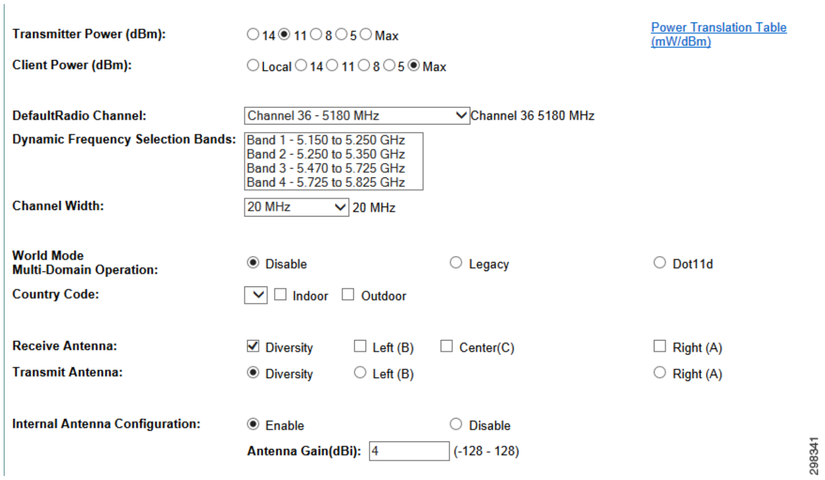
Step 2 On the same page, select *Transmitter Power (dBm)* value as recommended by the site survey. Typically, it is not necessary to select the maximum level.

Step 3 Configure the radio channel that has been allocated to the AP.

- It is recommended to not use DFS channels for IACS applications.
- Channels 36-48 are preferred in the 5 GHz band.
- Use channels 1, 6, and 11 in the 2.4 GHz band.
- The channel setting is not available in the WGB role.

Step 4 Configure the antenna gain value in dBi. This parameter can be found in the antenna specifications.

Figure 3-18 Radio Settings



Transmitter Power (dBm): ○ 14 ● 11 ○ 8 ○ 5 ○ Max

Power Translation Table (mW/dBm)

Client Power (dBm): ○ Local ○ 14 ○ 11 ○ 8 ○ 5 ● Max

DefaultRadio Channel: Channel 36 - 5180 MHz Channel 36 5180 MHz

Dynamic Frequency Selection Bands:
Band 1 - 5.150 to 5.250 GHz
Band 2 - 5.250 to 5.350 GHz
Band 3 - 5.470 to 5.725 GHz
Band 4 - 5.725 to 5.825 GHz

Channel Width: 20 MHz 20 MHz

World Mode Multi-Domain Operation: ● Disable ○ Legacy ○ Dot11d

Country Code: □ Indoor □ Outdoor

Receive Antenna: ☑ Diversity □ Left (B) □ Center(C) □ Right (A)

Transmit Antenna: ● Diversity ○ Left (B) ○ Right (A)

Internal Antenna Configuration: ● Enable ○ Disable

Antenna Gain(dBi): 4 (-128 - 128)

The equivalent CLI configuration is shown below:

```
configure terminal
interface Dot11Radio1
 antenna gain <GAIN dBi>
 power local <POWER dBm>
 channel <CHANNEL>
```

Workgroup Bridge Configuration

This section describes some of the considerations for the Stratix 5100 in the WGB role.

- *Channel* command is not available in the WGB mode. By default, all channels in the radio band are scanned by the WGB when trying to associate. To limit the list of channels to scan, use *Mobile Station Scan* setting on the WGB.
- If the Data Rate settings on the root AP and WGB are different, the following rules apply:
  - *Required* data rates must match exactly for successful association.
  - The AP will try use the highest rate for data traffic that is enabled on both AP and WGB.
- Certain applications require optimization of the WGB configuration for roaming speed. This includes fast roaming support in Unified WLAN architecture, and roaming to a backup AP in the Autonomous architecture based on the signal strength. Here is an example of the CLI configuration for roaming WGB:

```
configure terminal
workgroup?bridge timeouts eap?timeout 4
workgroup?bridge timeouts iapp?refresh 100
workgroup?bridge timeouts auth?response 800
workgroup?bridge timeouts assoc?response 800
workgroup?bridge timeouts client?add 800
interface Dot11Radio1
 station-role workgroup-bridge
 mobile station scan 5180 5200
 mobile station ignore neighbor-list
 mobile station minimum-rate 6.0
 mobile station period 1 threshold 67
```

Threshold value is the signal strength in dBm which is used to start a roaming process if the current signal is below it. This parameter should be adjusted based on the RF environment and application test results.

Switch Configuration

This section describes the recommended configuration for the IE switches in the Autonomous WLAN architecture.

- Configure Cell/Area Zone switches in a redundant topology (redundant star or ring) according to the best practices and recommendations. Use resiliency protocols, such as EtherChannel, REP, or Flex Links, with Cisco or Rockwell Automation Stratix switches.
- Configure redundant distribution switches for Layer 3 redundancy. Cisco StackWise switches are recommended.
- Make sure that Stratix switches are configured with Express Setup. Select appropriate Smartports for IACS devices and links between switches.
- Use the following port configuration (custom Smartport) when connecting to the AP without trunking (see Single SSID / VLAN Architecture, page 2-19):

```
interface <NAME>
 switchport access vlan <VLAN>
 switchport mode access
 ip device tracking maximum 0
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 alarm profile ab-alarm
 service-policy input CIP-PTP-Traffic
```

- Use the following port configuration (custom Smartport) when connecting to the AP in the trunk mode (see Multiple SSID / VLAN Architecture, page 2-20):

```
interface <NAME>
 switchport mode trunk
 switchport trunk native vlan <VLAN ID>
 switchport trunk allowed vlan <VLAN LIST>
 ip device tracking maximum 0
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 mls qos trust cos
 alarm profile ab-alarm
 service-policy input CIP-PTP-Traffic
```

The native VLAN in this example should be the native VLAN which is configured on the AP radio interface for WGB traffic. It may be different from the native VLAN used between switches.

- When connecting a switch to the WGB, configure the following:
  - Use the default VLAN 1 on the switch. Apply this port configuration (custom Smartport):

```
interface <NAME>
switchport mode access
ip device tracking maximum 0
srr-queue bandwidth share 1 19 40 40
priority-queue out
alarm profile ab-alarm
service-policy input CIP-PTP-Traffic
```

- Disable Spanning Tree protocol globally on the switch connected to the WGB (CLI only):

```
spanning-tree mode pvst
no spanning-tree vlan 1-1005
```

- It is recommended to use a single switch behind a WGB, if possible.

Note For information on best practices and recommendations for wired networks and switches in particular, refer to the Converged Plantwide Ethernet (CPwE) Design and Implementation Guide at the following URLs:

- Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
- Cisco site: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG.html

Unified WLAN Configuration

This section describes validated configurations for the Unified WLAN setup which includes Wireless LAN controller (WLC), Lightweight Access Point (LWAP), Workgroup Bridge (WGB) and IE switches to support IACS equipment in the Cell/Area Zone.

The following sections describe Unified WLAN setup and configuration details:

- Transport Network and Server Farm Setup
  - Cell/Area Zone access network
  - Cell/Area Zone distribution network
  - Industrial Zone core network
  - Industrial Zone server farm
- Stationary WLAN Setup
  - WLC and LWAP
  - WGB initial setup and configuration
  - WLAN EAP-TLS security
- Fast Roaming WLAN Setup
  - WLC and LWAP
  - WGB initial setup and configuration
  - WLAN EAP-TLS security
- QoS Configuration
  - Transport network QoS
  - WLC QoS
  - WGB QoS
- RF Configuration
  - Radio spectrum, signal power and data rate
  - WGB tune up

Note This document does not provide a complete configuration guide for the WLC, WGB and IE switches and does not cover all possible scenarios where these products may be used. For more information, refer to the specific documentation for each of these products.

Transport Network and Server Farm Setup

The CPwE architecture uses the campus model which is divided into Access, Distribution and Core layers. The transport network encompasses the Access, Distribution and Core networks. In the Server Farm access layer, provided network services include DHCP, RADIUS, Domain Name Service (DNS), Active Directory (AD) and Certificate Authority (CA). Detailed setup steps can be found in the following sections.

Cell / Area Zone Access Network

This section describes the recommended configuration for the access switches in the Unified WLAN architecture.

- The access switches are part of Layer 2 bridge domain. In addition to providing access transport network, the access switches also can power APs and WGBs using Power over Ethernet (PoE) technology. The recommended implementation is to separate network management and IACS control traffic into separate VLANs. The distribution switch acts as the default gateway for the hosts in the VLANs.
- Configure Cell/Area Zone switches in a redundant topology (redundant star or ring) according to the best practices and recommendations. Use resiliency protocols, such as EtherChannel, REP, Flex Links, or MSTP with Cisco or Rockwell Automation Stratix switches.
- Make sure that Stratix switches are configured with Express Setup. Select appropriate Smartports for IACS devices and links between switches.
- Use the following port configuration (custom Smartport) when connecting to the AP in the trunk mode:

```
interface <NAME>
 switchport mode trunk
 switchport trunk native vlan <VLAN ID>
 switchport trunk allowed vlan <VLAN LIST>
 ip device tracking maximum 0
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 alarm profile ab-alarm
 service-policy input CIP-PTP-Traffic
```

- When connecting a switch on the mobile equipment to the WGB, configure the following:
  - Use the following configuration (custom Smartport) on the port facing the WGB:

```
interface <NAME>
 switchport mode access
 ip device tracking maximum 0
 srr-queue bandwidth share 1 19 40 40
 priority-queue out
 alarm profile ab-alarm
 service-policy input CIP-PTP-Traffic
```

Cell / Area Zone Distribution Network

- In a Layer 2-bridged access network, a stacked or standalone distribution switch serves as the access network gateway. A stacked distribution switch provides more port density and redundant uplinks for network resiliency.
- In order for the LWAP to establish a CAPWAP tunnel using DHCP Option 43, an IP helper address must be configured to allow the LWAP to reach the DHCP server. An example is shown below:

```
interface Vlan200
 description REP Ring VLAN for Client access
 ip address 10.20.10.1 255.255.255.0
 ip helper-address 10.13.48.10
!
interface Vlan800
 description REP Native VLAN for LWAP
 ip address 10.20.80.1 255.255.255.0
 ip helper-address 10.13.48.10
end
```

Industrial Zone Core Network

- On the industrial zone distribution switch, WLC management and dynamic interface VLANs should be allowed as shown in the example below:

```
vlan 148
 name WLAN-Servers
vlan 150
 name WLAN-Mgmt
vlan 250
 name WLAN-Dynamic
!
```

- DHCP proxy gateway should be configured as shown below:

```
interface Vlan148
 description To Server Farm
 ip address 10.13.48.1 255.255.255.0
 ip directed-broadcast
end
```

Note For design recommendations and implementation details for the Industrial zone network, refer to the Chapter 4 of the Converged Plantwide Ethernet (CPwE) Design and Implementation Guide:

- http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf

Industrial Zone Server Farm (DHCP, RADIUS, DNS, AD and Root-CA)

Unified WLAN solution recommends EAP-TLS to provide comprehensive security service for plant-wide automation network. Unified WLAN setup for EAP-TLS requires multiple services to be configured in the infrastructure such as DHCP, DNS, AD and Root-CA services.

The overview of the server configuration is provided below. The details and step-by-step examples of server configuration are included in the Appendix (see Appendix C, "Server Infrastructure Configuration").

DHCP Server Configuration

- The DHCP service may either be hosted on a dedicated server in the large scale environments or may be installed alongside the security-related services if desired.
- DHCP scopes should be configured for the following subnets:
  - Primary WLC
  - Backup WLC
  - Each Cell/Area zone subnet
  - Plant-wide roaming subnet
- DHCP option 43 needs to be configured on the server to inform LWAPs of the WLC management address when they join the network for the first time.

DNS and Active Directory Server Configuration

- It is recommended for all WLAN devices and servers to have the same DNS domain.
- Assign users to correct AD domain service with right privileges. Include users "NDES Administrator" and "NDES Service Account" for Root-CA certification server, and users for each WGB client.
- Add any servers requiring authentication, for example RADIUS server.

Root-CA Server Configuration

- Enable Root-CA certification authority service. Create Root-CA server and define X.509 parameters.
- Set up manual certificate enrollment through the web server, for example Microsoft® IIS.
- Set up automated certificate enrollment (optional) using Simple Certificate Enrollment Protocol (SCEP) and Network Device Enrollment Services (NDES).
- Install a certificate from the configured Root-CA on each device, including WGBs and the RADIUS server.

Stationary WLAN

Based on the design recommendations given in Chapter 2, "System Design Considerations," the following sections explain the detailed steps for stationary WLAN configuration.

WLC and LWAP

WLC Setup and License Installation

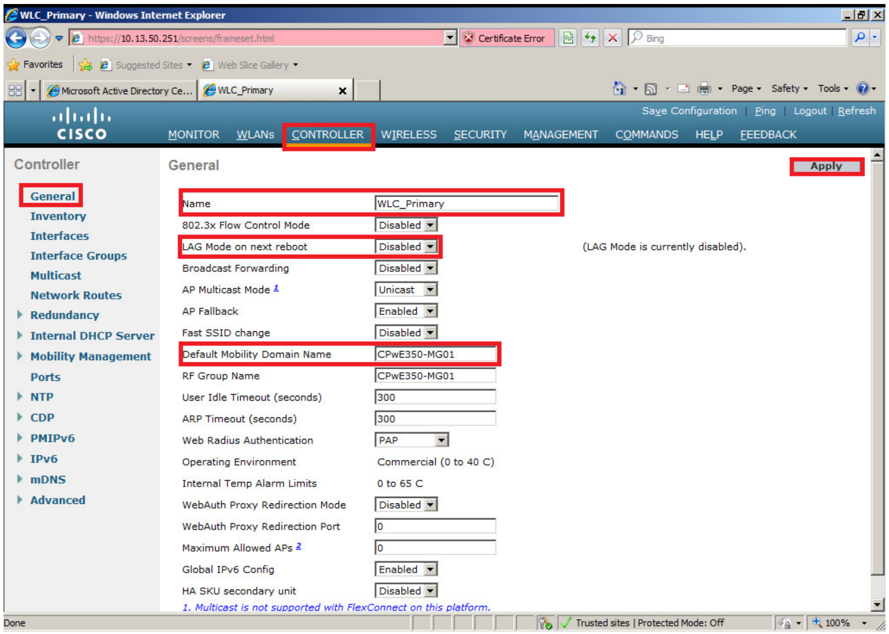
Step 1 Connect to network and perform basic setup: Connect distribution system ports to transport network core switch and follow the step-by-step wizard to set up SNMP, service interface IP and subnet, management IP and subnet, country code, virtual interface IP and subnet. Skip WLAN, Wireless and Security-related configuration steps since these will be explained in detail in the following sections.

- It is recommended to disable the LAG feature in order to be able to support multiple dynamic interfaces on the WLC. This is necessary for plant-wide roaming applications that scale beyond a single VLAN and IP subnet.

Note Do not enable WLC redundancy feature until you have a host PC that can access the WLC management interface subnet. WLC redundancy will disable service port access, and all management has to go through an in-band management interface.

Step 2 Access WLC Controller panel: Connect WLC through previously configured service port management interface, select *Controller* panel for WLC management interface setup. Figure 3-19 shows the *General* sub-panel configuration details.

Figure 3-19 WLC Controller General Setup



General

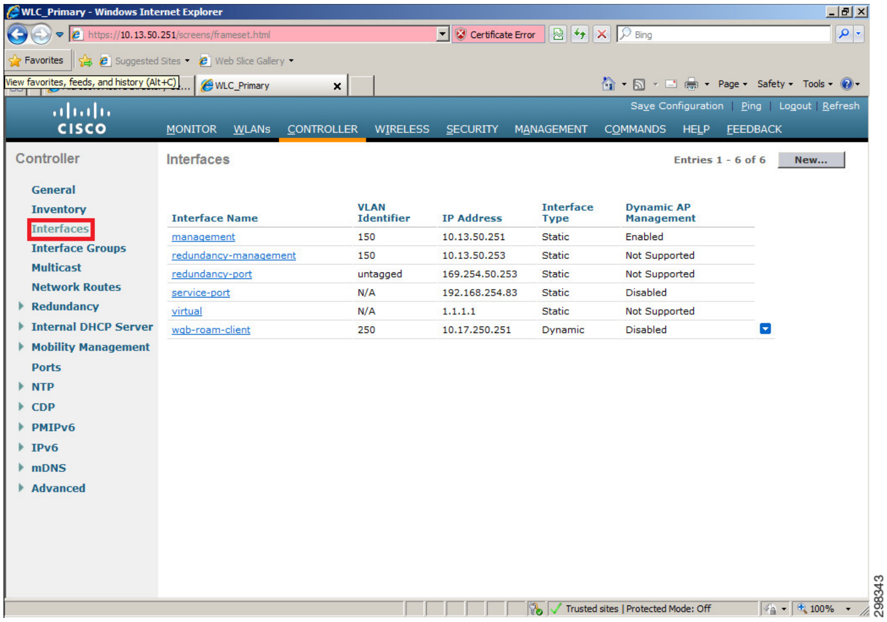
Name	WLC_Primary
802.3x Flow Control Mode	Disabled
LAG Mode on next reboot	Disabled
Broadcast Forwarding	Disabled
AP Multicast Mode [1]	Unicast
AP Fallback	Enabled
Fast SSID change	Disabled
Default Mobility Domain Name	CPwE350-MG01
RF Group Name	CPwE350-MG01
User Idle Timeout (seconds)	300
ARP Timeout (seconds)	300
Web Radius Authentication	PAP
Operating Environment	Commercial (0 to 40 C)
Internal Temp Alarm Limits	0 to 65 C
WebAuth Proxy Redirection Mode	Disabled
WebAuth Proxy Redirection Port	0
Maximum Allowed APs [2]	0
Global IPv6 Config	Enabled
HA SKU secondary unit	Disabled

(LAG Mode is currently disabled).

1. Multicast is not supported with FlexConnect on this platform.

Step 3 Set up general interfaces: WLC interface configuration is shown in Figure 3-20 For example, VLAN 150 is important for the core transport network in the figure.

Figure 3-20 WLC Controller Interface Setup



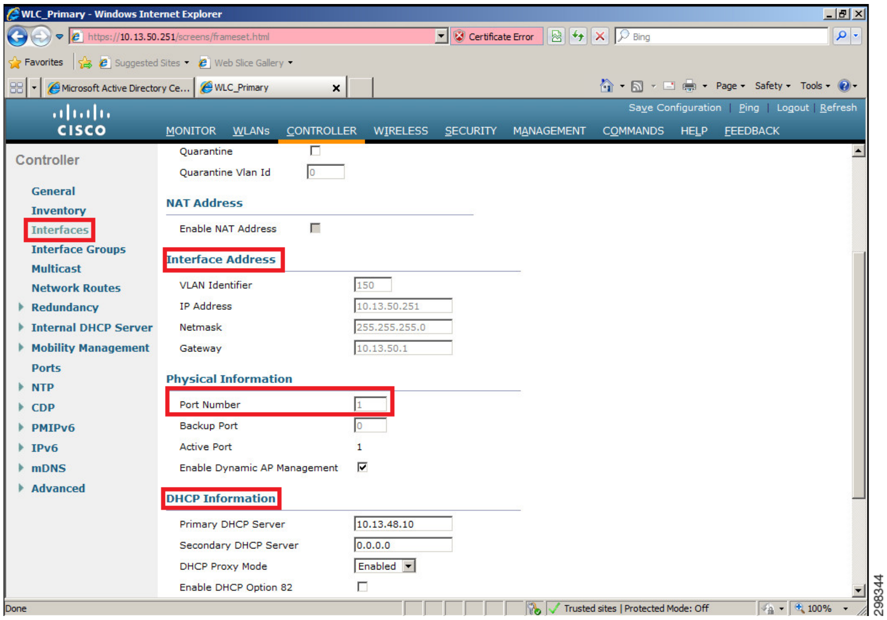
Interfaces

Entries 1 - 6 of 6

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	150	10.13.50.251	Static	Enabled
redundancy-management	150	10.13.50.253	Static	Not Supported
redundancy-port	untagged	169.254.50.253	Static	Not Supported
service-port	N/A	192.168.254.83	Static	Disabled
virtual	N/A	1.1.1.1	Static	Not Supported
wqb-roam-client	250	10.17.250.251	Dynamic	Disabled

Step 4 **Set up management interface**: WLC management interface configuration is shown in Figure 3-21. Configure IP address, netmask and gateway as highlighted. If an external centralized DHCP server is used, this part should be configured as highlighted.

Figure 3-21 WLC Controller Management Interface


WLC_Primary - Windows Internet Explorer
https://10.13.50.251/screens/frameset.html
Certificate Error
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Ce...
WLC_Primary
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
Network Routes
Redundancy
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
PMIPv6
IPv6
mDNS
Advanced
Done
Trusted sites | Protected Mode: Off
100%
298344

Quarantine ☐
Quarantine Vlan Id 0

NAT Address

Enable NAT Address ☐

Interface Address

VLAN Identifier 150
IP Address 10.13.50.251
Netmask 255.255.255.0
Gateway 10.13.50.1

Physical Information

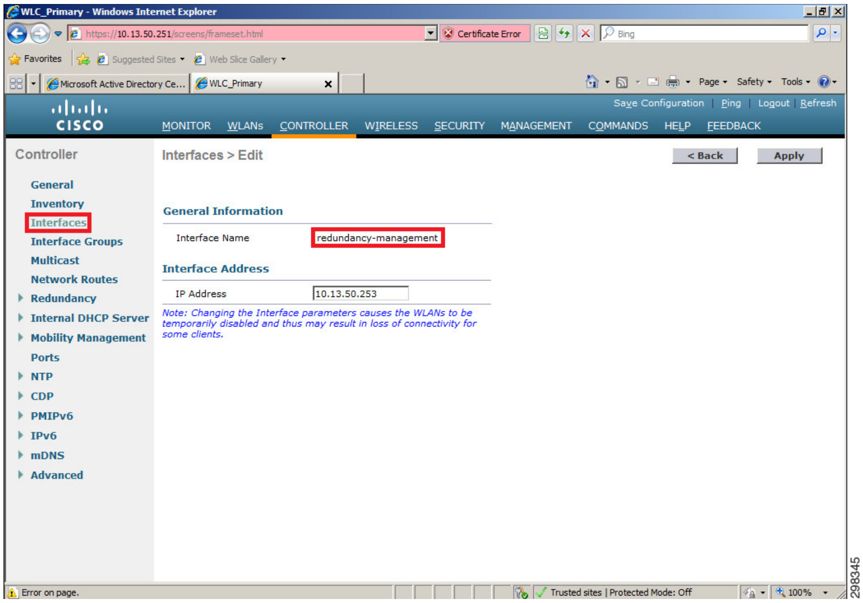
Port Number 1
Backup Port 0
Active Port 1
Enable Dynamic AP Management ☑

DHCP Information

Primary DHCP Server 10.13.48.10
Secondary DHCP Server 0.0.0.0
DHCP Proxy Mode Enabled
Enable DHCP Option 82 ☐

Step 5 **Configure WLC redundancy**: WLC redundancy-management interface setup is shown in Figure 3-22. This IP address serves as redundancy management interface and will be used for primary WLC to sync up configuration and database with backup WLC when WLC redundancy mode is enabled. Figure 3-23 highlights the global configuration for WLC redundancy.

Figure 3-22 WLC Controller In-band Management Interface



Interfaces > Edit

General Information

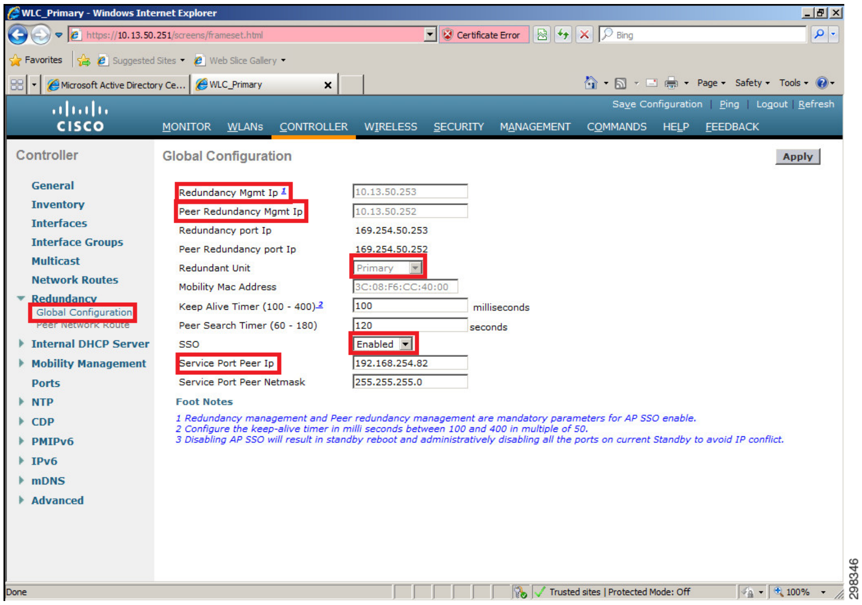
Interface Name: redundancy-management

Interface Address

IP Address: 10.13.50.253

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

Figure 3-23 WLC Controller Redundancy Management Interface



Global Configuration

Redundancy Mgmt Ip [1]	10.13.50.253	
Peer Redundancy Mgmt Ip	10.13.50.252	
Redundancy port Ip	169.254.50.253	
Peer Redundancy port Ip	169.254.50.252	
Redundant Unit	Primary	
Mobility Mac Address	3C:08:F6:CC:40:00	
Keep Alive Timer (100 - 400)[2]	100	milliseconds
Peer Search Timer (60 - 180)	120	seconds
SSO	Enabled	
Service Port Peer Ip	192.168.254.82	
Service Port Peer Netmask	255.255.255.0	

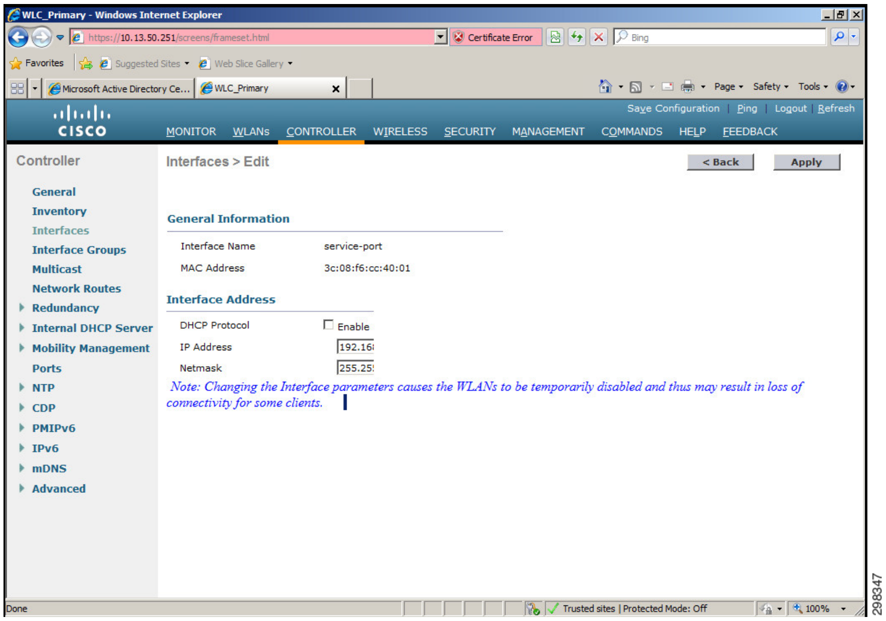
Foot Notes

1 Redundancy management and Peer redundancy management are mandatory parameters for AP SSO enable.
2 Configure the keep-alive timer in milli seconds between 100 and 400 in multiple of 50.
3 Disabling AP SSO will result in standby reboot and administratively disabling all the ports on current Standby to avoid IP conflict.

Step 6 Configure service port: Figure 3-24 shows the WLC service port IP address configuration.

Note Service port is for WLC GUI management purposes, and this port will be disabled once WLC redundancy mode is enabled.

Figure 3-24 WLC Controller Out-Band Management Interface



Interfaces > Edit

General Information

Interface Name service-port
MAC Address 3c:08:f6:cc:40:01

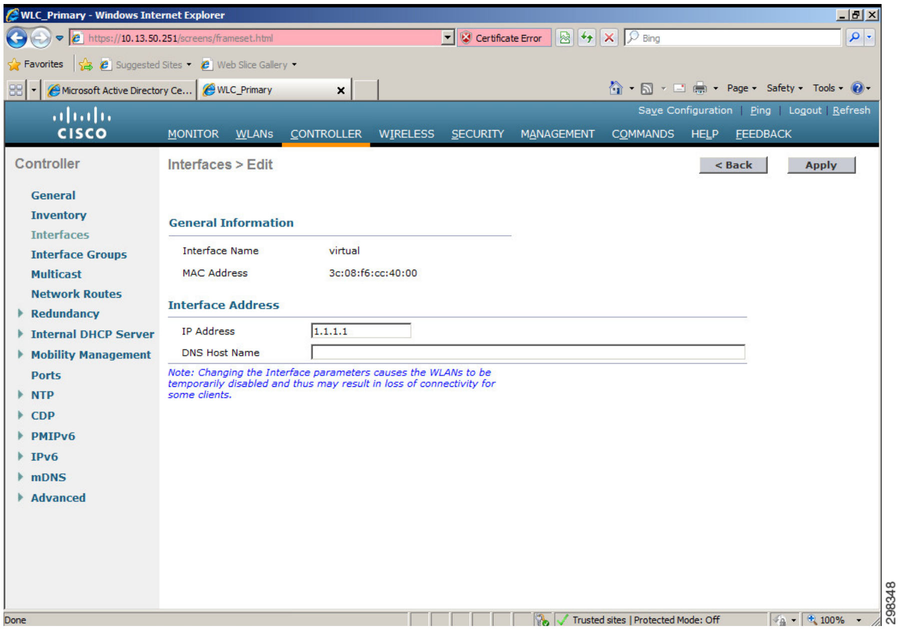
Interface Address

DHCP Protocol ☐ Enable
IP Address 192.16
Netmask 255.25

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

Step 7 **Configure virtual interface**: WLC virtual interface is critical for DHCP relay feature and it is also used for other features like mobility management and Layer 3 security. Assuming this interface is used for DHCP relay only, Figure 3-25 shows virtual interface configuration details.

Figure 3-25 WLC Controller Virtual Interface



Interfaces > Edit

General Information

Interface Name virtual
MAC Address 3c:08:f6:cc:40:00

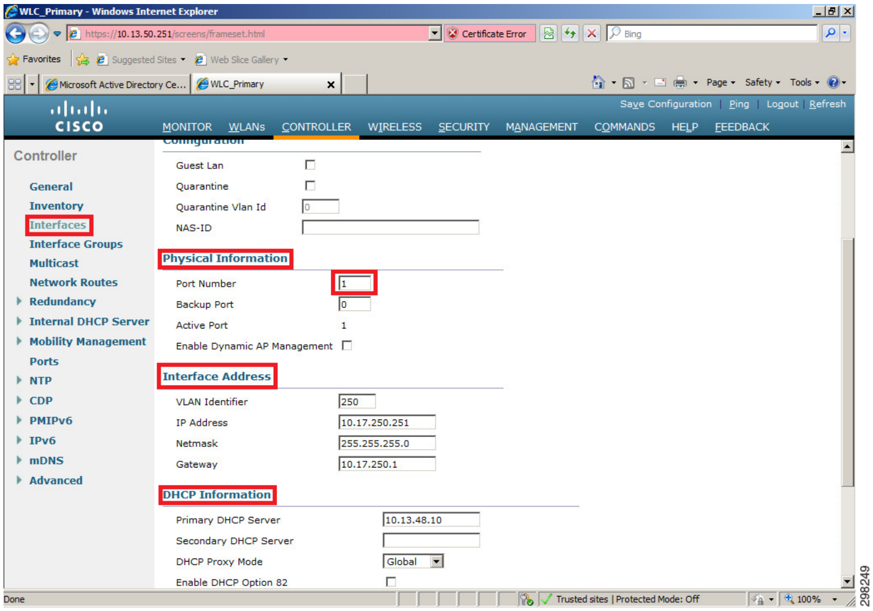
Interface Address

IP Address 1.1.1.1
DNS Host Name

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

Step 8 **Configure distribution interface**: WLC distribution system port is connected to the transport network core switch which carries customer data traffic and WLC control packets. Figure 3-26 shows the distributed system interface status where only Port 1 has been utilized.

Figure 3-26 WLC Controller Distributed System Interface



Configuration

Guest Lan ☐

Quarantine ☐

Quarantine Vlan Id 0

NAS-ID

Physical Information

Port Number 1

Backup Port 0

Active Port 1

Enable Dynamic AP Management ☐

Interface Address

VLAN Identifier 250

IP Address 10.17.250.251

Netmask 255.255.255.0

Gateway 10.17.250.1

DHCP Information

Primary DHCP Server 10.13.48.10

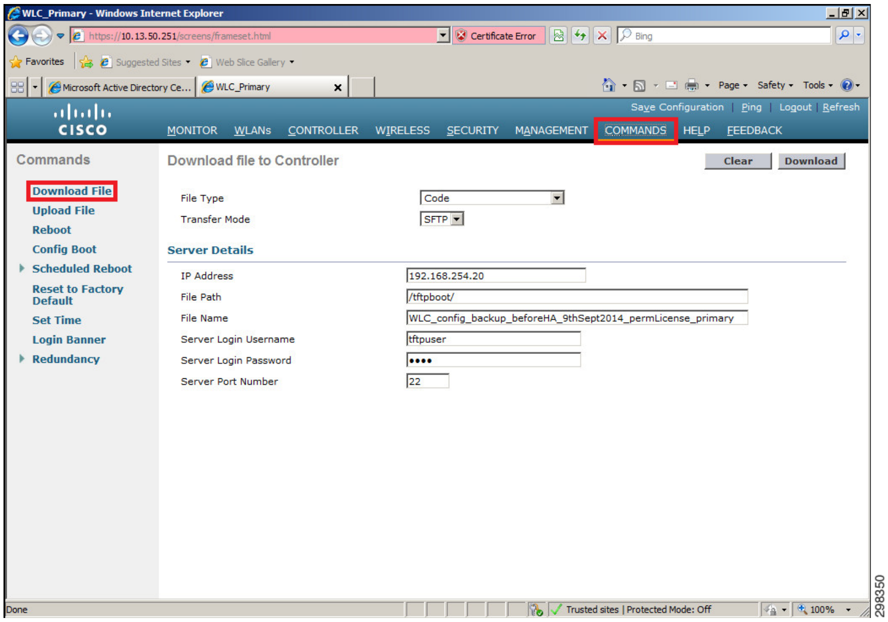
Secondary DHCP Server

DHCP Proxy Mode Global

Enable DHCP Option 82 ☐

Step 9 Configure licenses and upgrade images as required: WLC image bundle (including all supported LWAPs) upgrade and license management are through *Command* and *Management* panels. Image and license files can be uploaded into WLC data store via Secure File Transfer Protocol (SFTP) or other supported protocols. License upgrade can be done through *Management > Software Activation > Commands > Action > Install License*. License management can be done via the *Management* panel. Figure 3-27 through Figure 3-29 show the upgrade status pages.

Figure 3-27 WLC Controller License Upgrade



Download file to Controller

File Type Code

Transfer Mode SFTP

Server Details

IP Address 192.168.254.20

File Path /tftpboot/

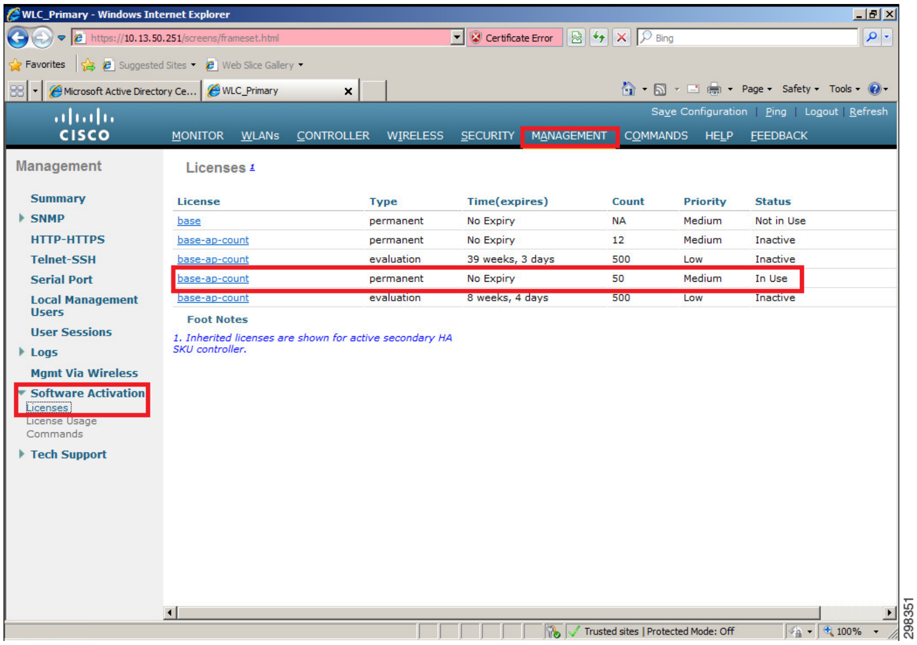
File Name WLC_config_backup_beforeHA_9thSept2014_permLicense_primary

Server Login Username tftpuser

Server Login Password ••••

Server Port Number 22

Figure 3-28 WLC Controller License Management



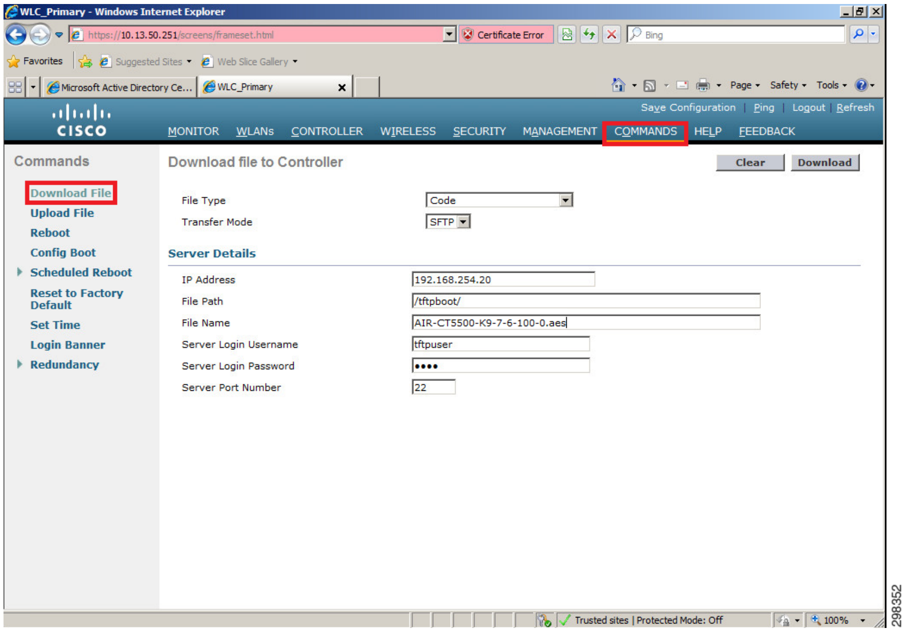
Licenses [1]

License	Type	Time(expires)	Count	Priority	Status
base	permanent	No Expiry	NA	Medium	Not in Use
base-ap-count	permanent	No Expiry	12	Medium	Inactive
base-ap-count	evaluation	39 weeks, 3 days	500	Low	Inactive
base-ap-count	permanent	No Expiry	50	Medium	In Use
base-ap-count	evaluation	8 weeks, 4 days	500	Low	Inactive

Foot Notes

1. Inherited licenses are shown for active secondary HA SKU controller.

Figure 3-29 WLC Controller Image Upgrade



Download file to Controller

File Type: Code
Transfer Mode: SFTP

Server Details

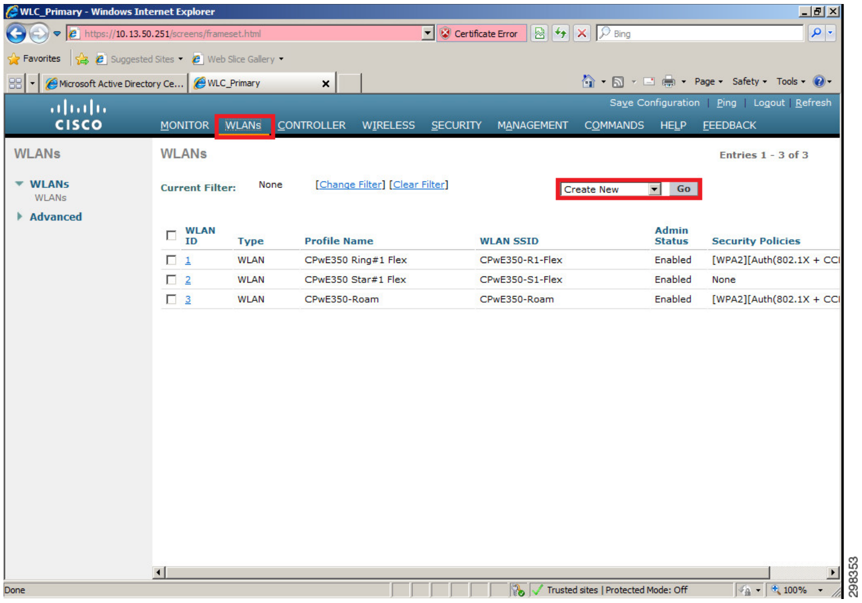
IP Address: 192.168.254.20
File Path: /tftpboot/
File Name: AIR-CT5500-K9-7-6-100-0.aes
Server Login Username: tftpuser
Server Login Password: ••••
Server Port Number: 22

WLC WLAN Setup

WLC supports up to 16 WLANs (SSID) with each access point group and assign specific APs to each group. Each AP advertises only the enabled WLANs that belong to its AP group. The AP does not advertise disabled WLANs in its AP group or WLAN that belong to another group. It is recommended to use unique VLANs for each WLAN.

Step 1 Different WLANs (SSIDs) may be configured for each Cell/Area Zone, in addition to the plant-wide roaming WLAN. Figure 3-30 show the WLAN general status page. Click the highlighted *Create New* drop-down box to create a new WLAN with the chosen SSID.

Figure 3-30 WLC WLAN Setup



WLANs

Entries 1 - 3 of 3

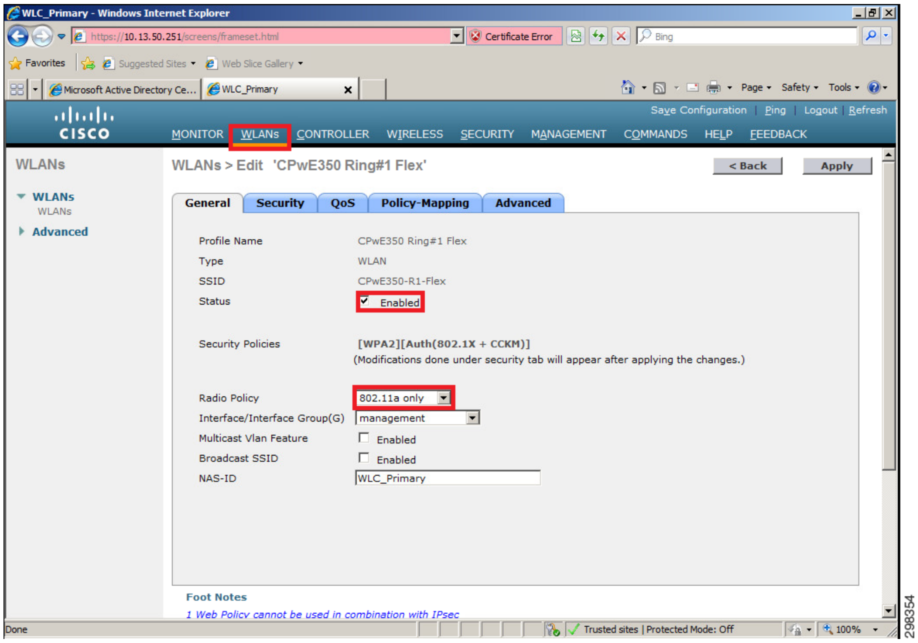
Current Filter: None [Change Filter] [Clear Filter]

Create New Go

□	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
□	1	WLAN	CPwE350 Ring#1 Flex	CPwE350-R1-Flex	Enabled	[WPA2][Auth(802.1X + CCI
□	2	WLAN	CPwE350 Star#1 Flex	CPwE350-S1-Flex	Enabled	None
□	3	WLAN	CPwE350-Roam	CPwE350-Roam	Enabled	[WPA2][Auth(802.1X + CCI

Step 2 Stationary devices are only required to access its Cell/Area zone resources. The WLAN is configured to use the *management* interface. Radio policy is selected as 802.11a to use the 5 GHz frequency band. Enable this WLAN, update the NAS-ID as needed. Figure 3-31 shows some important general WLAN parameters.

Figure 3-31 WLC WLAN General



WLANs > Edit 'CPwE350 Ring#1 Flex'

Profile Name CPwE350 Ring#1 Flex
Type WLAN
SSID CPwE350-R1-Flex
Status ☑ Enabled

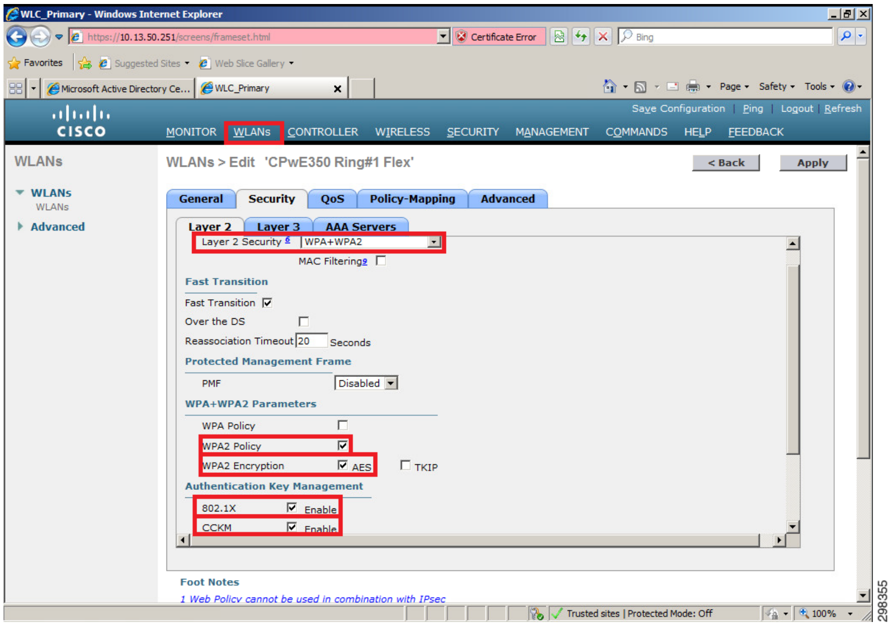
Security Policies [WPA2][Auth(802.1X + CCKM)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy 802.11a only
Interface/Interface Group(G) management
Multicast Vlan Feature ☐ Enabled
Broadcast SSID ☐ Enabled
NAS-ID WLC_Primary

Foot Notes
1 Web Policy cannot be used in combination with IPsec

Step 3 WLAN Layer 2 security polices include None (Open), Static (WEP or 802.1X), CKIP and WPA/WPA2 security methods, and 802.1X authentication key management parameters. 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802, which is known as EAP over LAN (EAPOL). 802.1X authentication involve 3 parties: a supplicant, an authenticator and an authentication server. The authentication server is the ACS 5.5 RADIUS server, authenticator is the WLC, and supplicant is the WGB. Figure 3-32 and Figure 3-33 show WLC Layer 2 security configurations.

Figure 3-32 WLC WLAN Security Layer 2 Configure



WLANs > Edit 'CPwE350 Ring#1 Flex'

Layer 2 Security[6] WPA+WPA2
MAC Filtering[9] ☐

Fast Transition
Fast Transition ☑
Over the DS ☐
Reassociation Timeout 20 Seconds

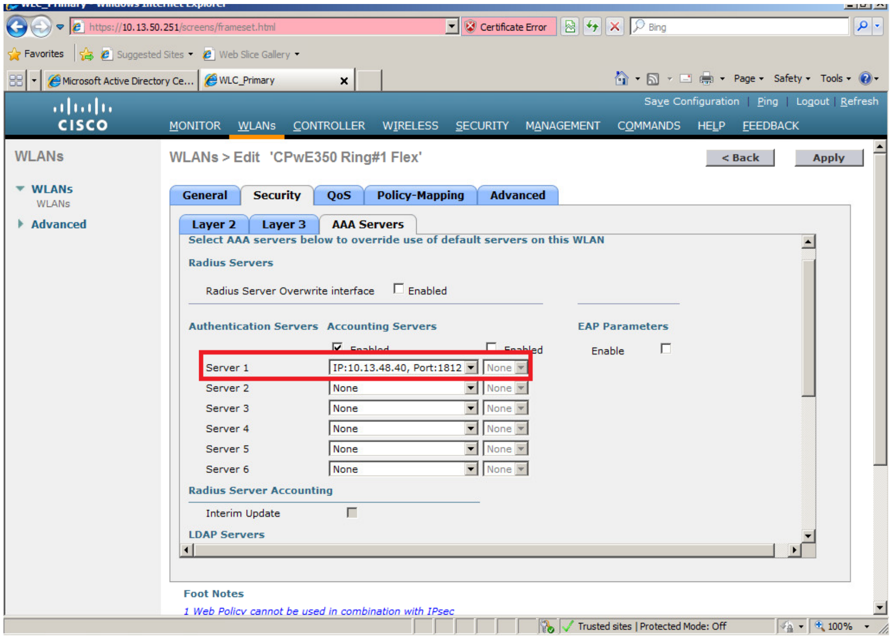
Protected Management Frame
PMF Disabled

WPA+WPA2 Parameters
WPA Policy ☐
WPA2 Policy ☑
WPA2 Encryption ☑ AES ☐ TKIP

Authentication Key Management
802.1X ☑ Enable
CCKM ☑ Enable

Foot Notes
1 Web Policy cannot be used in combination with IPsec

Figure 3-33 WLC WLAN Security AAA Server


https://10.13.50.251/screens/frameset.html
Certificate Error
Bing
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Ce...
WLC_Primary
Page
Safety
Tools
Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers
Trusted sites | Protected Mode: Off
100%
298356

WLANs > Edit 'CPwE350 Ring#1 Flex'

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface ☐ Enabled

Authentication Servers	Accounting Servers	EAP Parameters
☑ Enabled	☐ Enabled	Enable ☐

	Authentication Servers	Accounting Servers
Server 1	IP:10.13.48.40, Port:1812	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

Radius Server Accounting

Interim Update ☐

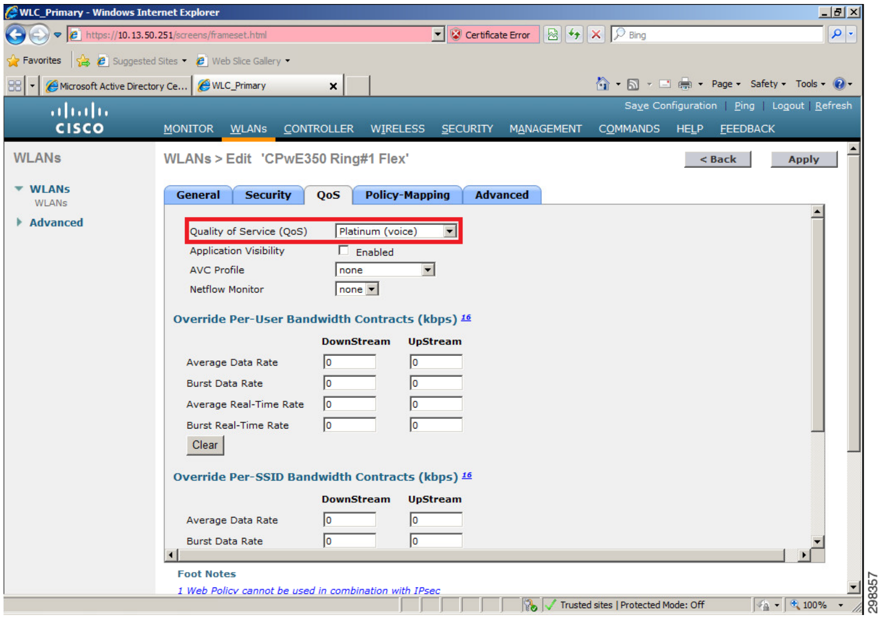
LDAP Servers

Foot Notes

1 Web Policy cannot be used in combination with IPsec

Step 4 It is recommended to use platinum QoS profile for all WLAN, which will setup the maximum threshold for QoS mapping between customer layer 3 DSCP, CAPWAP L3 IP tunnel DSCP and 802.11e UP value. During this mapping process, the original DSCP value remains intact in the data payload. WLAN QoS will ensure differentiated service treatment for all traffic flows when they across CAPWAP tunnel and wireless link. Figure 3-34 shows the WLAN QoS profile.

Figure 3-34 WLC WLAN QoS Profile


WLC_Primary - Windows Internet Explorer
https://10.13.50.251/screens/frameset.html
Certificate Error
Bing
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Ce...
WLC_Primary
Page
Safety
Tools
Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General Security QoS Policy-Mapping Advanced
Clear
Trusted sites | Protected Mode: Off
100%
298357

WLANs > Edit 'CPwE350 Ring#1 Flex'

Quality of Service (QoS) Platinum (voice)

Application Visibility ☐ Enabled

AVC Profile none

Netflow Monitor none

Override Per-User Bandwidth Contracts (kbps) [16]

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Override Per-SSID Bandwidth Contracts (kbps) [16]

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0

Foot Notes

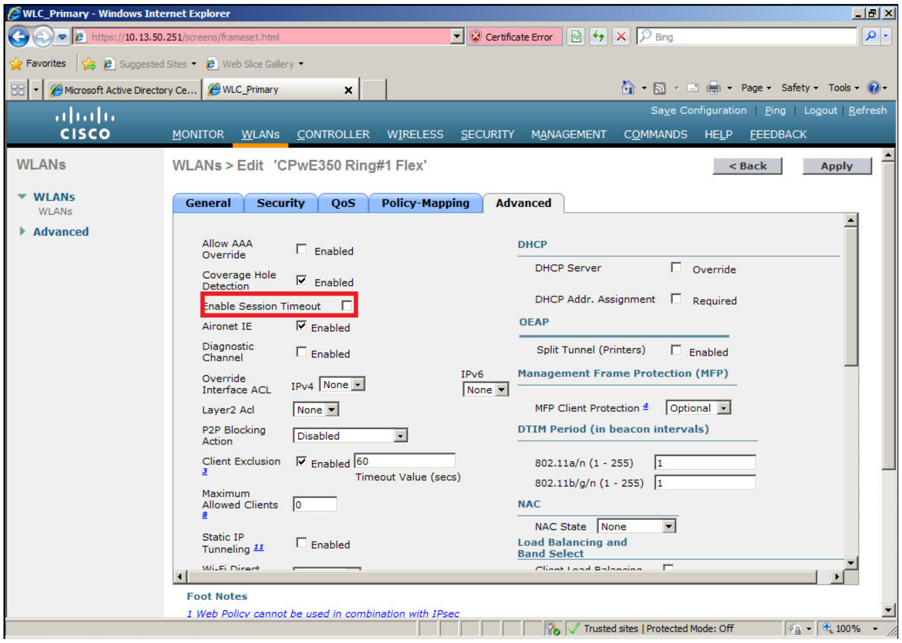
1 Web Policy cannot be used in combination with IPsec

Step 5 In the WLC WLAN *Advanced* sub-panel, disable the *Session Timeout Enable* option. A session timeout mechanism is used by WLC to remove stale client entries, and its default value is 1800 seconds. During the session timeout, LWAP and WLC will temporarily bring down the authenticated session which will create network convergence and may cause an IACS application timeout. It is recommended to turn the session-timeout setting off, which will cause the timeout to default to every 24 hours to process client entries cleanup task.

Note The maximum session timeout in the Unified WLAN using 802.1X security methods is 24 hours. The application needs to be designed to take this into account.

Figure 3-35 shows the WLAN advanced sub-panel configuration details.

Figure 3-35 WLC WLAN Advanced Configuration Part 1


WLC_Primary - Windows Internet Explorer
https://10.13.50.251/screens/frameset.html
Certificate Error
Bing
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Ce...
WLC_Primary
Page
Safety
Tools
CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Policy-Mapping
Advanced
Trusted sites | Protected Mode: Off
100%
298358

WLANs > Edit 'CPwE350 Ring#1 Flex'

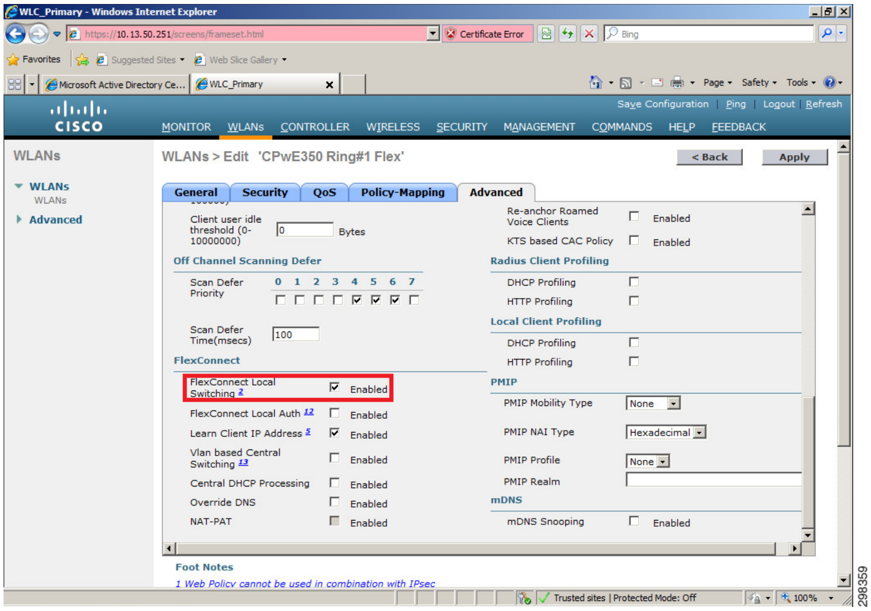
Allow AAA Override ☐ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☐
Aironet IE ☑ Enabled
Diagnostic Channel ☐ Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
P2P Blocking Action Disabled
Client Exclusion 3 ☑ Enabled 60 Timeout Value (secs)
Maximum Allowed Clients 8 0
Static IP Tunneling 11 ☐ Enabled
Wi-Fi Direct

DHCP
DHCP Server ☐ Override
DHCP Addr. Assignment ☐ Required
OEAP
Split Tunnel (Printers) ☐ Enabled
Management Frame Protection (MFP)
MFP Client Protection 4 Optional
DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1
NAC
NAC State None
Load Balancing and Band Select
Client Load Balancing ☐

Foot Notes
1 Web Policy cannot be used in combination with IPsec

Step 6 Also on the *Advanced* panel, select the *FlexConnect Local Switching* option once LWAP FlexConnect mode is enabled. See Figure 3-36.

Figure 3-36 WLC WLAN Advanced Configuration Part 2


WLC_Primary - Windows Internet Explorer
https://10.13.50.251/screens/frameset.html
Certificate Error
Bing
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Ce...
WLC_Primary
Page
Safety
Tools
CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Policy-Mapping
Advanced
Trusted sites | Protected Mode: Off
100%
298359

WLANs > Edit 'CPwE350 Ring#1 Flex'

Client user idle threshold (0-10000000) 0 Bytes

Off Channel Scanning Defer

Scan Defer Priority	0	1	2	3	4	5	6	7
	□	□	□	□	☑	☑	☑	□

Scan Defer Time(msecs) 100

FlexConnect

- FlexConnect Local Switching [2] ☑ Enabled
- FlexConnect Local Auth [12] □ Enabled
- Learn Client IP Address [5] ☑ Enabled
- Vlan based Central Switching [13] □ Enabled
- Central DHCP Processing □ Enabled
- Override DNS □ Enabled
- NAT-PAT □ Enabled

- Re-anchor Roamed Voice Clients □ Enabled
- KTS based CAC Policy □ Enabled

Radius Client Profiling

- DHCP Profiling □
- HTTP Profiling □

Local Client Profiling

- DHCP Profiling □
- HTTP Profiling □

PMIP

- PMIP Mobility Type None
- PMIP NAI Type Hexadecimal
- PMIP Profile None
- PMIP Realm

mDNS

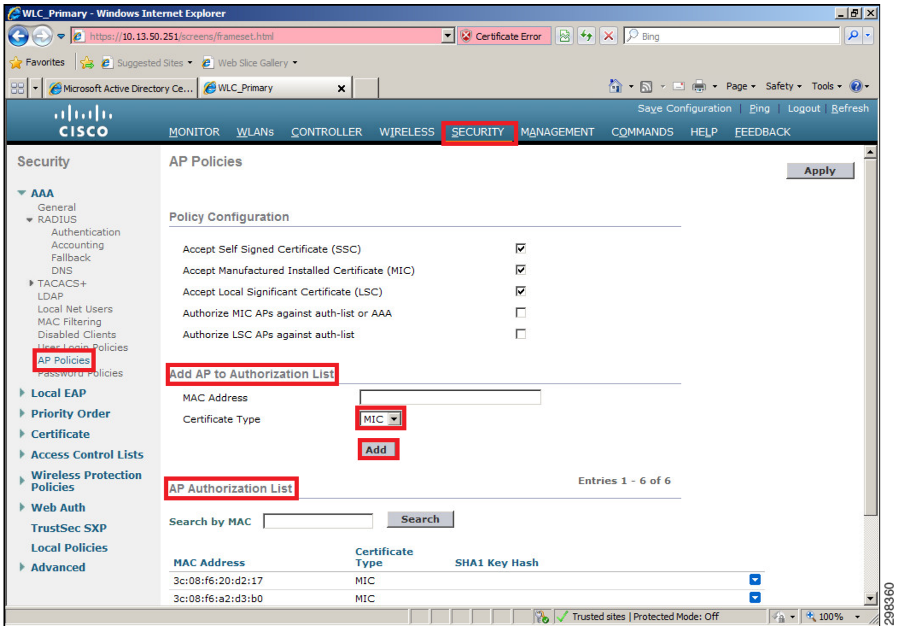
- mDNS Snooping □ Enabled

Foot Notes

1 Web Policy cannot be used in combination with IPsec

Step 7 After WLAN configuration is completed, add the LWAP MAC address with Manufacturer Installed Certificate (MIC) into WLC security *AP Policies* as shown in Figure 3-37. By default, WLC won't allow LWAP to register based on its default Security setting until you have added the LWAP MAC address with MIC.

Figure 3-37 WLC Security AP Policies



AP Policies

Policy Configuration

- Accept Self Signed Certificate (SSC) ☑
- Accept Manufactured Installed Certificate (MIC) ☑
- Accept Local Significant Certificate (LSC) ☑
- Authorize MIC APs against auth-list or AAA □
- Authorize LSC APs against auth-list □

Add AP to Authorization List

MAC Address

Certificate Type MIC

AP Authorization List

Entries 1 - 6 of 6

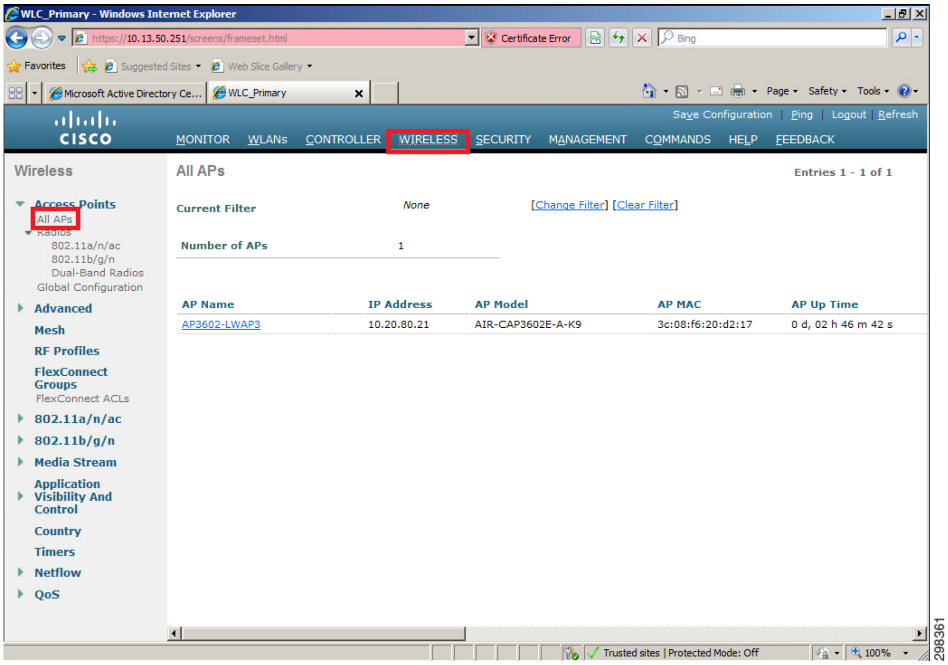
Search by MAC

MAC Address	Certificate Type	SHA1 Key Hash
3c:08:f6:20:d2:17	MIC	
3c:08:f6:a2:d3:b0	MIC	

WLC Wireless and LWAP FlexConnect Setup

Step 1 The WLC *Wireless* sub-panel is used for wireless radio related configurations. Figure 3-38 shows the general overview of LWAP status. 802.11a/n/ac and QoS-related parameters can be configured by selecting the corresponding directory.

Figure 3-38 WLC Wireless Overview



All APs

Entries 1 - 1 of 1

Current Filter *None* [Change Filter] [Clear Filter]

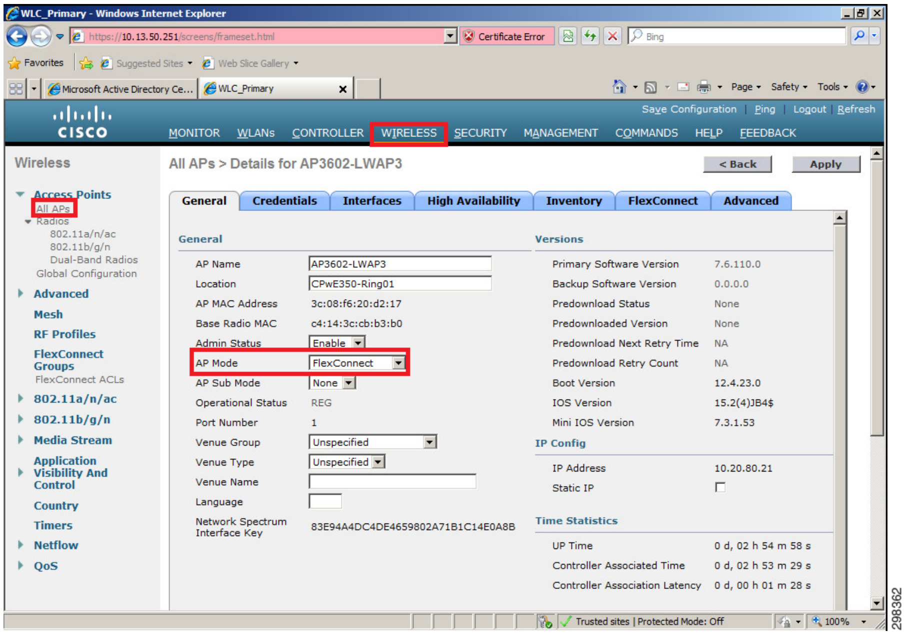
Number of APs 1

AP Name	IP Address	AP Model	AP MAC	AP Up Time
AP3602-LWAP3	10.20.80.21	AIR-CAP3602E-A-K9	3c:08:f6:20:d2:17	0 d, 02 h 46 m 42 s

Note LWAP can use trunk port or access port to attach to the access network. It is recommended to use a trunk port (native VLAN and access VLAN) to separate management traffic from WLAN data traffic. Without WLC VLAN mapping, all LWAPs will get DHCP addresses from the native VLAN DHCP helper subnet. After the VLAN mapping feature has been applied, the LWAP will get an address from its local access network data VLAN subnet.

Step 2 After the LWAP has registered with the WLC, change the AP mode to FlexConnect as shown in Figure 3-39, which will reload the AP and convert it to FlexConnect mode. Figure 3-40 shows the new FlexConnect tab that appears after conversion.

Figure 3-39 WLC LWAP FlexConnect Overview


WLC_Primary - Windows Internet Explorer
https://10.13.50.251/screens/frameset.html
Certificate Error
Favorites
Microsoft Active Directory Ce...
WLC_Primary
Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
RF Profiles
FlexConnect Groups
FlexConnect ACLs
802.11a/n/ac
802.11b/g/n
Media Stream
Application Visibility And Control
Country
Timers
Netflow
QoS
< Back
Apply
General Credentials Interfaces High Availability Inventory FlexConnect Advanced
Trusted sites | Protected Mode: Off
100%
298362

All APs > Details for AP3602-LWAP3

General

AP Name	AP3602-LWAP3
Location	CPwE350-Ring01
AP MAC Address	3c:08:f6:20:d2:17
Base Radio MAC	c4:14:3c:cb:b3:b0
Admin Status	Enable
AP Mode	FlexConnect
AP Sub Mode	None
Operational Status	REG
Port Number	1
Venue Group	Unspecified
Venue Type	Unspecified
Venue Name	
Language	
Network Spectrum Interface Key	83E94A4DC4DE4659802A71B1C14E0A8B

Versions

Primary Software Version	7.6.110.0
Backup Software Version	0.0.0.0
Predownload Status	None
Predownloaded Version	None
Predownload Next Retry Time	NA
Predownload Retry Count	NA
Boot Version	12.4.23.0
IOS Version	15.2(4)JB4$
Mini IOS Version	7.3.1.53

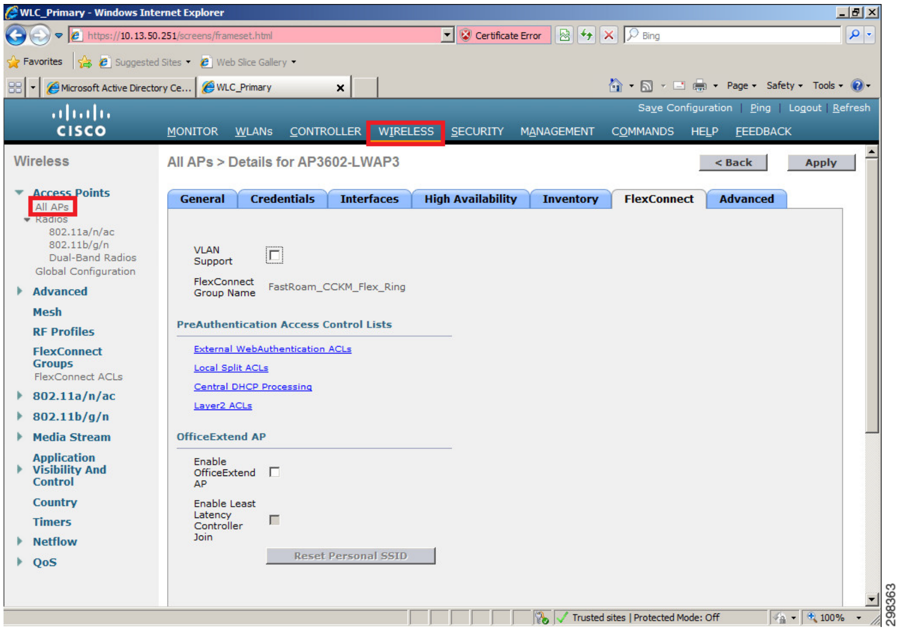
IP Config

IP Address	10.20.80.21
Static IP	□

Time Statistics

UP Time	0 d, 02 h 54 m 58 s
Controller Associated Time	0 d, 02 h 53 m 29 s
Controller Association Latency	0 d, 00 h 01 m 28 s

Figure 3-40 WLC LWAP FlexConnect LWAP


WLC_Primary - Windows Internet Explorer
https://10.13.50.251/screens/frameset.html
Certificate Error
Favorites
Microsoft Active Directory Ce...
WLC_Primary
Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
RF Profiles
FlexConnect Groups
FlexConnect ACLs
802.11a/n/ac
802.11b/g/n
Media Stream
Application Visibility And Control
Country
Timers
Netflow
QoS
< Back
Apply
General Credentials Interfaces High Availability Inventory FlexConnect Advanced
Reset Personal SSID
Trusted sites | Protected Mode: Off
100%
298363

All APs > Details for AP3602-LWAP3

VLAN Support	□
FlexConnect Group Name	FastRoam_CCKM_Flex_Ring

PreAuthentication Access Control Lists

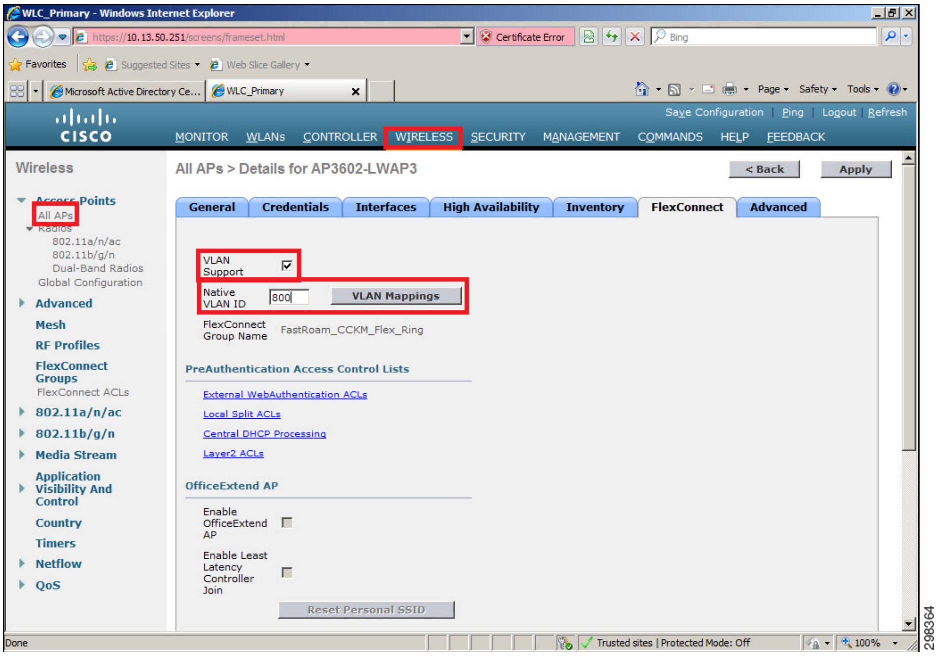
External WebAuthentication ACLs
Local Split ACLs
Central DHCP Processing
Layer2 ACLs

OfficeExtend AP

Enable OfficeExtend AP	□
Enable Least Latency Controller Join	□

Step 3 The FlexConnect VLAN mapping feature needs to be enabled as shown in Figure 3-41 and Figure 3-42. As shown in Figure 3-41, enable VLAN support, and fill the access network native VLAN to the desired value. Then click *VLAN Mappings* to access the view shown in Figure 3-42 for configuring WLAN to VLAN ID mapping.

Figure 3-41 WLC LWAP FlexConnect VLAN Mapping Part 1



All APs > Details for AP3602-LWAP3

VLAN Support ☑

Native VLAN ID 800

FlexConnect Group Name FastRoam_CCKM_Flex_Ring

PreAuthentication Access Control Lists

External WebAuthentication ACLs

Local Split ACLs

Central DHCP Processing

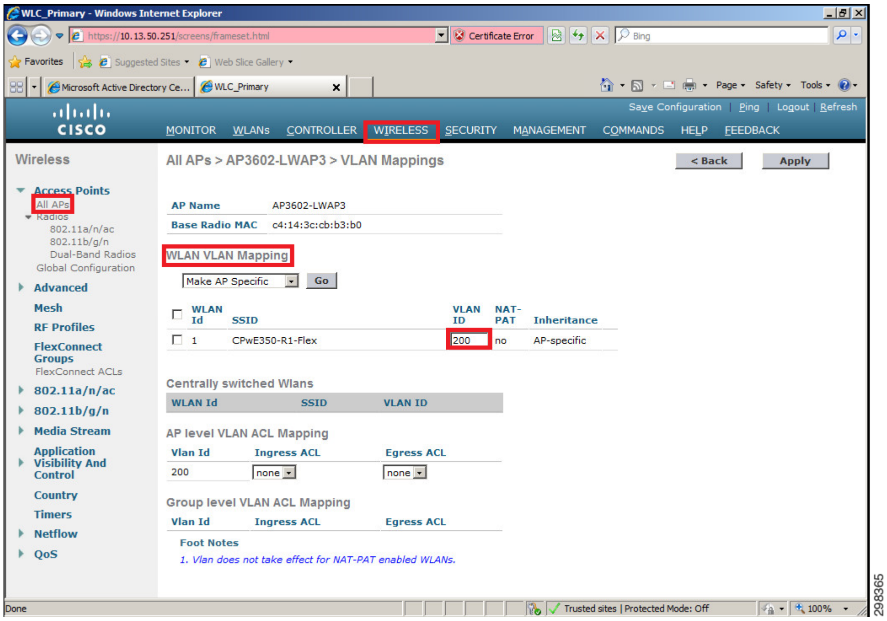
Layer2 ACLs

OfficeExtend AP

Enable OfficeExtend AP □

Enable Least Latency Controller Join □

Figure 3-42 WLC LWAP FlexConnect VLAN Mapping Part 2



All APs > AP3602-LWAP3 > VLAN Mappings

AP Name AP3602-LWAP3

Base Radio MAC c4:14:3c:cb:b3:b0

WLAN VLAN Mapping

Make AP Specific

□	WLAN Id	SSID	VLAN ID	NAT-PAT	Inheritance
□	1	CPwE350-R1-Flex	200	no	AP-specific

Centrally switched Wlans

WLAN Id	SSID	VLAN ID

AP level VLAN ACL Mapping

Vlan Id	Ingress ACL	Egress ACL
200	none	none

Group level VLAN ACL Mapping

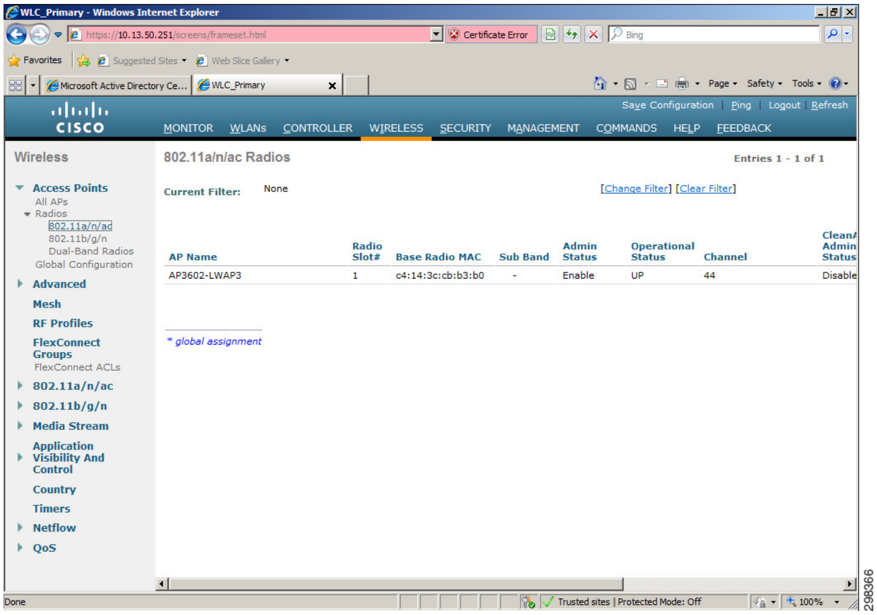
Vlan Id	Ingress ACL	Egress ACL

Foot Notes

1. Vlan does not take effect for NAT-PAT enabled WLANs.

Step 4 Click the highlighted drop-down box to configure each LWAP and assign radio channel manually as shown in Figure 3-43. Figure 3-44 shows the Radio assignment after manual configuration. When a LWAP registers to the WLC and comes online, it will get its wireless radio channel randomly. Figure 3-45 shows an initial LWAP status page with LWAP radio channel assignment.

Figure 3-43 WLC LWAP Radio



802.11a/n/ac Radios

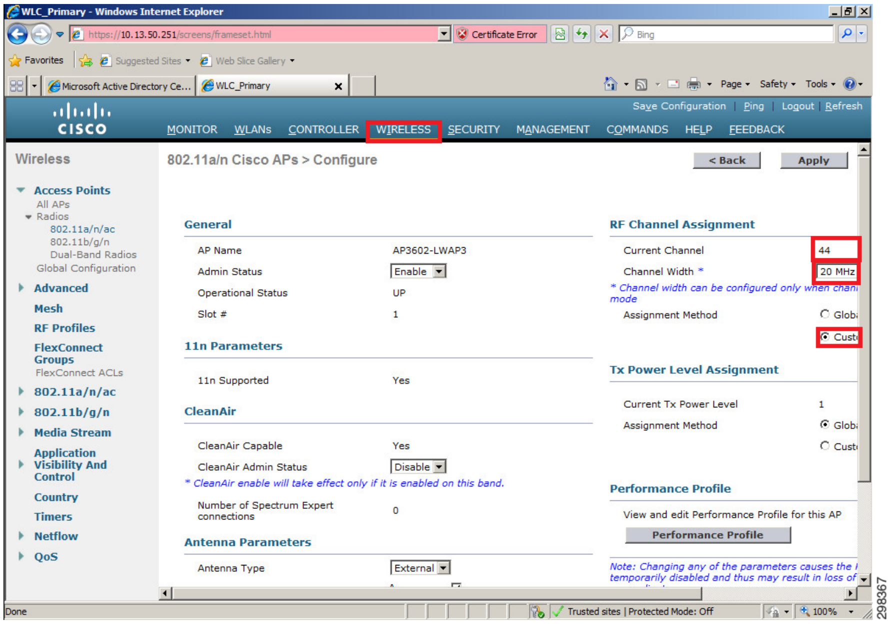
Entries 1 - 1 of 1

Current Filter: None [Change Filter] [Clear Filter]

AP Name	Radio Slot#	Base Radio MAC	Sub Band	Admin Status	Operational Status	Channel	CleanA Admin Status
AP3602-LWAP3	1	c4:14:3c:cb:b3:b0	-	Enable	UP	44	Disable

* global assignment

Figure 3-44 WLC LWAP Configure Radio Channel



802.11a/n Cisco APs > Configure

General

AP Name: AP3602-LWAP3
Admin Status: Enable
Operational Status: UP
Slot #: 1

11n Parameters

11n Supported: Yes

CleanAir

CleanAir Capable: Yes
CleanAir Admin Status: Disable

* CleanAir enable will take effect only if it is enabled on this band.

Number of Spectrum Expert connections: 0

Antenna Parameters

Antenna Type: External

RF Channel Assignment

Current Channel: 44
Channel Width *: 20 MHz

* Channel width can be configured only when chan mode

Assignment Method: ○ Glob ● Cust

Tx Power Level Assignment

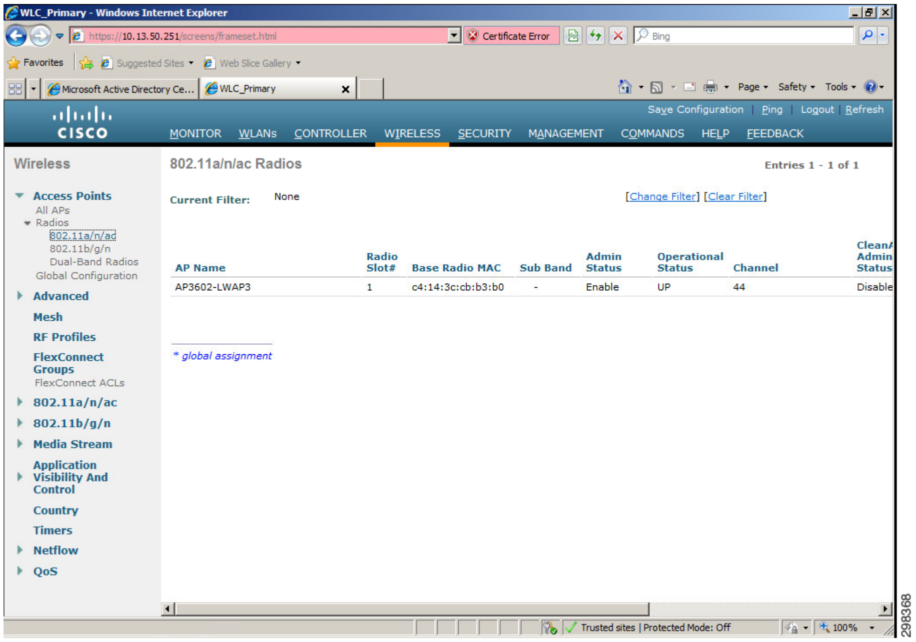
Current Tx Power Level: 1
Assignment Method: ● Glob ○ Cust

Performance Profile

View and edit Performance Profile for this AP

Note: Changing any of the parameters causes the temporarily disabled and thus may result in loss of

Figure 3-45 WLC LWAP Radio After Assignment



802.11a/n/ac Radios

Entries 1 - 1 of 1

Current Filter: None

[Change Filter] [Clear Filter]

AP Name	Radio Slot#	Base Radio MAC	Sub Band	Admin Status	Operational Status	Channel	CleanA Admin Status
AP3602-LWAP3	1	c4:14:3c:cb:b3:b0	-	Enable	UP	44	Disable

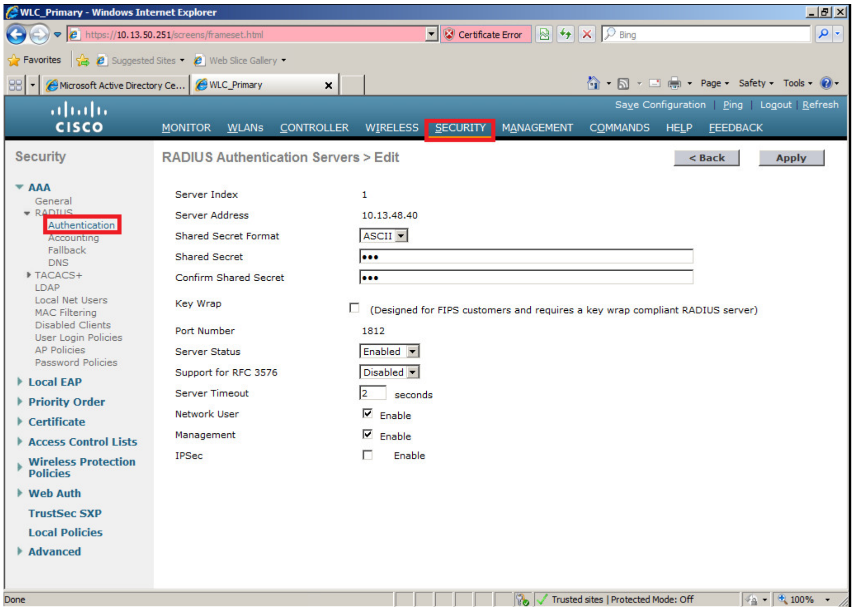
* global assignment

WLC Security and Optional LSC Certificate Setup

For Unified WLAN, it is recommended to use EAP-TLS for comprehensive device authentication using a certificate, where WLC assumes the authentication proxy server role.

Step 1 Configure the shared secret between WLC AAA proxy and ACS 5.5 RADIUS server during the initial setup. Leave the rest of the RADIUS configuration as default. Figure 3-46 shows the WLC AAA proxy configuration.

Figure 3-46 WLC Security AAA Setup

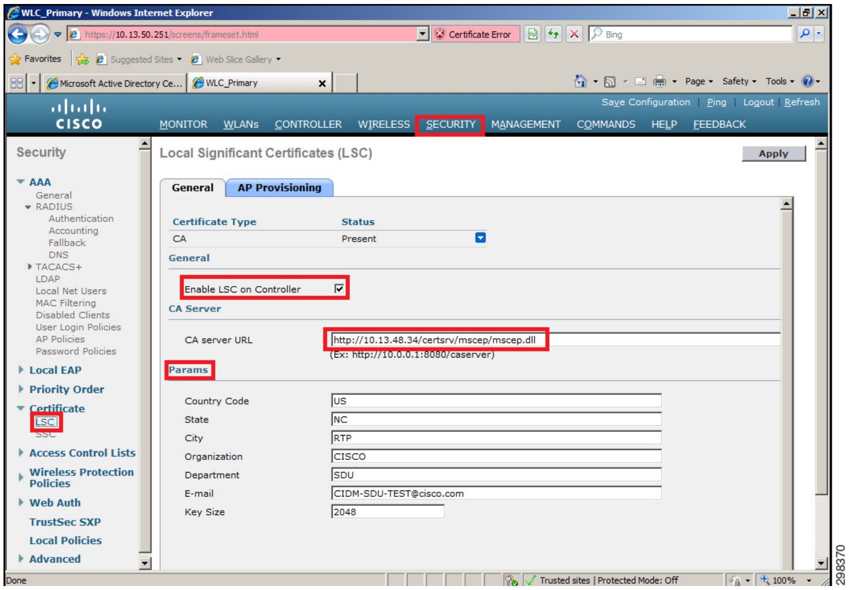


RADIUS Authentication Servers > Edit

Server Index	1
Server Address	10.13.48.40
Shared Secret Format	ASCII
Shared Secret	•••
Confirm Shared Secret	•••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Disabled
Server Timeout	2 seconds
Network User	☑ Enable
Management	☑ Enable
IPSec	□ Enable

Step 2 Add the LWAP MAC address into the provisioning list and enable the AP provisioning radio button to push Locally Significant Certificate (LSC) to the LWAP. The WLC and LWAP act as proxy relay under central authentication and local switching and it is not necessary to install the certificate during WGB and its client device's authentication. However, as an integrated solution, WLC and LWAP still need an optional LSC certificate to make sure every device is secured on the plant floor. The detailed configuration is shown in highlighted fields in Figure 3-47, and the LWAP certificate need to be pushed by WLC, which is shown in Figure 3-48. Figure 3-49 shows the LWAP certificate status.

Figure 3-47 WLC LSC Certificate Setup



Local Significant Certificates (LSC)

Certificate Type	Status
CA	Present

General

Enable LSC on Controller ☑

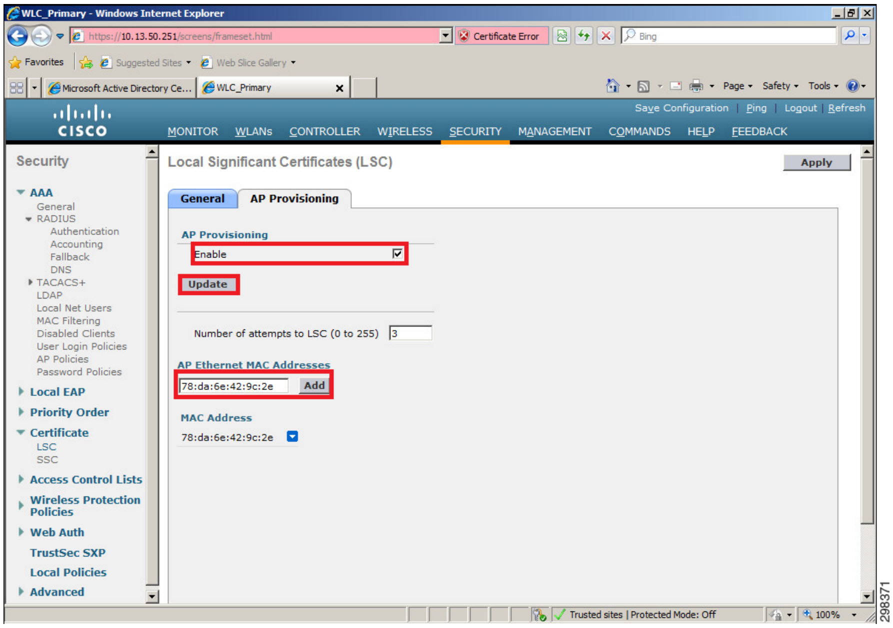
CA Server

CA server URL: http://10.13.48.34/certsrv/mscep/mscep.dll
(Ex: http://10.0.0.1:8080/caserver)

Params

Country Code	US
State	NC
City	RTP
Organization	CISCO
Department	SDU
E-mail	CIDM-SDU-TEST@cisco.com
Key Size	2048

Figure 3-48 WLC LWAP Certificate Setup



Local Significant Certificates (LSC)

Apply

General | AP Provisioning

AP Provisioning

Enable ☑

Update

Number of attempts to LSC (0 to 255) 3

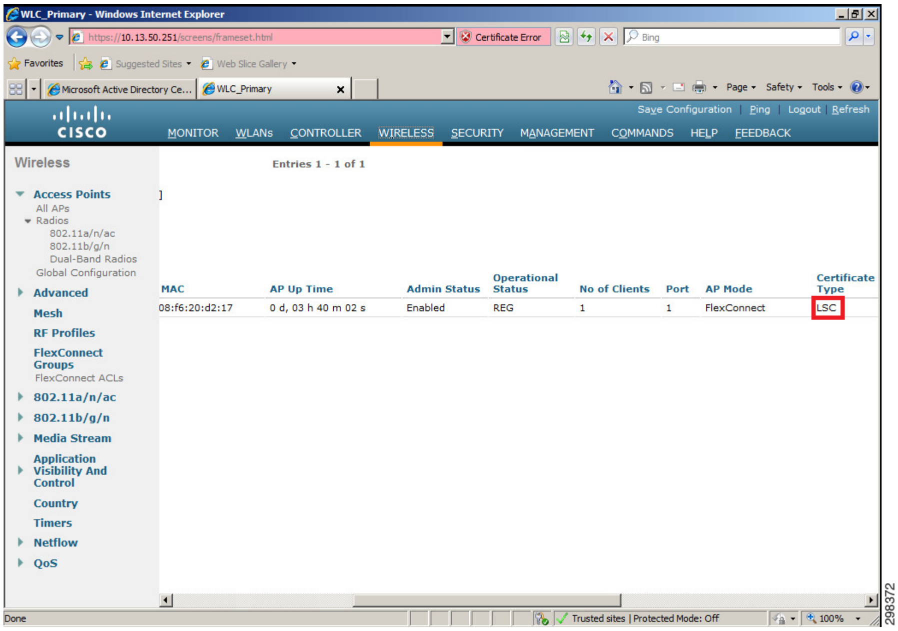
AP Ethernet MAC Addresses

78:da:6e:42:9c:2e Add

MAC Address

78:da:6e:42:9c:2e

Figure 3-49 WLC LWAP LSC Certificate Status



Entries 1 - 1 of 1

MAC	AP Up Time	Admin Status	Operational Status	No of Clients	Port	AP Mode	Certificate Type
08:f6:20:d2:17	0 d, 03 h 40 m 02 s	Enabled	REG	1	1	FlexConnect	LSC

Note By default, certificate services in the Root-CA on the Windows Server require password challenge. This feature can be disabled. See Appendix C, "Server Infrastructure Configuration" for details.

Workgroup Bridge (WGB) Initial Setup and Configuration

In the Unified WLAN environment, some IO and PAC devices are required to communicate with each other via wireless network. These devices are attached by APs configured as WGBs.

The WGB mode can be configured on the Stratix 5100 autonomous AP or on the Cisco lightweight AP converted to the autonomous mode.

WGB Initial Setup (Autonomous Mode)

The initial setup for Stratix 5100 or Cisco autonomous AP include assigning the management IP address and the device role. Please refer to Autonomous WLAN Configuration, page 3-1.

WGB Initial Setup (Lightweight Mode)

In order to configure a Cisco lightweight AP as a WGB, it needs to be converted to the autonomous mode. The following are the necessary steps for conversion.

Note WGB staging using the router prompt (Option 1) is preferred. However, under some circumstances, WGB conversion will experience timeout during archive download because image size is too big. If this occurs, it is recommended to use the ROMmon prompt (Option 2) to convert LWAP into WGB.

WGB Staging under Router Prompt (Option 1)

Step 1 Under router enable prompt, enter following CLI to enter configuration mode.

```
debug capwap console cli
debug capwap client no-reload
```

Step 2 Configure BVI interface with static provisioning network IP address.

```
capwap ap ip address 192.168.254.85 255.255.255.0
capwap ap ip default-gateway 192.168.254.1
```

Step 3 Download WGB image from the TFTP server.

```
archive download-sw /overwrite / reload
tftp://192.168.254.20/ap3g2-k9w7-tar.152-4.JA1.tar
```

WGB Staging under ROMmon Prompt (Option 2)

Step 1 Reload or power off LWAP and press "ESC" to enter into ROMmon prompt.

Step 2 Issue the following CLIs under ROMmon prompt to start LWAP to WGB conversion.

```
tftp_init
flash_inti
set IP_ADDR 192.168.254.85
set NETMASK 255.255.255.0
set DEFAULT_ROUTER 192.168.254.1
ether_init
tar -xtract tftp://192.168.254.20/ap3g2-k9w7-tar.152-4.JB3a.tar flash:
set BOOT flash://ap3g2-k9w7-mx.152-4.JB3a/ap3g2-k9w7-xx.152-4.JB3a
boot
```

Note Under some circumstance, WGB radio related index file does not get downloaded. In this case, it is recommended to repeat WGB initial setup under router prompt (option 1) to fix this issue.

WGB Certificate Setup

The WGB initial setup requires a dedicated provisioning network with open authentication. After the AP has been successfully converted into WGB mode, we need to install the certificate for the EAP-TLS security profile before changing the SSID into production environment.

Note It is assumed before proceeding with the following steps that the Unified WLAN Root-CA has been set up successfully (as shown in previous section).

Step 1 LWAP needs to be configured with a provisioning WLAN (SSID) with open authentication. In addition, the WGB needs to be configured with the following commands to get IP connectivity to the Root-CA:

```
!
dot11 ssid CPwE350-R1-Flex
 authentication open
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 ssid CPwE350-R1-Flex
 !
 antenna gain 0
 station-role workgroup-bridge
!
interface BVI1
 ip address dhcp
 load-interval 30
!
```

Step 2 Configure a crypto public RSA key with a modulus size of 2048.

```
!
crypto key generate rsa label EAP-TLS2048 modulus 2048 exportable
!
```

Step 3 Configure WGB security trustpoint and certificate download parameters.

```
!
ip domain name cpwe.cisco.local
!
crypto pki trustpoint CPwE350-CA
enrollment url http://10.13.48.34/certsrv/mscep/mscep.dll
subject-name cn=AP2602-F-WGB02.cpwe.cisco.local
revocation-check none
auto-enroll 90
rsakeypair EAP-TLS2048
!
crypto pki authenticate CPwE350-CA
!
```

Step 4 Save installed certificate into WGB NVRAM using "write memory".

Note If a "write erase" command is given on the WGB, it will erase the certificate from NVRAM.

Note The certificate RSA key modulus size of 2048 needs to be the same on both WGB and Root-CA side. WGB without certificate does not have the ability to communicate directly with Root-CA other than wireless link. Auto-enrollment for the certificate is set to 90% of quota; follow the wizard and enter *Yes* to the question to install certificate into WGB.

WGB SSID and Security Configuration

Step 1 Configure SSID parameters for the production network.

```
!
dot11 ssid CPwE350-R1-Flex
   no authentication open
   no ids mfp client
   authentication network-eap CPwE350-EAPTLS
   authentication key-management wpa version 2
   dot1x credentials CPwE350-dot1x
   dot1x eap profile CPwE350-EAPTLS
!
```

Step 2 Configure authentication method profile.

```
!
eap profile CPwE350-EAPTLS
 method tls
!
```

Step 3 Configure dot1x security profile and credentials.

```
!
dot1x credentials CPwE350-dot1x
 username AP2602-R-WGB02
 pki-trustpoint CPwE350-CA
!
```

Step 4 Configure the radio interface.

```
!
interface Dot11Radio1
!
encryption mode ciphers aes-ccm
ssid CPwE350-R1-Flex
!
```

Fast Roaming WLAN

Based on the design recommendations given in Chapter 2, "System Design Considerations," the following sections explain the detailed steps for fast roaming WLAN configuration.

WLC and LWAP Configuration for Fast Roaming

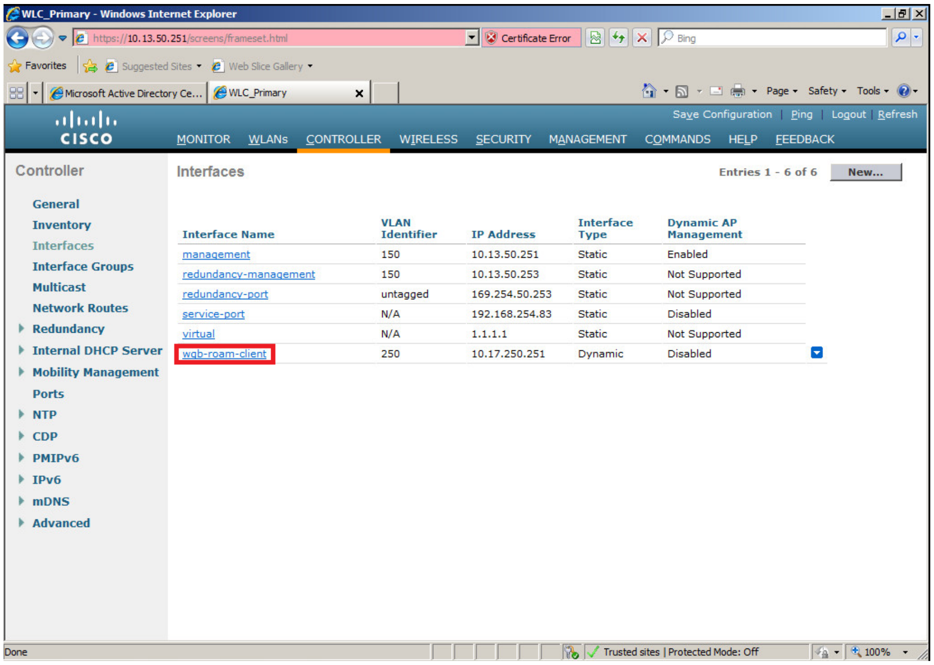
WLC configurations for fast roaming WGBs share a majority of the configurations as stationary WGBs with the following differences:

- Use dynamic interface on the WLC.
- Use LWAP in local mode (not FlexConnect) to achieve central authentication and switching model.
- WLAN should use CCKM key management protocol.

Note It is recommended that the total number of Ethernet devices on a Single VLAN (wired or wireless) should be less than 200 to restrict the amount of broadcast traffic. In a large scale plant-wide environment with many fast roaming devices, it is recommended to use single fast roaming WLAN (SSID) and associate with multiple VLANs (dynamic interfaces) in a group as shown later.

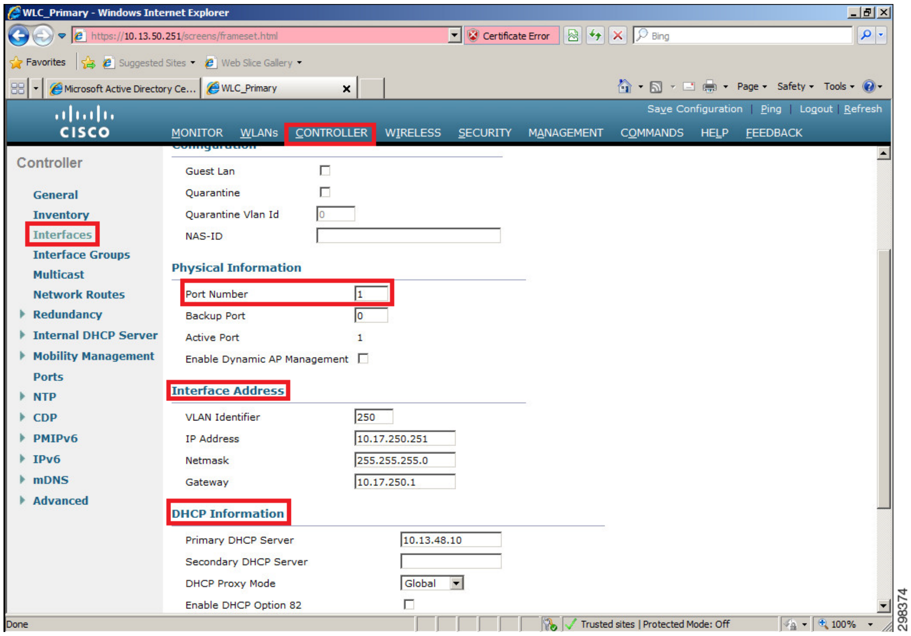
Step 1 Figure 3-50 and Figure 3-51 show the WLC dynamic interface configuration.

Figure 3-50 Controllers Dynamic Interface Configurations Part 1



Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	150	10.13.50.251	Static	Enabled
redundancy-management	150	10.13.50.253	Static	Not Supported
redundancy-port	untagged	169.254.50.253	Static	Not Supported
service-port	N/A	192.168.254.83	Static	Disabled
virtual	N/A	1.1.1.1	Static	Not Supported
wgb-roam-client	250	10.17.250.251	Dynamic	Disabled

Figure 3-51 Controllers Dynamic Interface Configurations Part 2


WLC_Primary - Windows Internet Explorer
https://10.13.50.251/screens/frameset.html
Certificate Error
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Ce...
WLC_Primary
Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
Network Routes
Redundancy
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
PMIPv6
IPv6
mDNS
Advanced
Done
Trusted sites | Protected Mode: Off
100%
298374

Guest Lan □
Quarantine □
Quarantine Vlan Id 0
NAS-ID

Physical Information

Port Number 1
Backup Port 0
Active Port 1
Enable Dynamic AP Management □

Interface Address

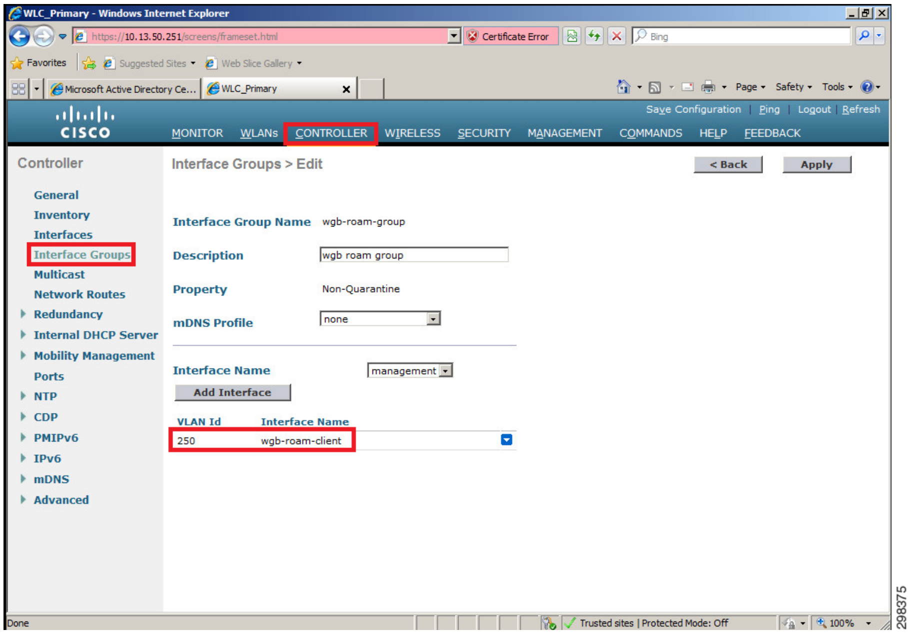
VLAN Identifier 250
IP Address 10.17.250.251
Netmask 255.255.255.0
Gateway 10.17.250.1

DHCP Information

Primary DHCP Server 10.13.48.10
Secondary DHCP Server
DHCP Proxy Mode Global
Enable DHCP Option 82 □

Step 2 If multiple dynamic interfaces have been configured, a dynamic interface group needs to be created to include all dynamic interfaces that are associated with the fast roaming WLAN. Figure 3-52 and Figure 3-53 show the dynamic interface group configurations. Figure 3-54 and Figure 3-55 show how to associate WLAN with dynamic interface groups.

Figure 3-52 Controller Dynamic Interface Group Configurations Part 1



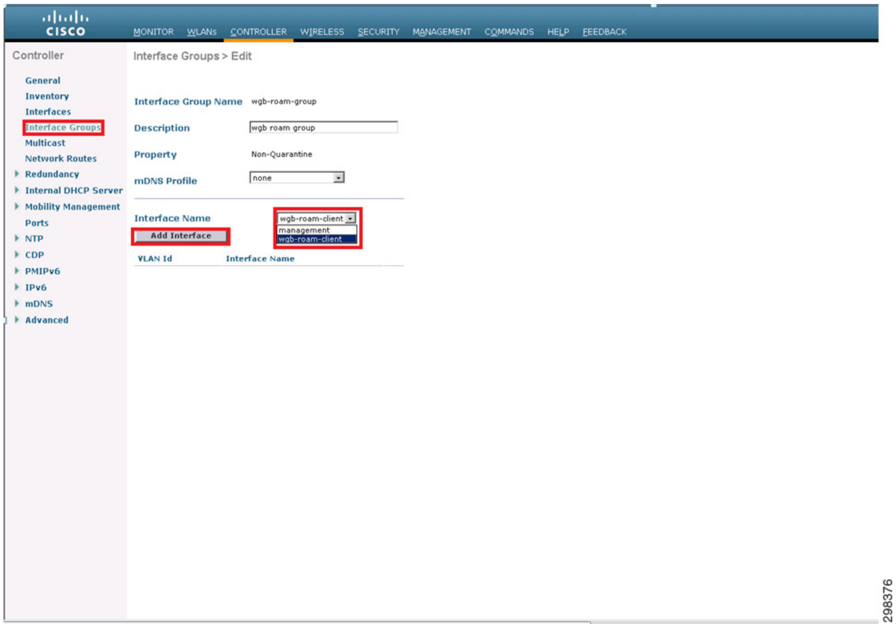
Interface Groups > Edit

Interface Group Name wgb-roam-group
Description wgb roam group
Property Non-Quarantine
mDNS Profile none

Interface Name management

VLAN Id	Interface Name
250	wgb-roam-client

Figure 3-53 Controller Dynamic Interface Group Configurations Part 2



Interface Groups > Edit

Interface Group Name wgb-roam-group

Description wgb roam group

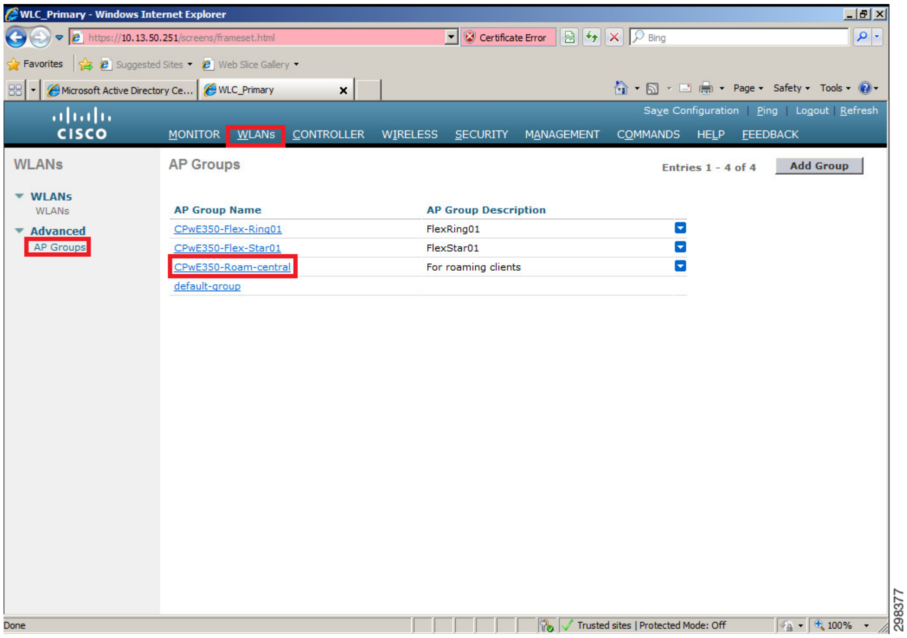
Property Non-Quarantine

mDNS Profile none

Interface Name wgb-roam-client (management, wgb-roam-client)

VLAN Id	Interface Name

Figure 3-54 AP Group Configurations Part 1

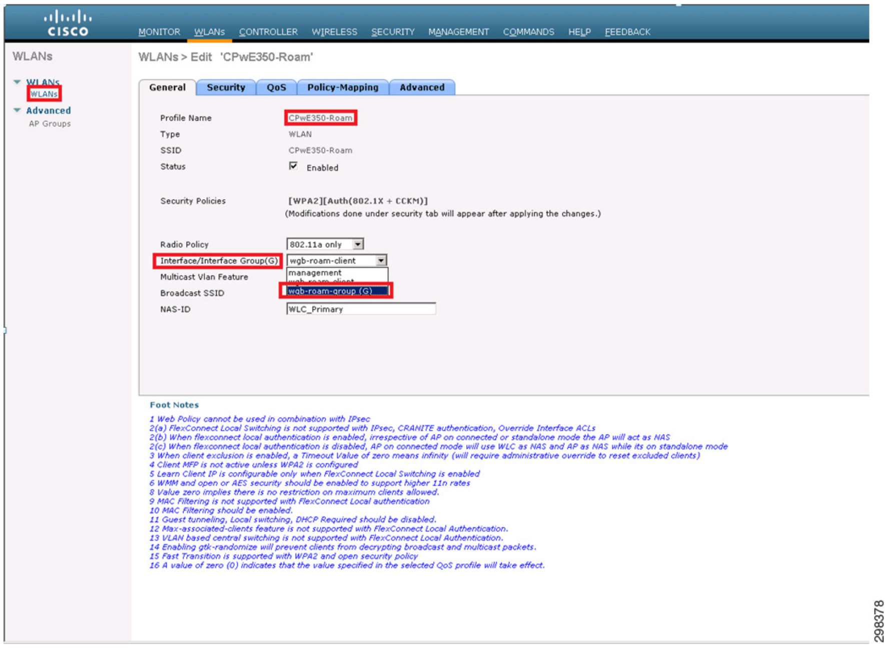

WLC_Primary - Windows Internet Explorer
https://10.13.50.251/screens/frameset.html
Certificate Error
Bing
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Ce...
WLC_Primary
Page
Safety
Tools
Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
AP Groups
Add Group
Done
Trusted sites | Protected Mode: Off
100%
298377

AP Groups

Entries 1 - 4 of 4

AP Group Name	AP Group Description
CPwE350-Flex-Ring01	FlexRing01
CPwE350-Flex-Star01	FlexStar01
CPwE350-Roam-central	For roaming clients
default-group	

Figure 3-55 AP Group Configurations Part 2



WLANs > Edit 'CPwE350-Roam'

Profile Name CPwE350-Roam
Type WLAN
SSID CPwE350-Roam
Status ☑ Enabled

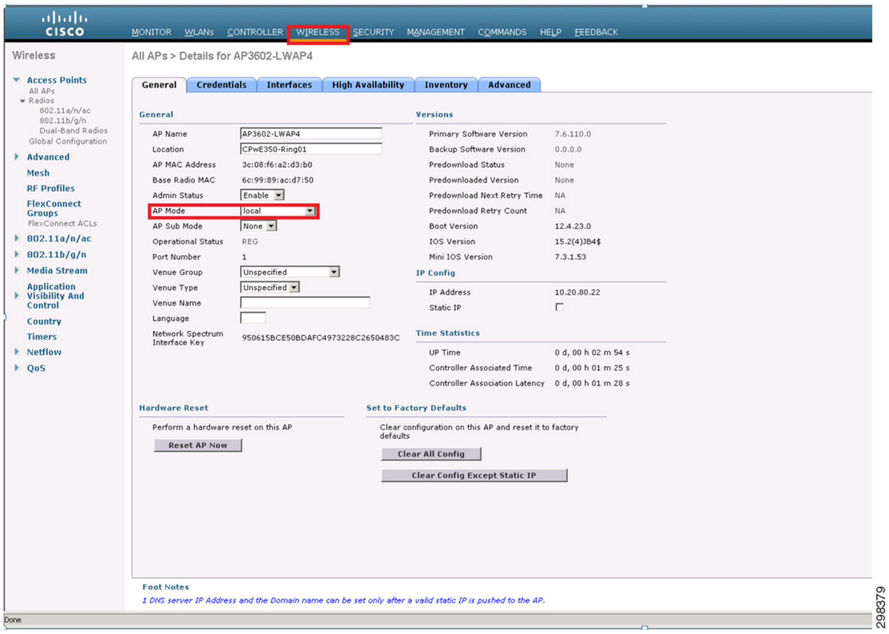
Security Policies [WPA2][Auth(802.1X + CCKM)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy 802.11a only
Interface/Interface Group(G) wgb-roam-client
management
wgb-roam-client
wgb-roam-group (G)
Multicast Vlan Feature
Broadcast SSID
NAS-ID WLC_Primary

Foot Notes
1 Web Policy cannot be used in combination with IPsec
2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
4 Client MFP is not active unless WPA2 is configured
5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled
6 WMM and open or AES security should be enabled to support higher 11n rates
8 Value zero implies there is no restriction on maximum clients allowed.
9 MAC Filtering is not supported with FlexConnect Local authentication
10 MAC Filtering should be enabled.
11 Guest tunneling, Local switching, DHCP Required should be disabled.
12 Max-associated-clients feature is not supported with FlexConnect Local Authentication.
13 VLAN based central switching is not supported with FlexConnect Local Authentication.
14 Enabling gtk-randomize will prevent clients from decrypting broadcast and multicast packets.
15 Fast Transition is supported with WPA2 and open security policy
16 A value of zero (0) indicates that the value specified in the selected QoS profile will take effect.

Step 3 In Unified WLAN WGB fast roaming, it is recommended to configure the LWAP with local mode with CCKM as shown in Figure 3-56.

Figure 3-56 Wireless LWAP Setup



All APs > Details for AP3602-LWAP4

General
AP Name AP3602-LWAP4
Location CPwE350-Ring01
AP MAC Address 3c:08:f6:a2:d3:b0
Base Radio MAC 6c:99:89:ac:d7:50
Admin Status Enable
AP Mode local
AP Sub Mode None
Operational Status REG
Port Number 1
Venue Group Unspecified
Venue Type Unspecified
Venue Name
Language
Network Spectrum Interface Key 950615BCE50BDAFC4973228C2650483C

Versions
Primary Software Version 7.6.110.0
Backup Software Version 0.0.0.0
Predownload Status None
Predownloaded Version None
Predownload Next Retry Time NA
Predownload Retry Count NA
Boot Version 12.4.23.0
IOS Version 15.2(4)JB4$
Mini IOS Version 7.3.1.53

IP Config
IP Address 10.20.80.22
Static IP □

Time Statistics
UP Time 0 d, 00 h 02 m 54 s
Controller Associated Time 0 d, 00 h 01 m 25 s
Controller Association Latency 0 d, 00 h 01 m 28 s

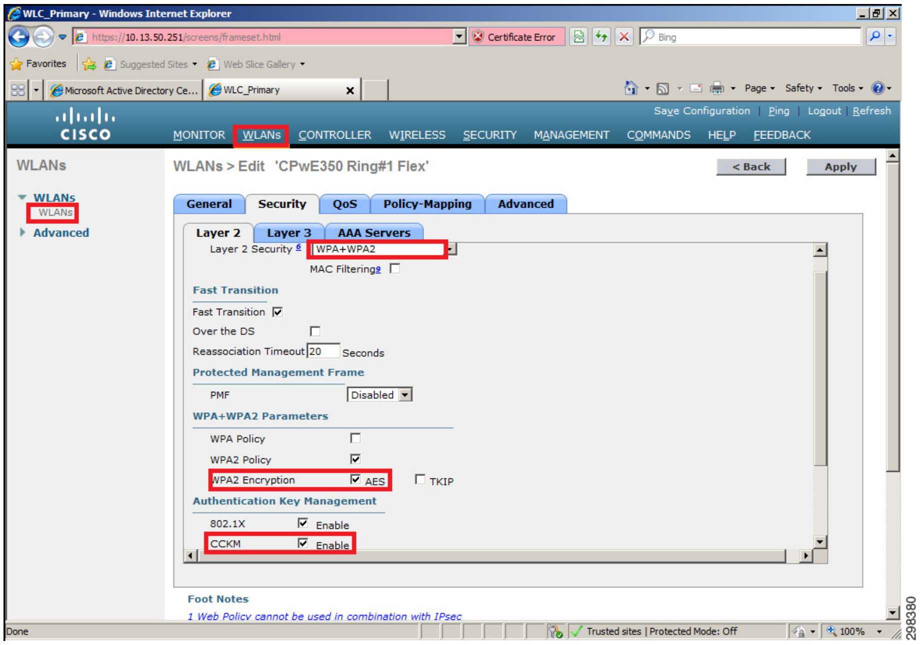
Hardware Reset
Perform a hardware reset on this AP

Set to Factory Defaults
Clear configuration on this AP and reset it to factory defaults

Foot Notes
1 DNS server IP Address and the Domain name can be set only after a valid static IP is pushed to the AP.

Step 4 EAP-TLS needs Layer 2 security method WPA2 with AES encryption. CCKM key management ensures WGB roaming between LWAPs will not result in a full EAP authentication call flow, so as to achieve faster convergence. Figure 3-57 shows the fast roaming WLAN (SSID) EAP-TLS CCKM configuration details.

Figure 3-57 WLAN CCKM Setup



WLANs > Edit 'CPwE350 Ring#1 Flex'

Layer 2 Security 6 WPA+WPA2

MAC Filtering9 □

Fast Transition

Fast Transition ☑

Over the DS □

Reassociation Timeout 20 Seconds

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP

Authentication Key Management

802.1X ☑ Enable

CCKM ☑ Enable

Foot Notes

1 Web Policy cannot be used in combination with IPsec

WGB Setup and Configuration for Fast Roaming

In Unified WLAN, fast roaming devices achieve fast convergence through CCKM enabled on both WLC WLAN and WGB sides. When a WGB roams between LWAPs, RSSI scanning threshold needs to be configured for fast roaming.

Note Refer to Workgroup Bridge (WGB) Initial Setup and Configuration, page 3-42 for configuration details about WGB initial and certificate setup.

Step 1 Configure SSID for fast roaming WGBs.

```
!
dot11 ssid CPwE350-Roam
   vlan 250
   authentication network-eap CPwE350-EAPTLS
   authentication key-management wpa version 2 cckm
   dot1x credentials CPwE350-dot1x
   dot1x eap profile CPwE350-EAPTLS
   no ids mfp client
!
```

Step 2 Configure authentication method and key management.

```
!
eap profile CPwE350-EAPTLS
 method tls
!
```

Step 3 Configure dot1x security profile and credentials.

```
!
dot1x credentials CPwE350-dot1x
```

```
 username AP2602-R-WGB05
 pki-trustpoint CPwE350-CA
!
```

Step 4 Configure radio interface parameters.

```
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 load-interval 30
 encryption vlan 250 mode ciphers aes-ccm
 ssid CPwE350-Roam
 station-role workgroup-bridge
 mobile station scan 5180
 mobile station period 2 threshold 65
 mobile station minimum-rate 6.0
!
interface Dot11Radio1.250
 encapsulation dot1Q 250 native
 no ip route-cache
 no cdp enable
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
!
interface GigabitEthernet0.250
 encapsulation dot1Q 250 native
 no ip route-cache
 no keepalive
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address dhcp
 no ip route-cache
 load-interval 30
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
```

Step 5 The example above shows the WGB configured for a single channel scanning (*mobile station scan* command). In this scenario, all APs that serve the roaming SSID are configured on the same channel. This setup provides the fastest roaming speed.

If WGBs have to use multiple channels for roaming due to channel utilization or other constraints, configure the WGB to scan these channels, for example:

```
!
interface Dot11Radio1
mobile station scan 5180 5200 5220 5240
```

Unified WLAN QoS

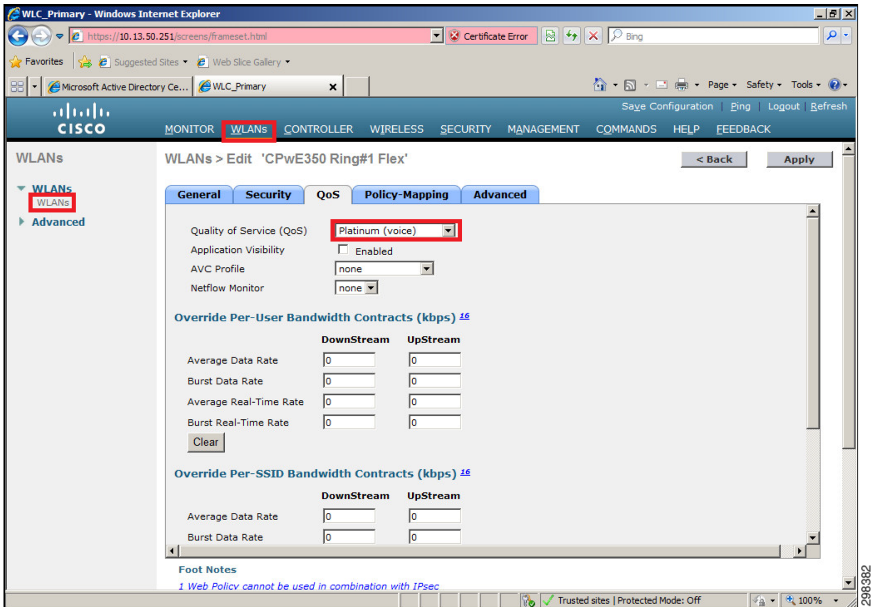
WLC QoS Profile Setup

As per the design recommendations of Chapter 2, “System Design Considerations,” the Platinum QoS profile should be chosen as shown in Table 3-1. Figure 3-58 shows the detailed configuration on the WLC.

Table 3-1 Unified WLAN QoS Mapping

Traffic Type	DSCP	802.11e UP	802.1p CoS	WLC Profile
Network Control	56 (CS7)	7	7	Platinum
CAPWAP	48 (CS6)	7	6	Platinum
Voice	46 (EF)	6	5	Platinum
Interactive Video	34 (AF41)	5	4	Gold
Streaming	26 (AF31)	4	3	Gold
X-Data	18 (AF21)	3	2	Gold
Bulk Data	10 (AF11)	2	1	Bronze
Best Effort	0 (BE)	0	0	Silver

Figure 3-58 WLC QoS Profile Configuration



WLC_Primary - Windows Internet Explorer

https://10.13.50.251/screens/frameset.html

WLANs > Edit 'CPwE350 Ring#1 Flex'

Quality of Service (QoS): Platinum (voice)
Application Visibility: ☐ Enabled
AVC Profile: none
Netflow Monitor: none

Override Per-User Bandwidth Contracts (kbps) 16

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Override Per-SSID Bandwidth Contracts (kbps) 16

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0

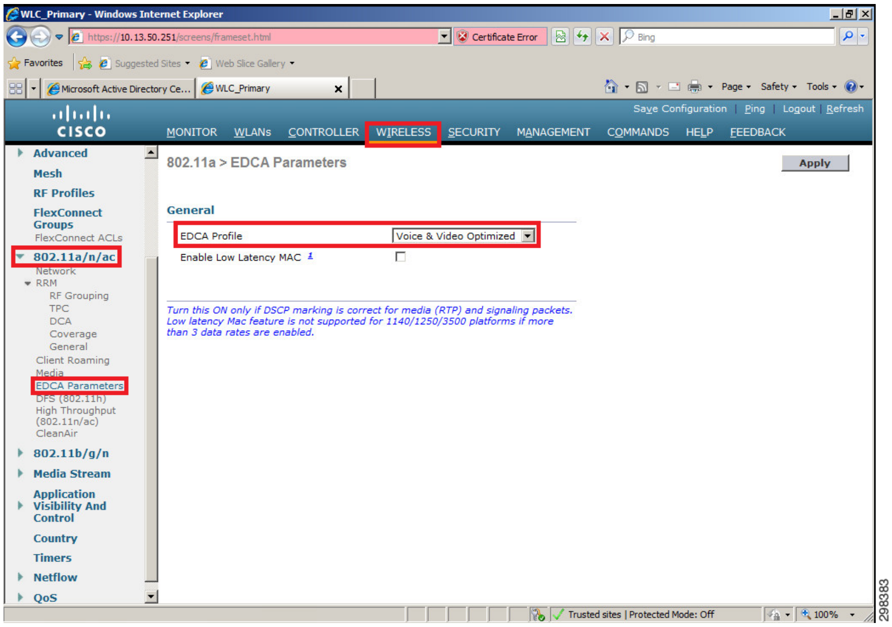
Foot Notes
1 Web Policy cannot be used in combination with IPsec

Note When changing WLAN QoS, it is required to disable the wireless radio network.

WLC QoS EDCA Setup

In a Unified WLAN environment, WLC Enhanced Distributed Channel Access (EDCA) configuration is not customer tunable, and it is a profile based mechanism. It is recommended to choose Voice/Video Optimized profile as shown in Figure 3-59.

Figure 3-59 EDCA QoS Profile Configuration



802.11a > EDCA Parameters

General

EDCA Profile: Voice & Video Optimized

Enable Low Latency MAC [1] ☐

Turn this ON only if DSCP marking is correct for media (RTP) and signaling packets. Low latency Mac feature is not supported for 1140/1250/3500 platforms if more than 3 data rates are enabled.

Note 802.11a/n/ac EDCA parameters are critical for wireless half-duplex channel with collision avoidance mechanism. Currently, Unified WLAN does not support customer tuning of EDCA parameters like Autonomous WLAN does. From comparing different Unified WLAN EDCA profiles, the Voice/Video Optimized profile is a close match to that of Autonomous WLAN.

WGB QoS in Unified WLAN

The WGB QoS includes traffic classifying and remarking, as well as 802.11a/n/ac EDCA parameters. The following is the WGB QoS configuration example.

```
!
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
 class _class_EXPLICIT
  set cos 0
!
interface Dot11Radio1
service-policy output ODVA
 packet retries 16 drop-packet
!
```

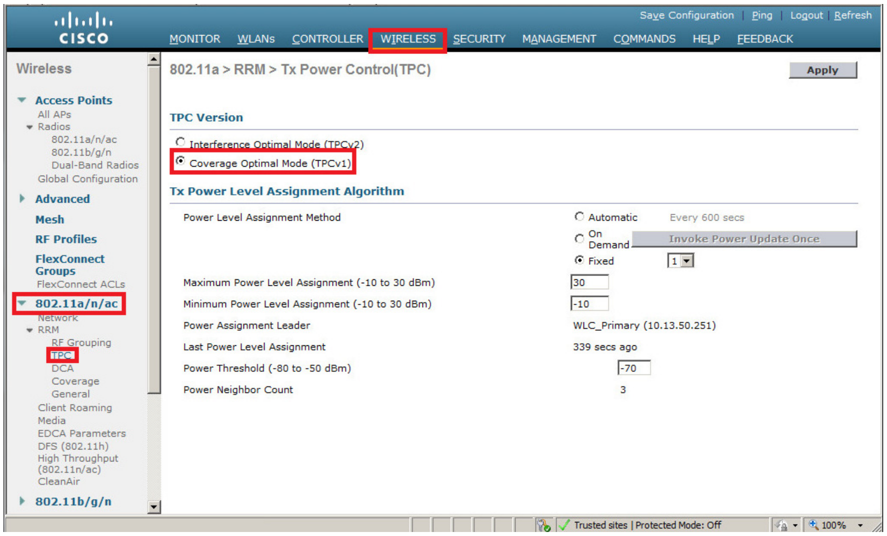
WLAN Radio Frequency

This section describes RF configuration for the Unified WLAN specific to the IACS applications. The following is recommended:

- Disable Radio Resource Management (RRM) functionality to prevent LWAPs from performing the off-channel scan. Leaving RRM enabled can create disruptions for the IACS traffic and cause application connection timeouts.
- As mentioned in Radio Frequency Design, page 2-13, disable 802.11n data rates for applications with real-time EtherNet/IP traffic (I/O, Produced/Consumed, CIP Safety).
- Manually assign channels and transmit power for the LWAPs.
- DFS channels in 5 GHz should be removed from the WLC channel list.

Step 1 Navigate to *Wireless > 802.11a/n/ac > TPC* to choose Coverage Optimal Mode (TPCv1) as shown in Figure 3-60.

Figure 3-60 WLC RRM Transmit Power Control Setup



802.11a > RRM > Tx Power Control(TPC)

TPC Version

○ Interference Optimal Mode (TPCv2)
● Coverage Optimal Mode (TPCv1)

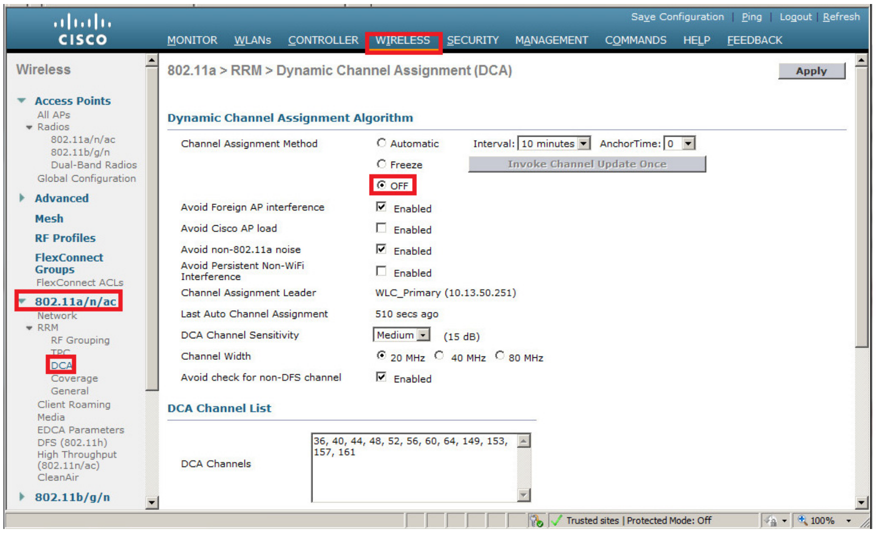
Tx Power Level Assignment Algorithm

Power Level Assignment Method: ○ Automatic Every 600 secs; ○ On Demand; ● Fixed 1

Maximum Power Level Assignment (-10 to 30 dBm): 30
Minimum Power Level Assignment (-10 to 30 dBm): -10
Power Assignment Leader: WLC_Primary (10.13.50.251)
Last Power Level Assignment: 339 secs ago
Power Threshold (-80 to -50 dBm): -70
Power Neighbor Count: 3

Step 2 In *Wireless > 802.11a/n/ac > DCA*, turn off dynamic channel assignment as shown in Figure 3-61.

Figure 3-61 WLC RRM Dynamic Channel Assignment Setup



802.11a > RRM > Dynamic Channel Assignment (DCA)

Dynamic Channel Assignment Algorithm

Channel Assignment Method: ○ Automatic   Interval: 10 minutes   AnchorTime: 0
○ Freeze
● OFF

Avoid Foreign AP interference: ☑ Enabled

Avoid Cisco AP load: □ Enabled

Avoid non-802.11a noise: ☑ Enabled

Avoid Persistent Non-WiFi Interference: □ Enabled

Channel Assignment Leader: WLC_Primary (10.13.50.251)

Last Auto Channel Assignment: 510 secs ago

DCA Channel Sensitivity: Medium (15 dB)

Channel Width: ● 20 MHz ○ 40 MHz ○ 80 MHz

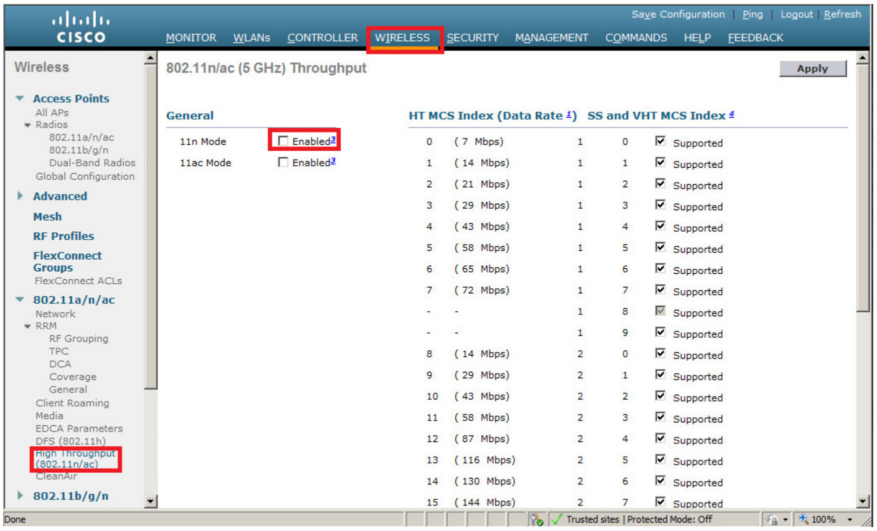
Avoid check for non-DFS channel: ☑ Enabled

DCA Channel List

DCA Channels: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161

Step 3 Navigate to *Wireless > 802.11a/n/ac > High Throughput* to disable 802.11n rate as shown in Figure 3-62.

Figure 3-62 WLC 802.11n Setup



802.11n/ac (5 GHz) Throughput

General

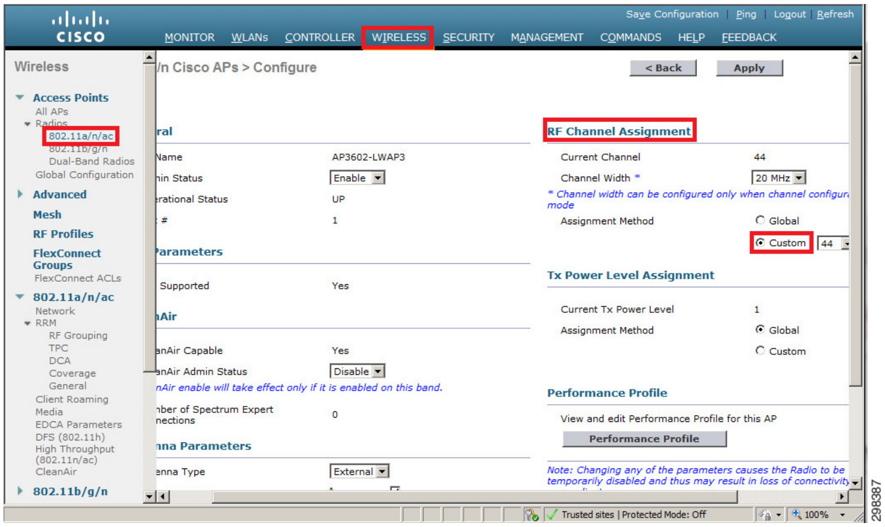
11n Mode: □ Enabled[3]

11ac Mode: □ Enabled[3]

HT MCS Index (Data Rate [1])		SS and VHT MCS Index [4]		
0	(7 Mbps)	1	0	☑ Supported
1	(14 Mbps)	1	1	☑ Supported
2	(21 Mbps)	1	2	☑ Supported
3	(29 Mbps)	1	3	☑ Supported
4	(43 Mbps)	1	4	☑ Supported
5	(58 Mbps)	1	5	☑ Supported
6	(65 Mbps)	1	6	☑ Supported
7	(72 Mbps)	1	7	☑ Supported
-	-	1	8	☑ Supported
-	-	1	9	☑ Supported
8	(14 Mbps)	2	0	☑ Supported
9	(29 Mbps)	2	1	☑ Supported
10	(43 Mbps)	2	2	☑ Supported
11	(58 Mbps)	2	3	☑ Supported
12	(87 Mbps)	2	4	☑ Supported
13	(116 Mbps)	2	5	☑ Supported
14	(130 Mbps)	2	6	☑ Supported
15	(144 Mbps)	2	7	☑ Supported

Step 4 Navigate to *Wireless > Radio > 802.11a/n/ac* and select *LWAP* in configuration mode to configure non-DFS channel manually as shown in Figure 3-63.

Figure 3-63 WLC Static Channel Assignment



/n Cisco APs > Configure

ral

Name	AP3602-LWAP3
in Status	Enable
rational Status	UP
#	1

arameters

Supported	Yes

Air

anAir Capable	Yes
anAir Admin Status	Disable

nAir enable will take effect only if it is enabled on this band.

ber of Spectrum Expert nections	0

nna Parameters

enna Type	External

RF Channel Assignment

Current Channel	44
Channel Width *	20 MHz

** Channel width can be configured only when channel configur mode*

Assignment Method ○ Global ● Custom 44

Tx Power Level Assignment

Current Tx Power Level	1
Assignment Method	● Global ○ Custom

Performance Profile

View and edit Performance Profile for this AP

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity

CHAPTER 4

Maintaining the Infrastructure

This chapter describes recommendations, best practices, and procedures for WLAN troubleshooting and maintenance.

After the WLAN has been deployed in the industrial environment, it has to be maintained to ensure the required level of availability and performance. The important activities when maintaining the WLAN infrastructure include:

- Monitoring the WLAN environment for changes in the RF spectrum and physical characteristics
- Assessing changes in the application, such as IACS parameters, performance requirements, area of operation, and number and type of wireless equipment, and adopting WLAN infrastructure and settings to the changes
- Verifying configured WLAN settings to make sure they match the recommended values
- Creating a baseline of the key WLAN metrics and monitoring these metrics during the operation
- Assessing changes in the application, such as IACS parameters, performance requirements, area of operation, and number and type of wireless equipment, and adopting WLAN infrastructure and settings to the changes
- Establishing procedures for quick replacement and provisioning of WLAN components to minimize downtime

Autonomous WLAN Maintenance and Troubleshooting

This section cover the maintenance and troubleshooting of the Autonomous WLAN using Stratix 5100 APs and WGBs.

RF Spectrum and Environment

After the WLAN has been deployed, it is important to monitor the environment for the RF interference and to assess any changes at the site that may affect wireless signal quality. Even a small amount of interference can severely disrupt or prevent control communication in a highly utilized wireless 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.

The following recommendations can be made for the Autonomous WLANs regarding to the RF spectrum and environment:

- In addition to the pre-deployment RF spectrum survey, perform periodic or continuous evaluation of the RF channels using spectrum analysis tools. The sources of interference can be non-802.11 devices (such as microwaves or radars), or other 802.11 wireless devices (unauthorized access points and wireless clients).
- Assess changes in the environment that may affect the wireless communication:
  - Newly installed industrial equipment with a potential to generate RF noise
  - Physical obstructions to the antennas (machines, moving parts, inventory stocks)
  - Damage to the antennas and connectors
  - Changes in layout and distance between the wireless clients and the APs
- Create a baseline and monitor for changes of the wireless and IACS metrics that may indicate RF issues:
  - RSSI and SNR values on the APs and WGBs
  - Retry and CRC error levels on the radio interfaces
  - Channel utilization, duty cycle and other data from the spectrum analysis tools
  - Increased latency, jitter and connection timeouts for the IACS application

Some of these parameters are discussed in the following sections.

- If necessary, conduct a new site survey and make changes to the WLAN infrastructure to mitigate the issues.

WLAN Diagnostics

This section describes some of the important metrics and diagnostic information available on the Stratix 5100 that can be used to monitor and troubleshoot a WLAN. The following methods exist to obtain the information from an AP or WGB:

- Web interface diagnostics (radio interface status and statistics, association data, log messages) in the Device Manager
- CLI diagnostic using "show" and "debug" command output
- SNMP (Simple Network Management Protocol) diagnostics using an SNMP management software
- System logging using a Syslog server software
- CIP diagnostic using Studio 5000 AOP (Add-On Profiles), controller tags and FactoryTalk View face plates

This guide focuses on the Device Manager and CLI information.

Radio Interface Information

Radio interface status and statistics provide the most useful information for monitoring and diagnostics of the Stratix 5100 operation. In order to correctly interpret the information, it is critical to determine a baseline for the normal WLAN operation in the production environment. During troubleshooting, the current data 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.

Radio Status and Configuration

Radio status and basic configured parameters can be verified on the *Network - Radio Status* page in the Device Manager (see Table 4-1). As the first step in the troubleshooting process, this data can be compared with the expected values for the device.

The same information can be obtained using the CLI commands.

Display radio software and hardware status:

```
show interface Dot11Radio 1
```

Display configured radio parameters:

```
show running-config interface Dot11Radio 1
```

Table 4-1 Radio Status and Configuration Parameters

Parameters	Action	Notes
Hardware Status (up / down / reset)	Verify radio hardware status.	*Reset* state may indicate that no SSID has been applied to the interface.
Software Status (enabled / disabled)	Verify radio software (administrative) status.	Radios are disabled in the factory default configuration.
Operational Rates Basic Rates	Verify that basic (required) and operational (allowed) data rates match the recommended values.	At least one basic rate on the AP and WGB should match for successful association. 802.11n MCS rates (m0...m23) should be disabled for the high performance IACS traffic.
Configured Radio Channel Active Radio Channel	Verify that configured and active channel on the AP matches the planned channel for the device.	Normally the channel is assigned statically to the AP. If using DFS channels in the 5 GHz band, changes in the active channel may indicate a DFS event due to radar interference.
Channel Width (20/40 MHz)	Verify that 20 MHz channel width is configured.	40 MHz channel width is not recommended for IACS applications.
Transmitter Power (dBm)	Verify that power levels on the AP and WGB are configured according to the site survey results.	For most deployments, the sum of Tx power and antenna gain should match between an AP and a WGB. It is not always necessary to select the maximum allowed power in the channel.
Role in Network (Access Point / WGB)	Verify the device role.	The default role is *Access Point*.

Radio Statistics

Radio packet rate and statistics can be viewed on the *Network - Radio Status* and *Detailed Status* pages in the Device Manager (see Figure 4-1 through Figure 4-3). The most important parameters are listed in Table 4-2.

Note The diagnostic pages provide the *Last 5 Seconds* radio statistics which may vary significantly between each measurements. For more accurate diagnostics, clear the statistics and use the cumulative numbers for at least 5 minutes.

The CLI commands are listed below:

Display input and output packet rate (5 minute average):

```
show interface Dot11Radio 1
```

Display radio statistics (cumulative total and last 5 seconds):

```
    show interface Dot11Radio 1 statistics
```

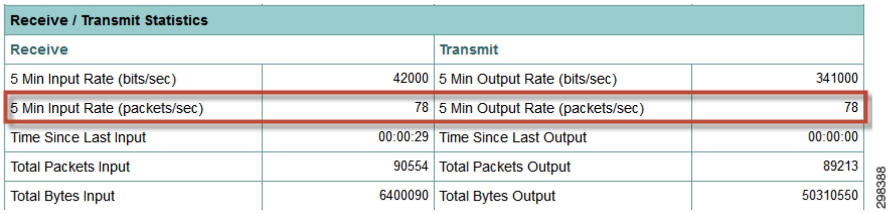
Clear interface counters:

```
    clear counters Dot11Radio 1
    clear dot11 statistics Dot11Radio 1
```

Table 4-2 Radio Statistics

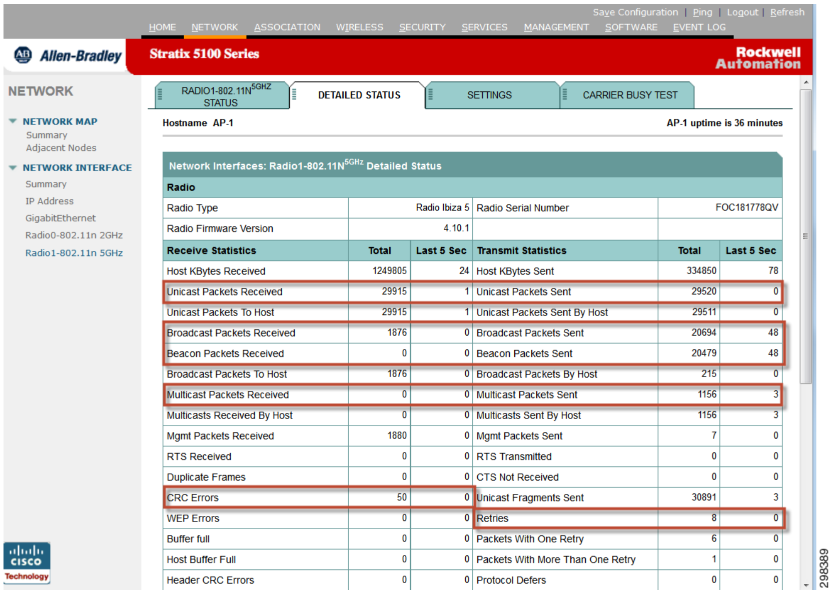
Parameters	Action	Notes
5 Min Input Rate (packets/sec) **5 Min Output Rate (packets/sec)**	Compare to the baseline values for the APs and WGBs. Make sure that the total packet rate for all APs in the channel does not exceed the recommended limit (see Packet Rate Considerations, page 2-7).	Increased packet rate may indicate excessive maintenance traffic (HMI tags, Studio 5000 online traffic, IT management traffic) or change in the IACS application (RPI, number of connections).
Unicast Packets Sent **Multicast Packets Sent**	Compare values to the baseline. Check for unexpected multicast traffic.	EtherNet/IP I/O and Produced/Consumed data should use unicast connections.
Broadcast Packets Sent **Beacons Packets Sent**	Compare values to the baseline.	Most broadcast traffic sent by the AP should be beacons. The default beacon rate is 100 ms.
Retries **Packets with One Retry** **Packets with >1 Retry**	Compare values to the baseline for each device. Clear statistics, capture results for 5 minutes, and calculate % of retries to unicast packets sent	Normally the retry level should be less than 2% (AP) and 5% (WGB) of the transmitted packets. High retry levels indicate excessive packet rate in the channel or RF issues.
Unicast Packets Received **Multicast Packets Received**	Compare values to the baseline. Check for unexpected multicast traffic.	EtherNet/IP I/O and Produced/Consumed data should use unicast connections.
Broadcast Packets Received **Beacon Packets Received**	Compare values to the baseline.	Most broadcast traffic received by the WGB should be beacons. Unexpected beacon rate may indicate the presence of unauthorized APs in the channel. Excessive broadcast rate may indicate network or application issues.
CRC Errors	Compare values to the baseline for each device.	Changes in the CRC error level may indicate excessive packet rate in the channel or RF issues.
Statistics per Data Rate: **Rx Packets** **Tx packets**	Verify data rates at which the packets are being transmitted.	Most data packets should be transmitted at the highest active data rate (typically 54 Mbps for the EtherNet/IP data). Beacons are transmitted at the lowest basic rate (typically 6 Mbps). Large packet counts for the other rates indicate excessive retransmissions in the channel due to overutilization or RF issues.

Figure 4-1 Radio Packet Rate



Receive / Transmit Statistics			
Receive		Transmit	
5 Min Input Rate (bits/sec)	42000	5 Min Output Rate (bits/sec)	341000
5 Min Input Rate (packets/sec)	78	5 Min Output Rate (packets/sec)	78
Time Since Last Input	00:00:29	Time Since Last Output	00:00:00
Total Packets Input	90554	Total Packets Output	89213
Total Bytes Input	6400090	Total Bytes Output	50310550

Figure 4-2 Radio Detailed Status



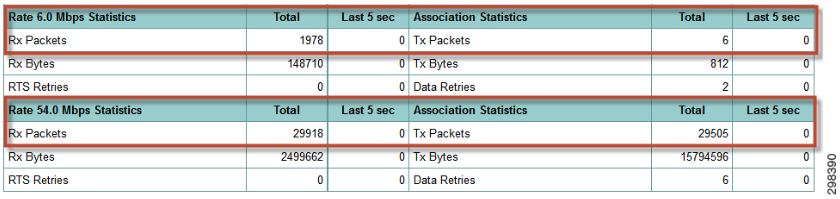
Hostname AP-1 AP-1 uptime is 36 minutes

Network Interfaces: Radio1-802.11N^{5GHz} Detailed Status

Radio			
Radio Type	Radio Ibiza 5	Radio Serial Number	FOC181778QV
Radio Firmware Version	4.10.1		

Receive Statistics	Total	Last 5 Sec	Transmit Statistics	Total	Last 5 Sec
Host KBytes Received	1249805	24	Host KBytes Sent	334850	78
Unicast Packets Received	29915	1	Unicast Packets Sent	29520	0
Unicast Packets To Host	29915	1	Unicast Packets Sent By Host	29511	0
Broadcast Packets Received	1876	0	Broadcast Packets Sent	20694	48
Beacon Packets Received	0	0	Beacon Packets Sent	20479	48
Broadcast Packets To Host	1876	0	Broadcast Packets By Host	215	0
Multicast Packets Received	0	0	Multicast Packets Sent	1156	3
Multicasts Received By Host	0	0	Multicasts Sent By Host	1156	3
Mgmt Packets Received	1880	0	Mgmt Packets Sent	7	0
RTS Received	0	0	RTS Transmitted	0	0
Duplicate Frames	0	0	CTS Not Received	0	0
CRC Errors	50	0	Unicast Fragments Sent	30891	3
WEP Errors	0	0	Retries	8	0
Buffer full	0	0	Packets With One Retry	6	0
Host Buffer Full	0	0	Packets With More Than One Retry	1	0
Header CRC Errors	0	0	Protocol Defers	0	0

Figure 4-3 Radio Rate Statistics



Rate 6.0 Mbps Statistics	Total	Last 5 sec	Association Statistics	Total	Last 5 sec
Rx Packets	1978	0	Tx Packets	6	0
Rx Bytes	148710	0	Tx Bytes	812	0
RTS Retries	0	0	Data Retries	2	0
Rate 54.0 Mbps Statistics	**Total**	**Last 5 sec**	**Association Statistics**	**Total**	**Last 5 sec**
Rx Packets	29918	0	Tx Packets	29505	0
Rx Bytes	2499662	0	Tx Bytes	15794596	0
RTS Retries	0	0	Data Retries	6	0

Association Data and Client Statistics

The *Association* page of the Device Manager for the AP provides information about the client devices, including WGBs and wired clients (see Figure 4-4). Client statistics can be useful in troubleshooting of the issues related to the specific client. The *Association* page for the WGB provides information about the parent AP, such as the signal strength.

Table 4-3 lists the most important association parameters. The corresponding CLI commands are shown below.

Display the list of associated devices and basic information:

```
show dot11 associations
```

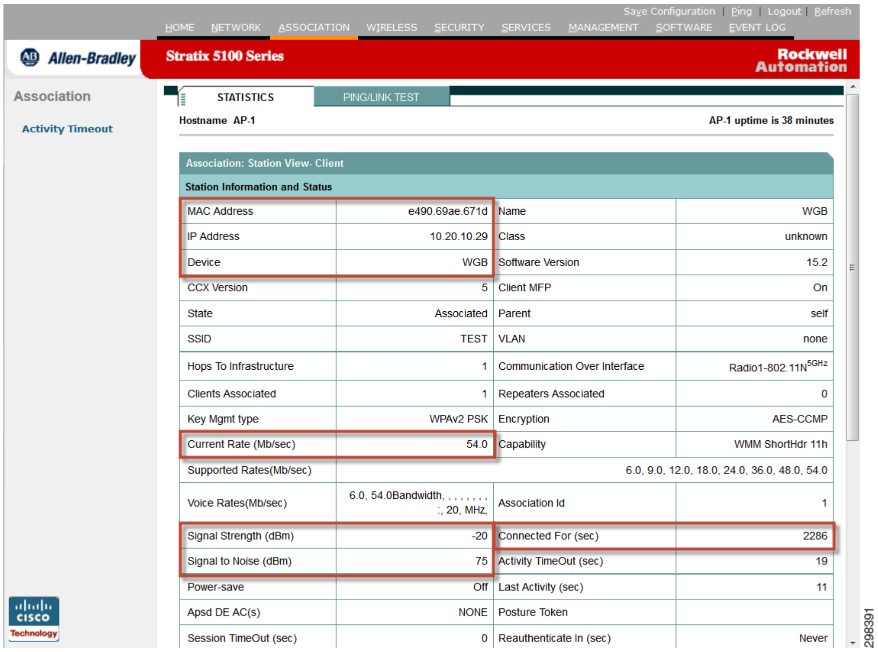
Display the detailed information about all devices or a single device:

```
show dot11 associations all
show dot11 associations <MAC address>
```

Table 4-3 Radio Association Parameters

Parameters	Action	Notes
IP Address **MAC Address** **Device Type**	Verify that all expected wireless clients are associated to the AP. Verify that the wired client information is communicated by the WGB to the AP (device type *WGB-client*).	
Current Rate (Mbps)	Verify the data rate for the client.	Should be highest enabled rate in normal RF conditions.
Signal Strength (dBm) **Signal to Noise (dB)**	Compare to the baseline or expected level for the client.	Recommended values for the IACS applications: Signal strength (RSSI) ≥ -67 dBm Signal to Noise (SNR) ≥ 25 dB
Connected For (sec)	Check for recent disassociation events.	
Input and Output Rate **Data Retries**	Compare to the baseline and to the values for other wireless clients (WGBs).	

Figure 4-4 Association—Client Details


Save Configuration | Ping | Logout | Refresh
HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG
Allen-Bradley
Stratix 5100 Series
Rockwell Automation
Association
Activity Timeout
STATISTICS
PING/LINK TEST
cisco Technology
298391

Hostname AP-1 AP-1 uptime is 38 minutes

Association: Station View- Client

Station Information and Status

MAC Address	e490.69ae.671d	Name	WGB
IP Address	10.20.10.29	Class	unknown
Device	WGB	Software Version	15.2
CCX Version	5	Client MFP	On
State	Associated	Parent	self
SSID	TEST	VLAN	none
Hops To Infrastructure	1	Communication Over Interface	Radio1-802.11N$^{\text{5GHz}}$
Clients Associated	1	Repeaters Associated	0
Key Mgmt type	WPAv2 PSK	Encryption	AES-CCMP
Current Rate (Mb/sec)	54.0	Capability	WMM ShortHdr 11h
Supported Rates(Mb/sec)	6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0		
Voice Rates(Mb/sec)	6.0, 54.0Bandwidth, , , , , , , , :, 20, MHz,	Association Id	1
Signal Strength (dBm)	-20	Connected For (sec)	2286
Signal to Noise (dBm)	75	Activity TimeOut (sec)	19
Power-save	Off	Last Activity (sec)	11
Apsd DE AC(s)	NONE	Posture Token	
Session TimeOut (sec)	0	Reauthenticate In (sec)	Never

System Logging and Debugging

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

- View log messages since the last reboot on the *Event Log page* in the Device Manager. Increase log buffer size in the *Configuration Options* if necessary to avoid overwriting of messages. The CLI command is:

  ```
  show logging
  ```

- Note any log messages with the level 4 (Warnings) and above. The explanation for some of the messages can be found in the Stratix 5100 User Manual.

Note Rebooting the Stratix 5100 will clear the log buffer. Save the information for the technical support before rebooting the AP.

- Configure logging to a Syslog server to permanently store the messages and to consolidate information from all devices in the WLAN.
- Configure Simple Network Time Protocol (SNTP) for AP / WGBs to keep the common clock between devices for logging.
- Configure debugging via CLI only if directed by the technical support.

Note Debugging mode can severely impact the performance and disrupt the data traffic. In some cases, rebooting the AP is required. Debugging should only be used during troubleshooting and should not be enabled during the normal operation.

- Detailed information for the technical support can be obtained on the *Software - System Configuration* page of the Device Manager (*Show tech-support*). It is recommended to create a baseline copy of this information for each device.

Autonomous AP and WGB Replacement

This section describes procedures for provisioning and replacement of the autonomous AP and WGBs that minimize downtime in case of the hardware failure.

When replacing a failed AP, the following is recommended:

- For fastest recovery time in case of the AP failure, use the backup AP that is preconfigured and installed in the same coverage area (see Redundant AP Coverage, page 2-24). The WGBs should roam to the backup AP within 30 seconds
- If installing a backup AP is not possible or practical, use the saved configuration of the AP to provision the new device. The steps are described below.
- It is recommended to preconfigure and keep a spare AP to minimize downtime.
- If replacing the failed AP with a new AP with default configuration, use a DHCP server in the network to assign an IP address for faster provisioning.

When replacing a failed WGB, the following is recommended:

- Use the WGB configuration template file to provision the new WGB.
- It is recommended to preconfigure and keep a spare WGB to minimize downtime.
- If replacing the failed WGB with a new WGB with default configuration, use the Rockwell Automation BOOTP Utility or the console connection to assign an IP address.

Autonomous AP Replacement

These steps describe how to back up the configuration and provision a new Stratix 5100 in the AP role.

Step 1 During the normal operation, use *Software - System Configuration* page in the Device Manager to save the copy of the AP configuration file *config.txt*. The file can also be copied using the CLI and the TFTP server software on the PC:

```
copy flash:config.txt tftp://<IP ADDRESS>/config.txt
```

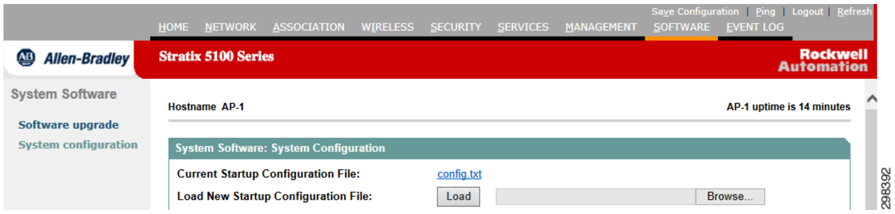
Step 2 Assign a management IP address for the replacement or spare AP using the DHCP server in the network, BOOTP utility, or the console connection. DHCP Persistence feature of the Stratix 5700 / Stratix 8000 switch can assign a persistent IP address when connecting to the specified switchport.

Note When configuring a spare AP, use the temporary IP address that is different from the active AP.

Step 3 Upload the configuration using the *Software - System Configuration* page in the Device Manager. The device will be restarted and the new configuration will take place. The configuration can also be uploaded using the CLI and the TFTP server software on the PC:

```
copy tftp://<IP ADDRESS>/<FILENAME> flash:config.txt
```

Figure 4-5 Software—System Configuration


Save Configuration | Ping | Logout | Refresh
HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG
Allen-Bradley
Stratix 5100 Series
Rockwell Automation
System Software
Software upgrade
System configuration
Load
Browse...
298392

Hostname AP-1 AP-1 uptime is 14 minutes

System Software: System Configuration

Current Startup Configuration File: config.txt

Load New Startup Configuration File:

WGB Replacement

These steps describe how to back up the configuration and provision a spare Stratix 5100 in the WGB role.

Step 1 During the normal operation, use the *Software - System Configuration* page in the Device Manager to save the copies of configuration files for every WGB.

Step 2 If configuring a spare WGB, use one of the configurations as a template and modify the device name and the management IP:

```
hostname <NAME>
interface BVI1
 ip address <IP> <MASK>
```

Use the name and IP address that have not been assigned to any of the operating WGBs. These can be modified after the installation if necessary.

Step 3 If using the EAP-FAST authentication with individual credentials for each WGB, modify the username and password in the profile:

```
dot1x credentials <PROFILE NAME>
 username <USERNAME>
 password <PASSWORD>
```

These credentials should be preconfigured on the RADIUS server.

Step 4 During the provisioning, assign the IP address for the replacement or spare WGB using the Rockwell Automation BOOTP utility or the console connection.

Note When configuring a spare WGB, use the IP address that is different from any of the active WGB.

Step 5 Upload the configuration using the *Software - System Configuration* page in the Device Manager. The device will be restarted and the new configuration will take place.

Step 6 Verify that the new WGB can join the WLAN and that the radio parameters are according to the baseline.

Unified WLAN Maintenance and Troubleshooting

This section covers maintenance and troubleshooting of the Unified WLAN using WLCs, LWAPs and WGBs.

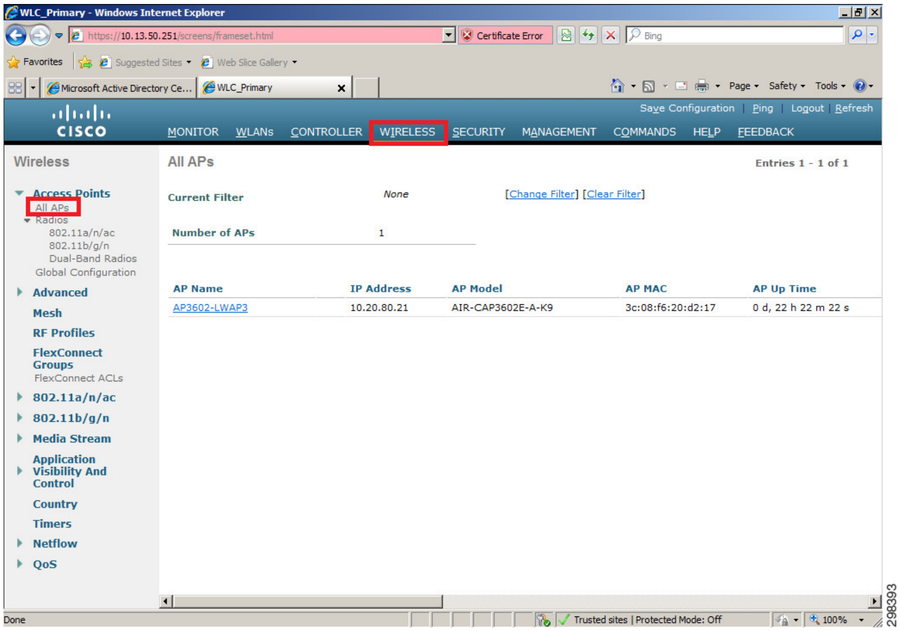
Unified WLAN Diagnostics

Association Data and Client Statistics

Please refer to Autonomous WLAN Maintenance and Troubleshooting, page 4-1 for details. In addition, the WLC provides valuable troubleshooting information, both using the web GUI and CLI.

Figure 4-6 and Figure 4-7 show the GUI-based summary outputs for LWAPs and WGBs / clients.

Figure 4-6 AP Summary View



All APs

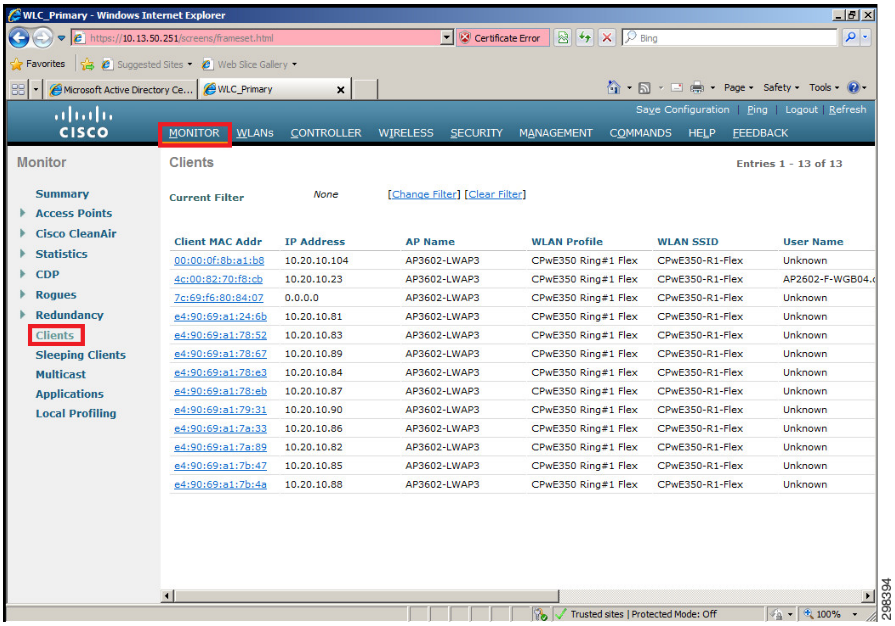
Entries 1 - 1 of 1

Current Filter: None [Change Filter] [Clear Filter]

Number of APs: 1

AP Name	IP Address	AP Model	AP MAC	AP Up Time
AP3602-LWAP3	10.20.80.21	AIR-CAP3602E-A-K9	3c:08:f6:20:d2:17	0 d, 22 h 22 m 22 s

Figure 4-7 Client Summary View



Clients

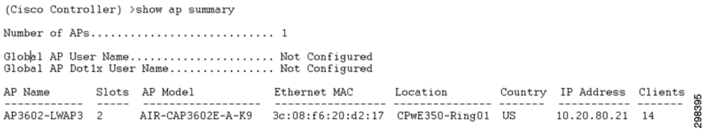
Entries 1 - 13 of 13

Current Filter: None [Change Filter] [Clear Filter]

Client MAC Addr	IP Address	AP Name	WLAN Profile	WLAN SSID	User Name
00:00:0f:8b:a1:b8	10.20.10.104	AP3602-LWAP3	CPwE350 Ring#1 Flex	CPwE350-R1-Flex	Unknown
4c:00:82:70:f8:cb	10.20.10.23	AP3602-LWAP3	CPwE350 Ring#1 Flex	CPwE350-R1-Flex	AP2602-F-WGB04.
7c:69:f6:80:84:07	0.0.0.0	AP3602-LWAP3	CPwE350 Ring#1 Flex	CPwE350-R1-Flex	Unknown
e4:90:69:a1:24:6b	10.20.10.81	AP3602-LWAP3	CPwE350 Ring#1 Flex	CPwE350-R1-Flex	Unknown
e4:90:69:a1:78:52	10.20.10.83	AP3602-LWAP3	CPwE350 Ring#1 Flex	CPwE350-R1-Flex	Unknown
e4:90:69:a1:78:67	10.20.10.89	AP3602-LWAP3	CPwE350 Ring#1 Flex	CPwE350-R1-Flex	Unknown
e4:90:69:a1:78:e3	10.20.10.84	AP3602-LWAP3	CPwE350 Ring#1 Flex	CPwE350-R1-Flex	Unknown
e4:90:69:a1:78:eb	10.20.10.87	AP3602-LWAP3	CPwE350 Ring#1 Flex	CPwE350-R1-Flex	Unknown
e4:90:69:a1:79:31	10.20.10.90	AP3602-LWAP3	CPwE350 Ring#1 Flex	CPwE350-R1-Flex	Unknown
e4:90:69:a1:7a:33	10.20.10.86	AP3602-LWAP3	CPwE350 Ring#1 Flex	CPwE350-R1-Flex	Unknown
e4:90:69:a1:7a:89	10.20.10.82	AP3602-LWAP3	CPwE350 Ring#1 Flex	CPwE350-R1-Flex	Unknown
e4:90:69:a1:7b:47	10.20.10.85	AP3602-LWAP3	CPwE350 Ring#1 Flex	CPwE350-R1-Flex	Unknown
e4:90:69:a1:7b:4a	10.20.10.88	AP3602-LWAP3	CPwE350 Ring#1 Flex	CPwE350-R1-Flex	Unknown

On the WLC CLI, you can enter the "show ap summary" command to verify that the APs registered with the WLC, as shown in Figure 4-8.

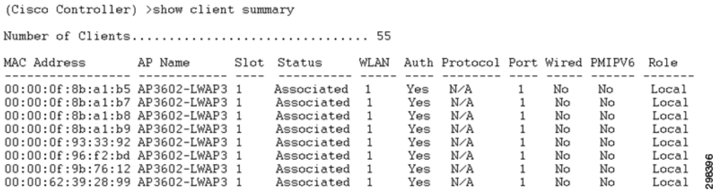
Figure 4-8 WLC AP Summary



```
(Cisco Controller) >show ap summary

Number of APs.......................... 1

Global AP User Name..................... Not Configured
Global AP Dot1x User Name............... Not Configured

AP Name       Slots  AP Model           Ethernet MAC       Location        Country  IP Address   Clients
------------  -----  -----------------  -----------------  --------------  -------  -----------  -------
AP3602-LWAP3  2      AIR-CAP3602E-A-K9  3c:08:f6:20:d2:17  CPwE350-Ring01  US       10.20.80.21  14
```

If you have Wireless LANs configured, you can enter the "show client summary" command in order to see the clients that are registered with the WLC, as shown in Figure 4-9.

Figure 4-9 WLC Client Summary



```
(Cisco Controller) >show client summary

Number of Clients................................ 55

MAC Address        AP Name       Slot  Status     WLAN  Auth Protocol Port Wired PMIPV6  Role
----------------- ------------ ----  ---------- ----- ---- -------- ---- ----- ------ -------
00:00:0f:8b:a1:b5 AP3602-LWAP3 1     Associated  1     Yes  N/A       1    No    No     Local
00:00:0f:8b:a1:b7 AP3602-LWAP3 1     Associated  1     Yes  N/A       1    No    No     Local
00:00:0f:8b:a1:b8 AP3602-LWAP3 1     Associated  1     Yes  N/A       1    No    No     Local
00:00:0f:8b:a1:b9 AP3602-LWAP3 1     Associated  1     Yes  N/A       1    No    No     Local
00:00:0f:93:33:92 AP3602-LWAP3 1     Associated  1     Yes  N/A       1    No    No     Local
00:00:0f:96:f2:bd AP3602-LWAP3 1     Associated  1     Yes  N/A       1    No    No     Local
00:00:0f:9b:76:12 AP3602-LWAP3 1     Associated  1     Yes  N/A       1    No    No     Local
00:00:62:39:28:99 AP3602-LWAP3 1     Associated  1     Yes  N/A       1    No    No     Local
```

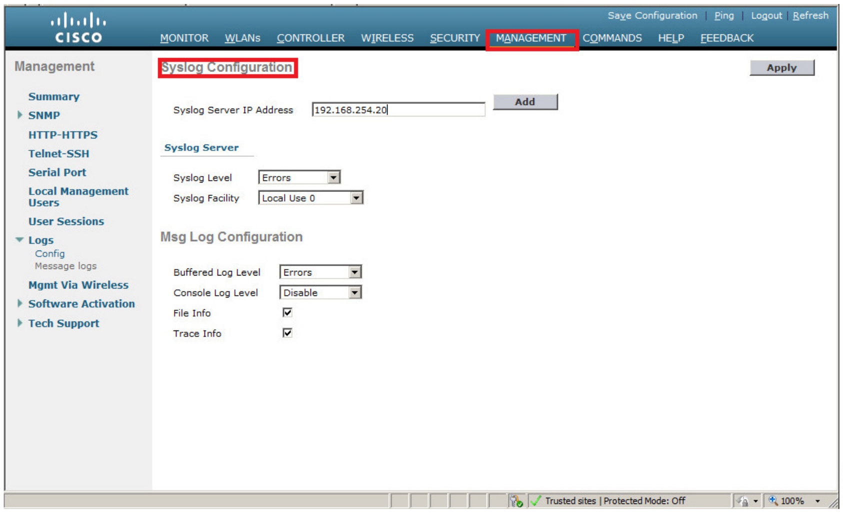
System Logging and Debugging

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

- Configure logging to a syslog server to permanently store the messages and to consolidate information from all devices in the WLAN as shown in Figure 4-10.
- Current message logs can be obtained from WLC message log section as shown in Figure 4-11.
- Configure "debug client mac-address" on the WLC CLI to view details for the associated clients.

Note Debugging mode can severely impact the performance and disrupt the data traffic. In some cases, rebooting the network devices is required. Debugging should only be used during troubleshooting and should not be enabled during the normal operation.

Figure 4-10 WLC Syslog Setup



Syslog Configuration

Syslog Server IP Address 192.168.254.20

Syslog Server

Syslog Level Errors

Syslog Facility Local Use 0

Msg Log Configuration

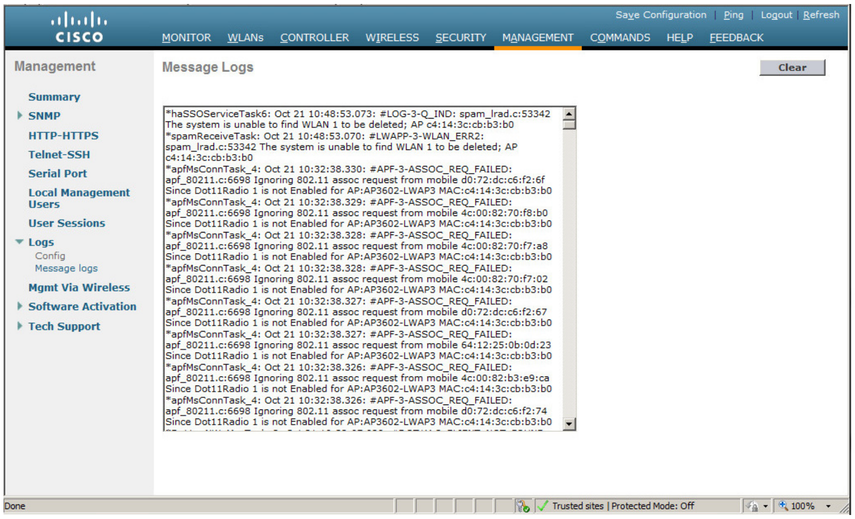
Buffered Log Level Errors

Console Log Level Disable

File Info ☑

Trace Info ☑

Figure 4-11 Message Log View



Message Logs

```
*haSSOServiceTask6: Oct 21 10:48:53.073: #LOG-3-Q_IND: spam_lrad.c:53342
The system is unable to find WLAN 1 to be deleted; AP c4:14:3c:cb:b3:b0
*spamReceiveTask: Oct 21 10:48:53.070: #LWAPP-3-WLAN_ERR2:
spam_lrad.c:53342 The system is unable to find WLAN 1 to be deleted; AP
c4:14:3c:cb:b3:b0
*apfMsConnTask_4: Oct 21 10:32:38.330: #APF-3-ASSOC_REQ_FAILED:
apf_80211.c:6698 Ignoring 802.11 assoc request from mobile d0:72:dc:c6:f2:6f
Since Dot11Radio 1 is not Enabled for AP:AP3602-LWAP3 MAC:c4:14:3c:cb:b3:b0
*apfMsConnTask_4: Oct 21 10:32:38.329: #APF-3-ASSOC_REQ_FAILED:
apf_80211.c:6698 Ignoring 802.11 assoc request from mobile 4c:00:82:70:f8:b0
Since Dot11Radio 1 is not Enabled for AP:AP3602-LWAP3 MAC:c4:14:3c:cb:b3:b0
*apfMsConnTask_4: Oct 21 10:32:38.328: #APF-3-ASSOC_REQ_FAILED:
apf_80211.c:6698 Ignoring 802.11 assoc request from mobile 4c:00:82:70:f7:a8
Since Dot11Radio 1 is not Enabled for AP:AP3602-LWAP3 MAC:c4:14:3c:cb:b3:b0
*apfMsConnTask_4: Oct 21 10:32:38.328: #APF-3-ASSOC_REQ_FAILED:
apf_80211.c:6698 Ignoring 802.11 assoc request from mobile 4c:00:82:70:f7:02
Since Dot11Radio 1 is not Enabled for AP:AP3602-LWAP3 MAC:c4:14:3c:cb:b3:b0
*apfMsConnTask_4: Oct 21 10:32:38.327: #APF-3-ASSOC_REQ_FAILED:
apf_80211.c:6698 Ignoring 802.11 assoc request from mobile d0:72:dc:c6:f2:67
Since Dot11Radio 1 is not Enabled for AP:AP3602-LWAP3 MAC:c4:14:3c:cb:b3:b0
*apfMsConnTask_4: Oct 21 10:32:38.327: #APF-3-ASSOC_REQ_FAILED:
apf_80211.c:6698 Ignoring 802.11 assoc request from mobile 64:12:25:0b:0d:23
Since Dot11Radio 1 is not Enabled for AP:AP3602-LWAP3 MAC:c4:14:3c:cb:b3:b0
*apfMsConnTask_4: Oct 21 10:32:38.326: #APF-3-ASSOC_REQ_FAILED:
apf_80211.c:6698 Ignoring 802.11 assoc request from mobile 4c:00:82:b3:e9:ca
Since Dot11Radio 1 is not Enabled for AP:AP3602-LWAP3 MAC:c4:14:3c:cb:b3:b0
*apfMsConnTask_4: Oct 21 10:32:38.326: #APF-3-ASSOC_REQ_FAILED:
apf_80211.c:6698 Ignoring 802.11 assoc request from mobile d0:72:dc:c6:f2:74
Since Dot11Radio 1 is not Enabled for AP:AP3602-LWAP3 MAC:c4:14:3c:cb:b3:b0
```

Unified AP Replacement

Unified WLAN provides "zero-touch" replacement of LWAPs. No specific configuration is required as the LWAP downloads the configuration and the updated firmware from the WLC.

Unified WLC Replacement

In the recommended WLC Stateful Switchover (SSO) environment, at any given time two WLCs exist: active and standby. In the case that the active WLC fails, the standby will become active. A new WLC can then be installed and brought into an SSO state with the current active one.

Note Please refer to the following link for further documentation on WLC redundancy: http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/7-5/High_Availability_DG.html

CHAPTER 5

Testing the Architecture

This chapter describes the validation and performance testing of the CPwE WLAN architectures that has been designed and configured as recommended in the previous chapters.

Autonomous WLAN Testing

The objective of the Autonomous WLAN testing was to validate the recommended architectures and configurations and characterize performance for typical IACS applications using wireless equipment in a Cell/Area Zone. Testing focused around the following performance characteristics:

- Long-term application reliability: operation without connection timeouts
- Real-time network performance: latency and packet loss
- CIP Safety performance: System Reaction Time

In addition to the performance testing, the following architecture areas described in Chapter 2, "System Design Considerations," and Chapter 3, "Configuring the Infrastructure," have been verified:

- WLAN security (WPA2-PSK, 802.1X with EAP)
- AP redundancy and failover
- Wireless QoS parameters and operation
- AP and WGB replacement procedures

Autonomous WLAN Test Setup

The test was conducted in the "best case" RF environment:

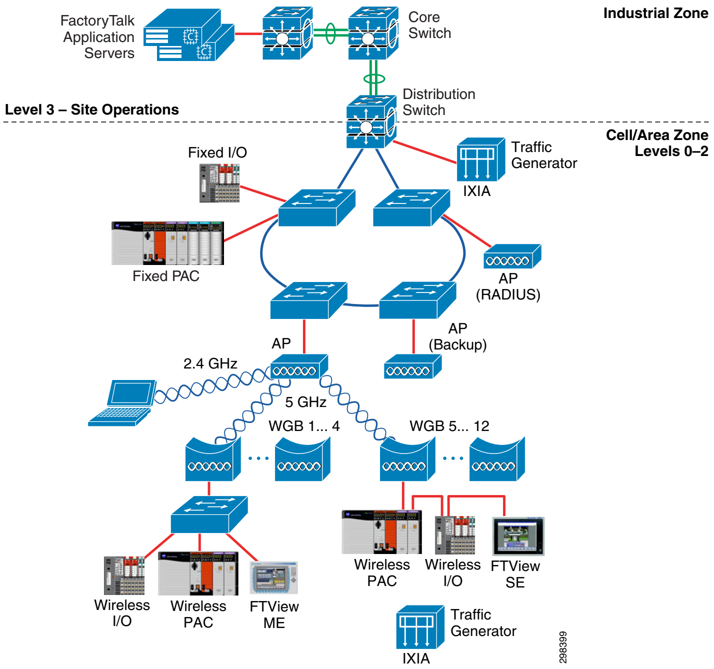
- No outside interference or significant signal obstruction
- A vacant wireless channel in the 5 GHz band
- Wireless clients (WGBs) in fixed positions
- An adequate signal level to support the highest enabled data rates

Because of the above conditions, test results represent the best achievable application performance given the channel load and the system size. Factors such as RF interference, signal propagation and antenna characteristics were not considered in the testing.

Autonomous WLAN Test Topology

Figure 5-1 shows the lab topology that was used during the testing. Network and IACS hardware and software versions are listed in Table E-1 on page E-1.

Figure 5-1 Autonomous WLAN Test Topology



Autonomous WLAN Network Configuration

The wired network infrastructure and WLAN setup was as follows:

- Resilient switch ring topology with REP
- Redundant stackable distribution switches
- The primary AP connecting to up to 12 WGBs on the 5GHz radio channel
- The backup AP for failover testing
- The RADIUS AP to test 802.1X authentication and EAP-FAST
- Ixia Test Chassis for traffic simulation, latency and packet loss measurements

Autonomous WLAN IACS Configuration

The IACS equipment and software consisted of the following:

- Fixed Safety PAC and I/O connected to the wired infrastructure
- FactoryTalk View server infrastructure

- Wireless Safety PAC and I/O (up to 12) connected to WGBs using a switch or a linear topology
- FactoryTalk View ME stations (4 nodes)
- FactoryTalk View SE clients (4 nodes)

Depending on the test case, the fixed PAC was communicating to the wireless I/O or PAC using standard and safety CIP traffic. These topologies were described in IACS Topologies in Autonomous WLANs, page 2-15.

Autonomous WLAN Test Cases and Parameters

The Autonomous WLAN test cases for the performance testing were created by selecting the following parameters:

- Number of WGBs in the topology:
  - Large (12 WGBs)
  - Small (4 WGBs)
- Type of CIP Class 1 traffic over wireless
  - Standard and Safety I/O
  - Standard and Safety Produced/Consumed

The standard and safety RPIs for each test case were selected to achieve the packet rate that allowed reliable communication without connection timeouts.

The FactoryTalk View traffic and simulated CIP Class 3 traffic was configured to be at about 20% of the total rate for all test cases.

The main test case parameters are listed in Table 5-1.

Table 5-1 Autonomous WLAN Test Case Parameters

Test Case Topology	# of Standard / Safety Connections	Packet Rate (I/O or P/C)	Packet Rate (Total)	Standard I/O or P/C RPI	Safety I/O RPI (Input/Output) or Safety P/C RPI
PAC to I/O, 4 WGBs	16 / 32	2,150 pps	2,590 pps	20 ms	18 ms / 40 ms
PAC to I/O, 12 WGBs	24 / 48	2,060 pps	2,440 pps	30 ms	30 ms / 60 ms
PAC to PAC, 4 WGBs	16 / 8	2,020 pps	2,490 pps	12 ms	15 ms
PAC to PAC, 12 WGBs	24 / 24	1,930 pps	2,250 pps	20 ms	40 ms

Autonomous WLAN Test Measurements

Table 5-2 lists the metrics that have been measured during the performance testing and pass criteria for each parameter..

Table 5-2 Autonomous WLAN Test Metrics

Test Metric	Pass Criteria
Safety System Reaction Time (SRT)	Maximum value < calculated Worst Case Single-fault SRT 99.99% samples < calculated Worst Case No-fault SRT
I/O or Produced/Consumed connection faults	No connection faults (standard or safety)
Network Latency	95% samples < ½ x RPI (standard I/O or Produced/Consumed)
% of lost packets, maximum number lost in a row	≤2 lost in a row

The following details how the measurements were performed:

- System Reaction Time was measured as the screw-to-screw time from a safety input module to a safety output module.
- For the PAC to I/O topology, the screw-to-screw time was measured between:
  - Fixed Input module to Wireless Output module
  - Wireless Input module to Fixed Output module
  - Wireless Input module to Wireless Output module
- For the PAC to PAC topology, the screw-to-screw time was measured between the I/O modules connected to the PACs:
  - Fixed PAC (Input module) to Wireless PAC (Output module)
  - Wireless PAC (Input module) to Fixed PAC (Output module)
- The observed SRT results were compared to the Worst Case values (Single Fault and No Fault) using the Rockwell Automation Safety Estimator tool.
- The tests have been run continuously for the period of 1 to 2 weeks to monitor for connection losses and to capture maximum values.
- Network latency and packet loss for the CIP Class 1 traffic were measured using the Ixia test chassis.

Note Latency and packet loss for the HMI traffic have not been characterized during the testing.

- To compare results with the wired network performance, the baseline tests were completed using wired connections to a switch.

Autonomous WLAN Test Results

This section describes the performance test results for the Autonomous WLAN and some of the observations.

Autonomous WLAN Safety System Reaction Time

Table 5-3 lists the results for the Safety System Reaction Time (SRT) which was measured as the screw-to-screw time between the safety input and the safety output module. The important observations for this parameter are:

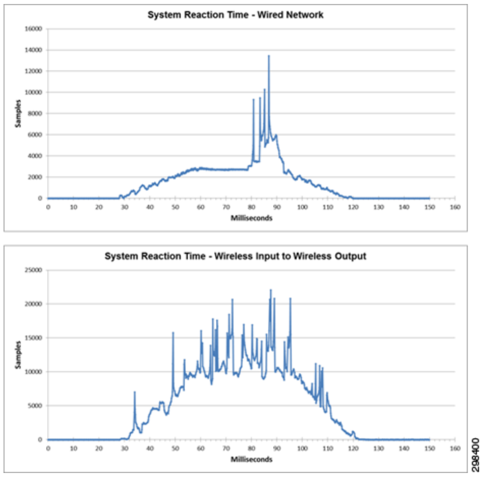
- 99.99% observed SRT were below "Worst Case No Fault" calculated SRT.
- Maximum observed SRT were below "Worst Case Single Fault" calculated SRT.

- Results for the safety reaction times were the same for wired and wireless systems except for a very small percentage of samples (<0.01%). Examples of the SRT distribution for wired vs. wireless are shown in Figure 5-2..

Table 5-3 Autonomous WLAN System Reaction Time

Test Case Topology	Safety I/O RPI (Input/Output) or Safety P/C RPI	Safety I/O CRTL (Input/Output) or Safety P/C CRTL	Observed SRT 99.99% samples	Observed SRT Maximum	Calculated SRT Worst Case No Fault	Calculated SRT Worst Case Single Fault
PAC to I/O, 4 WGBs	18 ms / 40 ms	72 ms / 160 ms	90 ms	124 ms	127 ms	251 ms
PAC to I/O, 12 WGBs	30 ms / 60 ms	120 ms / 240 ms	122 ms	172 ms	183 ms	363 ms
PAC to PAC, 4 WGBs	15 ms	60 ms	76 ms	143 ms	140 ms	188 ms
PAC to PAC, 12 WGBs	40 ms	160 ms	123 ms	156 ms	200 ms	336 ms

Figure 5-2 Wired vs. Wireless SRT



Autonomous WLAN Network Latency and Packet Loss

Table 5-4 and Figure 5-3 shows the results for the network latency and packet loss. The latency values in the table are shown for the downstream and upstream wireless traffic. The important observations are listed below:

- Average latency was 1.5 ms or less.
- Latency for 95% of the samples was below 4 ms.
- Latency for 99.99% of the samples was below 10ms.
- Downstream (AP to WGB) latency was significantly less than the upstream due to the selected QoS parameters.
- The packet loss for the CIP Class 1 traffic was 0.05% or less.
- The system run reliably without any connection losses for the listed test cases.

An example of the latency distribution for the downstream (AP to WGB) and the upstream (WGB to AP) traffic is shown in Figure 5-4

Table 5-4 Autonomous WLAN Latency and Packet Loss

Test Case Topology	Standard I/O or P/C RPI	Safety I/O RPI (Input/Output) or Safety P/C RPI	Latency Average Down/Up	Latency 95% samples Down/Up	Latency 99.99% samples Down/Up	Latency Maximum Observed Down/Up	Packet Loss
PAC to I/O, 4 WGBs	20 ms	18 ms / 40 ms	0.5 / 1.3 ms	1.0 / 3.5 ms	2.5 / 8.0 ms	5.5 / 22.0 ms	0.007%
PAC to I/O, 12 WGBs	30 ms	30 ms / 60 ms	0.5 / 1.4 ms	1.0 / 3.5 ms	3.5 / 8.2 ms	10.3 / 19.1 ms	0.051%
PAC to PAC, 4 WGBs	12 ms	15 ms	0.5 / 1.3 ms	1.0 / 3.5 ms	2.0 / 7.6 ms	5.9 / 17.1 ms	0.005%
PAC to PAC, 12 WGBs	20 ms	40 ms	0.5 / 1.0 ms	1.0 / 3.5 ms	2.5 / 8.0 ms	12.5 / 32.2 ms	0.003%

Figure 5-3 Autonomous WLAN Latency per Test Case

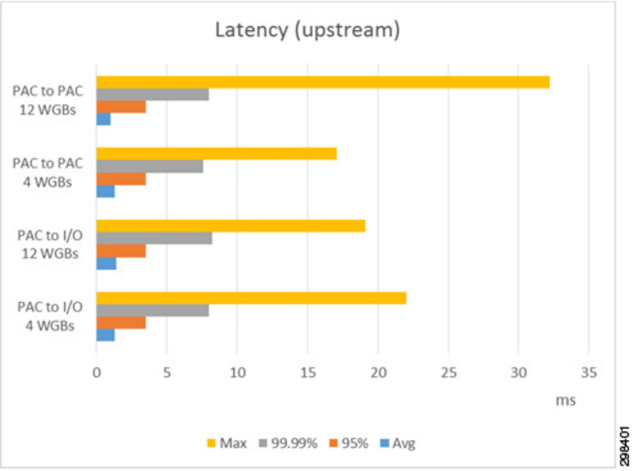
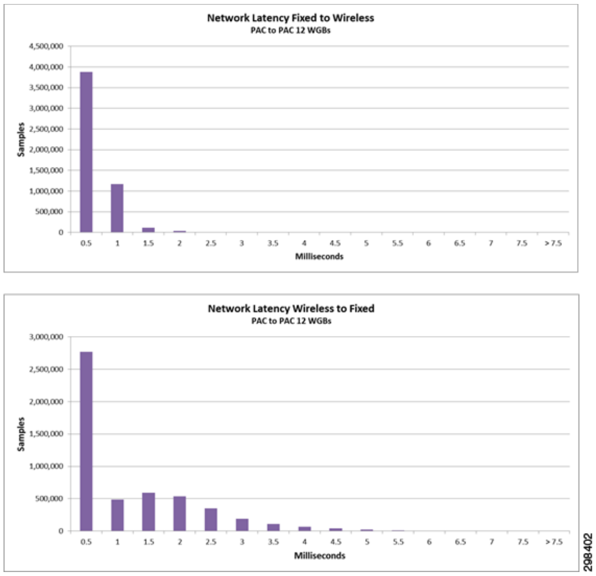


Figure 5-4 Latency Distribution Example



Unified WLAN Testing

The objective of the Unified WLAN testing was to validate centralized architecture for wireless with the recommended architectures and configurations to characterize performance for IACS applications using wireless equipment in same Cell/Area Zone. Testing focused around the following performance characteristics:

- Long-term application reliability: operation without connection timeouts
- Real-time network performance: latency and packet loss
- CIP Safety performance: System Reaction Time

In addition to the performance testing, the following architecture areas described in Chapter 2, "System Design Considerations" and Chapter 3, "Configuring the Infrastructure" have been verified:

- WLAN security (EAP-TLS with CCKM)
- AP redundancy and failover
- Wireless QoS parameters and operation
- AP and WGB replacement procedures
- WLC SSO redundancy

Finally, roaming tests were conducted to validate the use cases for a roaming Industrial device on the plant floor and if it will it lose any connectivity while roaming in the same Cell/Area Zone or different Cell/Area Zones.

Roaming scenarios included two types:

- Inter Cell (between different Cell/Area Zones)
- Intra Cell (within the same Cell/Area Zone)

Roaming testing was focused on following parameters:

- LWAPs running in Local mode (Centralized switching)

- Speed at which the WGB clients move between APs
- Data rates supported for specific speed
- Real-time network performance: latency and packet loss

Unified WLAN Test Setup

The test was conducted in the "best case" RF environment:

- No outside interference or significant signal obstruction
- Wireless channel in the 5 GHz band
- 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. Factors such as RF interference, signal propagation, and antenna characteristics were not considered in the testing.

Roaming tests were conducted in the controlled RF environment:

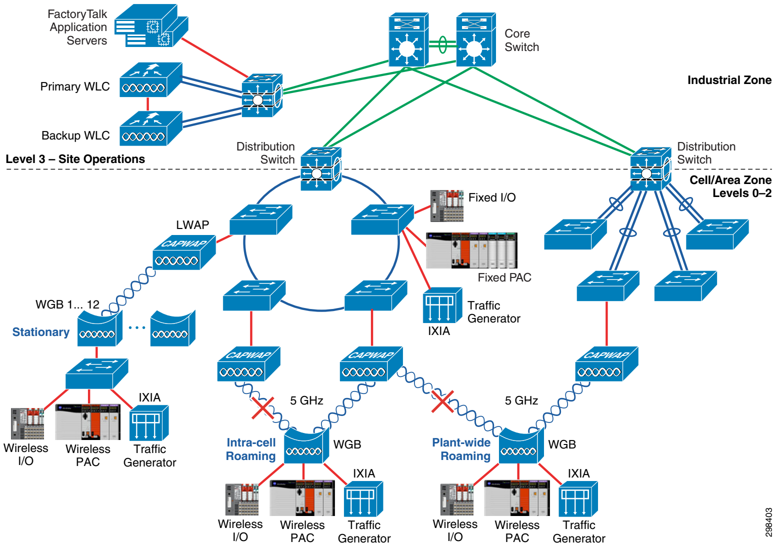
- Two LWAPs connected to the RF attenuator tool to perform attenuation on the signal strength for the graceful handover.
- Setup was run with APs in the local mode (run over CAPWAP).
- Wireless channel in the 5 GHz band with 802.11a/n radios
- One WGB with IACS device and Ixia traffic behind it

An RF attenuation tool was used to perform roaming tests with regards to the speed and signal strength attenuation on AP antennas. Speed of the client was selected based upon certain general assumptions for the output power settings, the initial Received Signal Strength Indicator (RSSI) and Signal to Noise Ratio (SNR) on the WGB client. Refer to Unified WLAN Test Results, page 5-12 for more details on the observations.

Unified WLAN Test Topology

Figure 5-5 shows the lab topology that was used during the testing for all scenarios. Network and IACS hardware and software versions are listed in Table E-1 on page E-1.

Figure 5-5 Unified WLAN Test Topology



Unified WLAN Network Configuration

The wired network infrastructure and WLAN setup were as follows:

- Resilient switch ring topology with REP
- Redundant stackable distribution switches
- Wireless LAN Controller (WLC)
- One LWAP connecting to up to 10 WGBs on the 5GHz radio channel
- The backup LWAP for failover testing
- Standby WLC for WLC SSO
- The RADIUS server to test authentication for EAP-TLS with CCKM
- Ixia Test Chassis for traffic simulation for FactoryTalk View nodes, latency and packet loss measurements

Unified WLAN IACS Configuration

The IACS equipment and software consisted of the following:

- Fixed Safety PAC and I/O connected to the wired infrastructure
- FactoryTalk View server infrastructure
- Wireless Safety PAC and I/O (up to 10) connected to WGBs using a switch topology
- FactoryTalk View nodes simulated using Ixia test chassis

Depending on the test case, the fixed PAC was communicating to the wireless I/O or PAC using standard and safety CIP traffic.

Unified WLAN Test Cases and Parameters

The Unified WLAN test cases for the performance testing were created by selecting the following parameters:

- Number of WGBs in the topology:
  - Large (10 WGBs)
  - Medium (4 WGBs)
  - Small (1 WGBs)
- Type of CIP Class 1 traffic over wireless:
  - Standard and Safety I/O
  - Standard and Safety Produced/Consumed

The standard and safety RPIs for each test case were selected to achieve the packet rate that allowed reliable communication without connection timeouts.

The FactoryTalk View traffic and simulated CIP Class 3 traffic was configured with reference to the total rate for all test cases.

The main test case parameters are listed in Table 5-5.

Table 5-5 Unified WLAN Test Case Parameters

Test Case Topology	# of Standard / Safety Connections	Packet Rate (I/O or P/C)	Packet Rate (Total)	Standard I/O or P/C RPI	Safety I/O RPI (Input/Output) or Safety P/C RPI
PAC to I/O, 1 WGBs	20 / 40	4,050 pps	4,450 pps	10 ms	18 ms / 30 ms
PAC to I/O, 4 WGBs	16 / 32	2,160 pps	2,400 pps	20 ms	18 ms / 40 ms
PAC to I/O, 10 WGBs	20 / 40	1,400 pps	1,600 pps	60 ms	30 ms / 60 ms
PAC to PAC, 1 WGBs	40 / 20	3,800 pps	4,200 pps	20 ms	15 ms
PAC to PAC, 4 WGBs	16 / 8	2,032 pps	2,250 pps	10 ms	15 ms
PAC to PAC, 10 WGBs	20 / 20	1,000 pps	1,200 pps	60 ms	40 ms

The Unified WLAN use cases for Inter cell and Intra cell roaming were created considering the following factors:

- 2 x LWAPs for client roaming
- 1 x WGB client
- Type of CIP Class 1 traffic over wireless—Standard and Safety Produced/Consumed (1 x PLC)
- Ixia streams for higher data traffic simulation & latency measurements
- Test tool for signal attenuation on the APs

Unified WLAN Test Measurements

Table 5-6 lists the metrics that have been measured during the performance testing and pass criteria for each parameter.

Table 5-6 Unified WLAN Test Metrics

Test Metric	Pass Criteria
Safety System Reaction Time (SRT)	Maximum value < calculated Worst Case Single-fault SRT
I/O or Produced/Consumed connection faults	No connection faults (standard or safety)
Network Latency	% of lost packets over the period of test for high priority traffic
% of lost packets, maximum number lost in a row	$\leq$ 2 lost in a row

The details of how the measurements were performed are listed below:

- System Reaction Time was measured as the screw-to-screw time from a safety input module to a safety output module.
- For the PAC to I/O topology, the screw-to-screw time was measured between:
  - Fixed Input module to Wireless Output module
  - Wireless Input module to Fixed Output module
  - Wireless Input module to Wireless Output module
- For the PAC to PAC topology, the screw-to-screw time was measured between the I/O modules connected to the PACs:
  - Fixed PAC (Input module) to Wireless PAC (Output module)
  - Wireless PAC (Input module) to Fixed PAC (Output module)
- The observed SRT results were compared to the Worst Case values (Single Fault and No Fault).
- The tests have been run continuously to monitor for connection losses and to capture maximum values.
- Network latency and packet loss for the CIP Class 1 traffic were measured using the Ixia test chassis.

Note Latency and packet loss for the HMI traffic have not been characterized during the testing.

For the roaming tests, Table 5-7 lists the metrics measured and pass criteria for each parameter.

Table 5-7 Unified WLAN Test Metrics for Roaming

Test Metric	Pass Criteria
CCKM Fast roaming	Client performs fast roaming with re-association to new AP
I/O or Produced/Consumed connection faults	No connection faults (standard or safety)
% of lost packets, Network Latency	Total convergence time for traffic < 100 ms when client roams between APs

The following measurements were done:

- Application convergence time when a WGB roams from one AP to another
- If the IACS device behind the WGB reports connection timeouts

- Data throughput that can be achieved for specific speeds when client roams. Four different speeds were considered: 5, 25, 50, and 100 mph

Unified WLAN Test Results

This section describes the performance test results for the Unified WLAN and some of the observations.

Unified WLAN Safety System Reaction Time

Table 5-8 lists the results for the Safety SRT (screw-to-screw time). The important observations for this parameter are:

- Maximum observed SRT were below "Worst Case Single Fault" and "Worst Case No Fault" calculated SRT
- Results for the safety reaction times were the same for wired and wireless systems except for a very small percentage of samples (<0.01%)

Table 5-8 Unified WL:AN System Reaction Time

Test Case Topology	Safety I/O RPI (Input/Output) or Safety P/C RPI	Safety I/O CRTL (Input/Output) or Safety P/C CRTL	Observed SRT Maximum	Calculated SRT Worst Case No Fault	Calculated SRT Worst Case Single Fault
PAC to I/O, 1 WGBs	18 ms / 30 ms	72 ms / 120 ms	93 ms	117 ms	201 ms
PAC to I/O, 4 WGBs	18 ms / 40 ms	72 ms / 160 ms	95 ms	127 ms	251 ms
PAC to I/O, 10 WGBs	30 ms / 60 ms	120 ms / 240 ms	124 ms	183 ms	363 ms
PAC to PAC, 1 WGBs	15 ms	60 ms	100 ms	140 ms	188 ms
PAC to PAC, 4 WGBs	15 ms	60 ms	81 ms	140 ms	188 ms
PAC to PAC, 10 WGBs	40 ms	160 ms	130 ms	200 ms	336 ms

Unified WLAN Roaming Convergence Time

Table 5-9 lists the WGB roaming with different speeds and the maximum throughput achieved for each speed. In addition, the maximum application convergence as measured by the Ixia tool and whether an IACS timeout was observed are shown.

Table 5-9 Roaming Data Rates and Convergence Results

Speed (mph)	Max Throughput (Mbps)	IACS timeout	Standard RPI (ms)	Safety RPI (ms)	Maximum convergence on IXIA (ms)
5	15	No	20	40	89
25	12	No	20	40	97
50	6.5	No	20	40	83
100	4.5	No	20	40	63

Unified WLAN Network Latency and Packet Loss

Table 5-10 shows the results for the network latency and packet loss. The latency values in the table are shown for the downstream and upstream wireless traffic. The important observations are listed below:

- Average latency was 2.6 ms or less
- Downstream & upstream (AP to WGB) latency were almost the same
- The packet loss for the CIP Class 1 traffic was 0.05% or less
- The system run reliably without any connection losses for the listed test cases

Table 5-10 Unified WLAN Latency and Packet Loss

Test Case Topology	Standard I/O or P/C RPI	Safety I/O RPI (Input/Output) or Safety P/C RPI	Latency Average Down/ Up	Latency Maximum Observed Down/ Up	Packet Loss
PAC to I/O, 1 WGBs	10 ms	18 ms / 30 ms	1.3 / 1.3 ms	22 / 27 ms	0.02%
PAC to I/O, 4 WGBs	20 ms	18 ms / 40 ms	2.1 / 1.6 ms	15 / 16 ms	0.0004%
PAC to I/O, 10 WGBs	60 ms	30 ms / 60 ms	0.9 / 0.8 ms	19 / 23 ms	0.0001%
PAC to PAC, 1 WGBs	10 ms	15 ms	1.7 / 2.4 ms	29 / 40 ms	0.037%
PAC to PAC, 4 WGBs	10 ms	15 ms	2.6 / 2.5 ms	13 / 18 ms	0.0002%
PAC to PAC, 10 WGBs	60 ms	40 ms	1.02 / 0.98 ms	100 / 32 ms	0.0002%

APPENDIX A

References

This appendix includes references for CPwE, Cisco Unified Access, RF Design and QoS and Wireless Security.

Converged Plantwide Ethernet (CPwE)

- Converged Plantwide Ethernet (CPwE) Design and Implementation Guide (CPwE)
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
  - Cisco site: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG.html
- Deploying the Resilient Ethernet Protocol (REP) in a Converged Plantwide Ethernet System (CPwE) Design Guide:
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td005_-en-p.pdf
  - Cisco site: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/REP/CPwE_REP_DG.html

Cisco Unified Access

- Cisco Unified Access webpage
  http://www.cisco.com/en/US/netsol/ns1187/index.html
- Enterprise Mobility Design Guide
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob73dg/eMob73.pdf
- The Benefits of Centralization in Wireless LANs
  http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd8040f7b2.pdf

- Outdoor Wireless Network Solution
http://www.cisco.com/en/US/netsol/ns621/index.html
- Cisco Wireless Mesh Access Points Design and Deployment Guide
http://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/7-6/design/guide/mesh76.html

RF Design and QoS

- Wireless LAN Compliance Status
http://www.cisco.com/go/aironet/compliance
- RF Spectrum Policy: Future-Proof Wireless Investment through Better Compliance
http://www.cisco.com/c/en/us/products/collateral/wireless/spectrum-expert/prod_white_paper0900aecd8073bef9.html
- Design Zone for Mobility - High Density Wireless
http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-mobility/density_wireless.html
- Enterprise Mobility 7.3 Design Guide
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob73dg/emob73.html
- Cisco Aironet 1600/2600/3600 Series Access Point Deployment Guide
http://www.cisco.com/c/en/us/td/docs/wireless/technology/apdeploy/Cisco_Aironet.html
- Antenna Product Portfolio for Cisco Aironet 802.11n Access Points
http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/at_a_glance_c45-513837.pdf
- Cisco Aironet Antennas and Accessories Reference Guide
http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.pdf
- Antenna Patterns and Their Meaning
http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/prod_white_paper0900aecd806a1a3e.pdf
- Antenna Cabling
http://www.cisco.com/image/gif/paws/27222/antcable.pdf
- Site Survey Guidelines for WLAN Deployment
http://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html
- Site Survey and RF Design Validation
http://www.cisco.com/en/US/docs/wireless/technology/vowlan/troubleshooting/8_Site_Survey_RF_Design_Valid.pdf
- Cisco Unified Wireless QoS
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob73dg/emob73/ch5_QoS.html

Wireless Security

- Cisco Unified Wireless Network Architecture -Base Security Features http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob73dg/emob73/ch4_Secu.html
- Design Zone for Mobility - Wireless Security http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns820/landing_sec_wireless.html

APPENDIX B

CLI Configuration Examples

This appendix includes Autonomous WLAN and Unified WLAN CLI examples.

Autonomous WLAN CLI Examples

This section contains examples of the Stratix 5100 configurations that have been used in the testing of the Autonomous WLAN architecture.

- The configurations are provided for reference only and must not be used "as is" without adapting for a particular IACS application and topology.
- The examples here were used with the IOS 15.2(4)JAZ. Future software releases may change some of the commands.
- Many commands are factory default and do not have to be configured during the initial setup.

Example: Access Point with WPA2-PSK and no VLANs

This example shows a Stratix 5100 configured in the AP role with no VLANs, a single SSID on the 5 GHz radio, and WPA2-PSK security.

```
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname <AP NAME>
!
logging rate-limit console 9
enable secret <ENABLE PASSWORD>
!
no aaa new-model
no ip routing
no ip cef
!
dot11 syslog
!
dot11 ssid <SSID>
```

```
   authentication open
   authentication key-management wpa version 2
   wpa-psk ascii <PRESHARED KEY>
   no ids mfp client
!
dot11 phone dot11e
dot11 guest
!
cip security password <CIP PASSWORD>
username <USERNAME> secret <PASSWORD>
!
!
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 CIP-PTP-Traffic-AP
 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
 no ip route-cache
 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 <SSID>
 !
 antenna gain 4
 peakdetect
 dfs band 3 block
 stbc
 guard-interval long
 speed basic-6.0 basic-9.0 basic-12.0 basic-18.0 basic-24.0 basic-36.0 basic-48.0
basic-54.0
 power local <POWER LEVEL>
 packet retries 8 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 <CHANNEL>
 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 7
    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 7
    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 output CIP-PTP-Traffic-AP
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 no keepalive
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 ip address <IP ADDRESS> <MASK>
 no ip route-cache
 cip enable
 no cip write
!
ip default-gateway <GATEWAY>
ip forward-protocol nd
ip http server
ip http secure-server
!
bridge 1 route ip
!
line con 0
 logging synchronous
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
end
```

Example: Access Point with WPA2-PSK and two VLANs / SSIDs

This example shows a Stratix 5100 configured in the AP role with two VLANs and two SSIDs (one per radio), and WPA2-PSK security.

```
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname <AP NAME>
!
logging rate-limit console 9
enable secret <ENABLE PASSWORD>
!
```

```
no aaa new-model
no ip routing
no ip cef
!
dot11 syslog
!
dot11 ssid <CONTROL SSID>
   vlan 10
   authentication open
   authentication key-management wpa version 2
   wpa-psk ascii <PRESHARED KEY>
   no ids mfp client
!
dot11 ssid <MAINT SSID>
   vlan 20
   authentication open
   authentication key-management wpa version 2
   wpa-psk ascii <PRESHARED KEY>
   no ids mfp client
!
dot11 phone dot11e
dot11 guest
!
cip security password <CIP PASSWORD>
username <USERNAME> secret <PASSWORD>
!
!
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 CIP-PTP-Traffic-AP
 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
 no ip route-cache
 !
 encryption vlan 20 mode ciphers aes-ccm
 !
 ssid <MAINT SSID>
 !
 antenna gain 2
 peakdetect
 dfs band 3 block
 stbc
 guard-interval long
 speed basic-6.0 basic-9.0 basic-12.0 basic-18.0 basic-24.0 basic-36.0 basic-48.0
basic-54.0
 power local <POWER LEVEL>
 packet retries 8 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 <CHANNEL>
 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 7
    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 7
    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
!
interface Dot11Radio0.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
 bridge-group 20 subscriber-loop-control
 bridge-group 20 spanning-disabled
 bridge-group 20 block-unknown-source
 no bridge-group 20 source-learning
 no bridge-group 20 unicast-flooding
 service-policy output CIP-PTP-Traffic-AP
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 encryption vlan 10 mode ciphers aes-ccm
 !
 ssid <CONTROL SSID>
 !
 antenna gain 4
 peakdetect
 dfs band 3 block
 stbc
 guard-interval long
 speed basic-6.0 basic-9.0 basic-12.0 basic-18.0 basic-24.0 basic-36.0 basic-48.0
basic-54.0
 power local <POWER LEVEL>
 packet retries 8 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 <CHANNEL>
 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 7
    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 7
    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
!
interface Dot11Radio1.10
 encapsulation dot1Q 10 native
 no ip route-cache
 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 output CIP-PTP-Traffic-AP
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 no keepalive
!
interface GigabitEthernet0.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface GigabitEthernet0.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
 bridge-group 20 spanning-disabled
 no bridge-group 20 source-learning
!
interface BVI1
 ip address <IP ADDRESS> <MASK>
 no ip route-cache
 cip enable
 no cip write
```

```
!
ip default-gateway <GATEWAY>
ip forward-protocol nd
ip http server
ip http secure-server
!
bridge 1 route ip
!
line con 0
 logging synchronous
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
end
```

Example: Workgroup Bridge with WPA2-PSK

This example shows a Stratix 5100 configured in the WGB role with the WPA2-PSK security.

```
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname <WGB NAME>
!
logging rate-limit console 9
enable secret <ENABLE PASSWORD>
!
no aaa new-model
no ip routing
no ip cef
!
dot11 syslog
!
dot11 ssid <SSID>
   authentication open
   authentication key-management wpa version 2
   wpa-psk ascii <PRESHARED KEY>
   no ids mfp client
!
dot11 phone dot11e
dot11 guest
!
cip security password <CIP PASSWORD>
username <USERNAME> secret <PASSWORD>
!
!
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 CIP-PTP-Traffic-AP
 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
 no ip route-cache
 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 <SSID>
 !
 antenna gain 4
 peakdetect
 dfs band 3 block
 stbc
 guard-interval long
 speed basic-6.0 basic-9.0 basic-12.0 basic-18.0 basic-24.0 basic-36.0 basic-48.0
basic-54.0
 power local <POWER LEVEL>
 packet retries 8 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
 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
 no bridge-group 1 unicast-flooding
 service-policy output CIP-PTP-Traffic-AP
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 no keepalive
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 ip address <IP ADDRESS> <MASK>
 no ip route-cache
 cip enable
 no cip write
!
ip default-gateway <GATEWAY>
ip forward-protocol nd
ip http server
ip http secure-server
!
bridge 1 route ip
!
line con 0
 logging synchronous
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
End
```

Unified WLAN CLI Examples

This section contains examples of the configurations that have been used in the testing of the Unified WLAN architecture.

- The configurations are provided for reference only and must not be used "as is" without adapting for a particular IACS application and topology.
- Future software releases may change some of the commands shown in the configurations.
- Many commands are factory default and do not have to be configured during the initial setup.

Example: Stationary WGB with EAP-TLS Authentication

```
version 15.2
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname <WGB NAME>
!
logging rate-limit console 9
enable secret 5 <ENABLE PASSWORD>
!
no aaa new-model
clock timezone EST -5 0
clock summer-time EDT recurring
clock save interval 8
no ip routing
no ip cef
ip domain name cpwe.cisco.local
!
dot11 syslog
!
dot11 ssid CPwE350-R1-Flex
    authentication network-eap CPwE350-EAPTLS
    authentication key-management wpa version 2
    dot1x credentials CPwE350-dot1x
    dot1x eap profile CPwE350-EAPTLS
    no ids mfp client
!
dot11 guest
!
eap profile CPwE350-EAPTLS
 method tls
!
crypto pki trustpoint TP-self-signed-2188441776
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2188441776
 revocation-check none
 rsakeypair TP-self-signed-2188441776
!
crypto pki trustpoint CPwE350-CA
 enrollment mode ra
 enrollment url http://10.13.48.34:80/certsrv/mscep/mscep.dll
 subject-name cn=AP2602-F-WGB01.cpwe.cisco.local
 revocation-check none
 rsakeypair EAP-TLS2048
 auto-enroll 90
!
dot1x credentials CPwE350-dot1x
 username AP2602-R-WGB01
 pki-trustpoint CPwE350-CA
!
username Cisco password 7 123A0C041104
!
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
 class _class_EXPLICIT
  set cos 0
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 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
 load-interval 30
 !
 encryption mode ciphers aes-ccm
 !
 ssid CPwE350-R1-Flex
 !
 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 5
 packet retries 16 drop-packet
 packet speed 6.0 54.0 priority 6
 station-role workgroup-bridge
 mobile station scan 5180 5200 5220 5240
 mobile station minimum-rate 6.0
 !
 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
 service-policy input ODVA
 service-policy output ODVA
!
interface GigabitEthernet0
```

```
 no ip address
 no ip route-cache
 load-interval 30
 duplex auto
 speed auto
 no keepalive
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address dhcp
 no ip route-cache
 load-interval 30
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
ip forward-protocol nd
ip http server
ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
!
bridge 1 route ip
bridge 1 aging-time 3600
!
line con 0
 exec-timeout 0 0
line vty 0 4
 login local
 length 0
 transport input all
!
sntp server 10.13.48.20
workgroup-bridge timeouts eap-timeout 4
workgroup-bridge timeouts auth-response 800
workgroup-bridge timeouts assoc-response 800
workgroup-bridge timeouts client-add 800
end
```

Example: Roaming WGB with EAP-TLS Authentication

```
version 15.2
 no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname <WGB NAME>!
!
logging rate-limit console 9
enable secret 5 <ENABLE PASSWORD>
!
no aaa new-model
clock timezone EST -5 0
clock summer-time EDT recurring
clock save interval 8
no ip routing
no ip cef
ip domain name cpwe.cisco.local
!
dot11 syslog
!
```

```
dot11 ssid CPwE350-Roam
   vlan 250
   authentication network-eap CPwE350-EAPTLS
   authentication key-management wpa version 2 cckm
   dot1x credentials CPwE350-dot1x
   dot1x eap profile CPwE350-EAPTLS
   no ids mfp client
!
dot11 guest
!
eap profile CPwE350-EAPTLS
method tls
!
crypto pki trustpoint TP-self-signed-2188441346
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-2188441346
revocation-check none
rsakeypair TP-self-signed-2188441346
!
crypto pki trustpoint CPwE350-CA
enrollment mode ra
enrollment url http://10.13.48.34:80/certsrv/mscep/mscep.dll
subject-name cn=AP2602-R-WGB05.cpwe.cisco.local
revocation-check none
rsakeypair EAP-TLS2048
auto-enroll 90
!
dot1x credentials CPwE350-dot1x
username AP2602-R-WGB05
pki-trustpoint CPwE350-CA
!
username Cisco password 7 112A1016141D
!
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
class _class_EXPLICIT
  set cos 0
!
```

```
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
shutdown
antenna gain 0
stbc
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
load-interval 30
!
encryption vlan 250 mode ciphers aes-ccm
!
ssid CPwE350-Roam
!
antenna gain 4
peakdetect
stbc
stbc
 no ampdu transmit priority 0
 no ampdu transmit priority 4
 no ampdu transmit priority 5
 guard-interval long
 power local 5
 packet retries 16 drop-packet

packet speed 6.0 54.0 priority 6
station-role workgroup-bridge
mobile station scan 5220
mobile station minimum-rate 6.0
mobile station period 1 threshold 60
!
no cdp enable
service-policy input ODVA
service-policy output ODVA
!
interface Dot11Radio1.250
encapsulation dot1Q 250 native
no ip route-cache
no cdp enable
bridge-group 1
bridge-group 1 spanning-disabled
!
interface GigabitEthernet0
no ip address
no ip route-cache
load-interval 30
duplex auto
speed auto
!
interface GigabitEthernet0.250
encapsulation dot1Q 250 native
no ip route-cache
no keepalive
```

```
bridge-group 1
bridge-group 1 spanning-disabled
!
interface BVI1
ip address dhcp
no ip route-cache
load-interval 30
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
!
ip forward-protocol nd
ip http server
ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
!
bridge 1 route ip
bridge 1 aging-time 3600
!
line con 0
exec-timeout 0 0
line vty 0 4
login local
transport input all
!
sntp server 10.13.48.20
workgroup-bridge timeouts eap-timeout 4
workgroup-bridge timeouts auth-response 800
workgroup-bridge timeouts assoc-response 800
workgroup-bridge timeouts client-add 800
end
```

Example: WLC Configuration

```
(Cisco Controller) >show run-config commands

redundancy mode SSO (Both AP and Client SSO)

802.11a 11nSupport a-mpdu tx priority 6 enable
802.11a 11nSupport a-mpdu tx priority 7 enable
802.11a 11nSupport a-mpdu tx scheduler enable
802.11a 11nSupport a-mpdu tx scheduler timeout rt 10
802.11a 11nSupport disable
802.11a 11nSupport guard_interval long
802.11a beacon range 0
802.11a rx-sop threshold 0 default
802.11a cca threshold 0 default
802.11a multicast buffer 0
802.11a multicast data-rate 0 default
802.11a cac voice max-bandwidth 40
802.11a cac video max-bandwidth 40
802.11a cac voice roam-bandwidth 15
802.11a cac video roam-bandwidth 15
802.11a channel global off
802.11a rssi-check enable
802.11a max-clients 200
802.11a rate disabled 9
802.11a rate disabled 18
802.11a rate disabled 36
802.11a rate disabled 48
802.11a txPower global 1
802.11a dfs-peakdetect enable
```

```
802.11b 11nSupport a-mpdu tx scheduler enable
802.11b 11nSupport a-mpdu tx scheduler timeout rt 10
802.11b 11gSupport disable
802.11b beacon range 0
802.11b rx-sop threshold 0 default
802.11b cca threshold 0 default
802.11b multicast buffer 0
802.11b multicast data-rate 0 default
802.11b cac video cac-method static
802.11b channel global off
802.11b max-clients 200
802.11b txPower global 1

aaa auth mgmt local radius
flexconnect fallback-radio-shut disable

advanced 802.11a channel dca interval 0
advanced 802.11a channel dca anchor-time 0
advanced 802.11a channel dca channel-width 20
advanced 802.11a channel dca sensitivity 15
advanced 802.11a channel dca min-metric -95
advanced 802.11a channel delete 20
advanced 802.11a channel delete 26
advanced 802.11a reporting neighbor 180
advanced 802.11a reporting interference 120
advanced 802.11b channel dca interval 0
advanced 802.11b channel dca anchor-time 0
advanced 802.11b channel dca sensitivity 10
advanced 802.11b channel dca min-metric -95
advanced 802.11b reporting neighbor 180
advanced 802.11b reporting interference 120

location rssi-half-life tags 0
location rssi-half-life client 0
location rssi-half-life rogue-aps 0
location expiry tags 5
location expiry client 5
location expiry calibrating-client 5
location expiry rogue-aps 5

advanced timers ap-heartbeat-timeout 10
advanced timers ap-fast-heartbeat flexconnect enable 1
advanced backup-controller primary
advanced backup-controller secondary
advanced backup-controller
advanced backup-controller
advanced sip-snoop-ports 0 0
avc profile PAC_IO_SAFETY create
advanced eap bcast-key-interval 3600
advanced hotspot cmbk-delay 50

ap syslog host global 0.0.0.0
ap dtls-cipher-suite RSA-AES128-SHA

auth-list ap-policy ssc enable
auth-list add mic 3c:08:f6:20:d2:17
auth-list add mic 3c:08:f6:a2:d3:b0
auth-list add mic 3c:08:f6:b2:8d:d6
auth-list add mic 3c:08:f6:b2:98:e4
auth-list add mic 78:da:6e:42:9c:2e
auth-list add mic a8:0c:0d:be:a6:7e

cdp advertise-v2 enable
```

```
cts sxp disable
cts sxp connection default password ****
cts sxp retry period 120
cts sxp sxpversion 2

database size 2048

dhcp opt-82 remote-id ap-mac

flexconnect group FastRoam_CCKM_Flex_Ring add
flexconnect group FastRoam_CCKM_Flex_Ring ap add 3c:08:f6:20:d2:17
flexconnect group FastRoam_CCKM_Flex_Ring radius ap server-key <hidden>
flexconnect group FastRoam_CCKM_Flex_Ring radius ap authority id
436973636f0000000000000000000000
flexconnect group FastRoam_CCKM_Flex_Ring radius ap authority info Cisco A_ID
flexconnect group FastRoam_CCKM_Flex_Star add
flexconnect group FastRoam_CCKM_Flex_Star radius ap server-key <hidden>
flexconnect group FastRoam_CCKM_Flex_Star radius ap authority id
436973636f0000000000000000000000
flexconnect group FastRoam_CCKM_Flex_Star radius ap authority info Cisco A_ID

local-auth eap-profile add CPwE350-EAP-FAST
local-auth eap-profile add CPwE350-EAP-TLS
local-auth eap-profile cert-issuer cisco CPwE350-EAP-FAST
local-auth eap-profile cert-issuer vendor CPwE350-EAP-TLS
local-auth eap-profile method add fast CPwE350-EAP-FAST
local-auth eap-profile method add tls CPwE350-EAP-TLS
local-auth eap-profile method fast client-cert enable CPwE350-EAP-TLS
local-auth eap-profile method fast local-cert enable CPwE350-EAP-TLS
local-auth method fast server-key ****
local-auth eap-profile cert-verify ca-issuer disable CPwE350-EAP-FAST
local-auth eap-profile cert-verify date-valid disable CPwE350-EAP-FAST

interface create wgb-roam-client 250
interface address management 10.13.50.251 255.255.255.0 10.13.50.1
interface address service-port 192.168.254.83 255.255.255.0
interface address virtual 1.1.1.1
interface address dynamic-interface wgb-roam-client 10.17.250.251 255.255.255.0
10.17.250.1
interface address redundancy-management 10.13.50.253 (null) (null)
redundancy interface address peer-redundancy-management 10.13.50.252
interface dhcp management primary 10.13.48.10
interface dhcp dynamic-interface wgb-roam-client primary 10.13.48.10
interface vlan management 150
interface vlan wgb-roam-client 250
interface nasid wgb-roam-client
interface port management 1
interface port wgb-roam-client 1

ipv6 ra-guard ap enable
ipv6 multicast mode unicast

load-balancing aggressive enable
load-balancing window 5

wlan apgroup add CPwE350-Flex-Ring01 FlexRing01
wlan apgroup add CPwE350-Flex-Star01 FlexStar01
wlan apgroup add CPwE350-Roam-central "For roaming clients"
wlan apgroup add default-group
wlan apgroup interface-mapping add CPwE350-Flex-Ring01 1 management
wlan apgroup interface-mapping add CPwE350-Flex-Star01 2 management
wlan apgroup interface-mapping add CPwE350-Roam-central 3 wgb-roam-client
wlan apgroup interface-mapping add default-group 1 management
wlan apgroup interface-mapping add default-group 2 management
wlan apgroup interface-mapping add default-group 3 wgb-roam-client
wlan apgroup nac-snmp disable CPwE350-Flex-Ring01 1
wlan apgroup nac-snmp disable CPwE350-Flex-Star01 2
wlan apgroup nac-snmp disable CPwE350-Roam-central 3
wlan apgroup nac-snmp disable default-group 1
wlan apgroup nac-snmp disable default-group 2
wlan apgroup nac-snmp disable default-group 3

memory monitor errors enable
memory monitor leak thresholds 10000 30000

mesh security rad-mac-filter disable
mesh security rad-mac-filter disable
mesh security eap

mgmtuser add admin **** read-write

mobility group domain CPwE350-MG01
mobility dscp 0

netuser add AP2602-R-WGB05 **** wlan 0 userType permanent description
netuser wlan-id AP2602-R-WGB05 0
netuser guest-role create PAC_IO_SAFETY

network ap-priority disabled
network rf-network-name CPwE350-MG01
network secureweb cipher-option rc4-preference disable

port adminmode 2 disable
port adminmode 3 disable
port adminmode 4 disable
port adminmode 5 disable
port adminmode 6 disable
port adminmode 7 disable
port adminmode 8 disable

qos protocol-type bronze dot1p
qos protocol-type silver dot1p
qos protocol-type gold dot1p
qos protocol-type platinum dot1p
qos priority bronze background background background
qos priority gold video video video
qos priority platinum voice voice voice
qos priority silver besteffort besteffort besteffort
qos dot1p-tag silver 2
qos dot1p-tag gold 4
qos dot1p-tag platinum 5

radius auth add 1 10.13.48.40 1812 ascii ****
radius callStationIdType macaddr
radius auth callStationIdType ap-macaddr-ssid
radius fallback-test mode off
radius fallback-test username cisco-probe
radius fallback-test interval 300
radius dns disable

tacacs dns disable

rogue detection report-interval 10
rogue detection min-rssi -128
rogue detection transient-rogue-interval 0
rogue detection client-threshold 0
rogue detection security-level custom
rogue ap ssid alarm
rogue ap valid-client alarm
rogue adhoc enable
rogue adhoc alert
rogue ap rldp disable
config rogue auto-contain level 1
rogue containment flex-connect disable
rogue containment auto-rate disable

serial timeout 0
sessions timeout 0

snmp version v2c enable
snmp version v3 enable
snmp snmpEngineId 000037630000a360fb320d0a
snmp community ipsec ike auth-mode pre-shared-key ****

switchconfig strong-pwd case-check enabled
switchconfig strong-pwd consecutive-check enabled
switchconfig strong-pwd default-check enabled
switchconfig strong-pwd username-check enabled
switchconfig strong-pwd position-check disabled
switchconfig strong-pwd case-digit-check disabled
switchconfig strong-pwd minimum upper-case 0
switchconfig strong-pwd minimum lower-case 0
switchconfig strong-pwd minimum digits-chars 0
switchconfig strong-pwd minimum special-chars 0
switchconfig strong-pwd min-length 3

sysname WLC_Primary

stats-timer realtime 5
stats-timer normal 180

time ntp interval 3600
time ntp server 1 192.168.254.20

rf-profile create 802.11a CPwE350-Flex-RFPolicy
rf-profile create 802.11a CPwE350-Roam-RFPolicy
rf-profile description "Single Cell/Area LWAP RF Policy" CPwE350-Flex-RFPolicy
rf-profile description "Plant-wide Roaming LWAP RF Policy" CPwE350-Roam-RFPolicy
rf-profile data-rates 802.11a mandatory 6 CPwE350-Flex-RFPolicy
rf-profile data-rates 802.11a supported 9 CPwE350-Flex-RFPolicy
rf-profile data-rates 802.11a mandatory 12 CPwE350-Flex-RFPolicy
rf-profile data-rates 802.11a supported 18 CPwE350-Flex-RFPolicy
rf-profile data-rates 802.11a mandatory 24 CPwE350-Flex-RFPolicy
rf-profile data-rates 802.11a supported 36 CPwE350-Flex-RFPolicy
rf-profile data-rates 802.11a supported 48 CPwE350-Flex-RFPolicy
rf-profile data-rates 802.11a supported 54 CPwE350-Flex-RFPolicy
rf-profile data-rates 802.11a mandatory 6 CPwE350-Roam-RFPolicy
rf-profile data-rates 802.11a supported 9 CPwE350-Roam-RFPolicy
rf-profile data-rates 802.11a mandatory 12 CPwE350-Roam-RFPolicy
rf-profile data-rates 802.11a supported 18 CPwE350-Roam-RFPolicy
rf-profile data-rates 802.11a mandatory 24 CPwE350-Roam-RFPolicy
rf-profile data-rates 802.11a supported 36 CPwE350-Roam-RFPolicy
rf-profile data-rates 802.11a supported 48 CPwE350-Roam-RFPolicy
rf-profile data-rates 802.11a supported 54 CPwE350-Roam-RFPolicy

trapflags client nac-alert enable
trapflags ap ssidKeyConflict disable
trapflags ap timeSyncFailure disable
trapflags adjchannel-rogueap disable
trapflags mesh excessive hop count disable
trapflags mesh sec backhaul change disable
```

```
wlan create 1 "CPwE350 Ring#1 Flex" CPwE350-R1-Flex
wlan create 2 "CPwE350 Star#1 Flex" CPwE350-S1-Flex
wlan create 3 CPwE350-Roam CPwE350-Roam
wlan nac snmp disable 1
wlan nac snmp disable 2
wlan nac snmp disable 3
wlan nac radius disable 1
wlan nac radius disable 2
wlan nac radius disable 3
wlan interface 3 wgb-roam-client
wlan multicast interface 1 disable
wlan multicast interface 2 disable
wlan multicast interface 3 disable
wlan broadcast-ssid disable 1
wlan broadcast-ssid disable 2
wlan broadcast-ssid disable 3
wlan band-select allow disable 1
wlan band-select allow disable 2
wlan band-select allow disable 3
wlan load-balance allow disable 1
wlan load-balance allow disable 2
wlan load-balance allow disable 3
wlan multicast buffer disable 0 1
wlan multicast buffer disable 0 2
wlan multicast buffer disable 0 3
wlan qos 1 platinum
wlan qos 2 platinum
wlan qos 3 platinum
wlan radio 1 802.11a-only
wlan radio 2 802.11a-only
wlan radio 3 802.11a-only
wlan session-timeout 1 disable
wlan session-timeout 2 1800
wlan session-timeout 3 1800
wlan flexconnect local-switching 1 enable
wlan flexconnect local-switching 2 enable
wlan flexconnect local-switching 3 disable
wlan flexconnect learn-ipaddr 1 enable
wlan flexconnect learn-ipaddr 2 enable
wlan flexconnect learn-ipaddr 3 enable
wlan security wpa disable 2
wlan radius_server auth add 1 1
wlan radius_server acct disable 1
wlan radius_server auth add 2 1
wlan radius_server acct disable 2
wlan radius_server auth add 3 1
wlan radius_server acct disable 3
wlan radius_server overwrite-interface apgroup 3
wlan security splash-page-web-redir disable 1
wlan security splash-page-web-redir disable 2
wlan security splash-page-web-redir disable 3
wlan user-idle-threshold 70 1
wlan user-idle-threshold 70 2
wlan user-idle-threshold 70 3
wlan security wpa akm 802.1X enable 1
wlan security wpa akm cckm enable 1
wlan security wpa akm 802.1X enable 3
wlan security wpa akm cckm enable 3
wlan security wpa akm cckm timestamp-tolerance 1000 1
wlan security wpa akm cckm timestamp-tolerance 1000 2
wlan security wpa akm cckm timestamp-tolerance 1000 3
wlan security ft enable 1
wlan security ft over-the-ds disable 1
wlan security ft over-the-ds disable 2
wlan security ft over-the-ds disable 3
wlan security wpa gtk-random disable 1
wlan security wpa gtk-random disable 2
wlan security wpa gtk-random disable 3
wlan security pmf association-comeback 1 1
wlan security pmf association-comeback 1 2
wlan security pmf association-comeback 1 3
wlan security pmf saquery-retrytimeout 200 1
wlan security pmf saquery-retrytimeout 200 2
wlan security pmf saquery-retrytimeout 200 3
wlan profiling radius dhcp disable 1
wlan profiling radius http disable 1
wlan profiling radius dhcp disable 2
wlan profiling radius http disable 2
wlan profiling radius dhcp disable 3
wlan profiling radius http disable 3
wlan apgroup hotspot venue type CPwE350-Flex-Ring01 0 0
wlan apgroup hotspot venue type CPwE350-Flex-Star01 0 0
wlan apgroup hotspot venue type CPwE350-Roam-central 0 0
802.11b disable network
wlan enable 1
wlan enable 2
wlan enable 3

license agent default authenticate none
license boot base
WMM-AC disabled
coredump disable

media-stream multicast-direct disable
media-stream message url
media-stream message email
media-stream message phone
media-stream message note denial
media-stream message state disable
802.11a media-stream multicast-direct enable
802.11b media-stream multicast-direct enable
802.11a media-stream multicast-direct radio-maximum 0
802.11b media-stream multicast-direct radio-maximum 0
802.11a media-stream multicast-direct client-maximum 0
802.11b media-stream multicast-direct client-maximum 0
802.11a media-stream multicast-direct admission-besteffort disable
802.11b media-stream multicast-direct admission-besteffort disable
802.11a media-stream video-redirect enable
802.11b media-stream video-redirect enable

ipv6 neighbor-binding timers reachable-lifetime 300
ipv6 neighbor-binding timers stale-lifetime 86400
ipv6 neighbor-binding timers down-lifetime 30
ipv6 neighbor-binding ra-throttle disable
ipv6 neighbor-binding ra-throttle allow at-least 1 at-most 1
ipv6 neighbor-binding ra-throttle max-through 10
ipv6 neighbor-binding ra-throttle throttle-period 600
ipv6 neighbor-binding ra-throttle interval-option passthrough
ipv6 NS Multicast Cachemiss Forward disable
ipv6 NA Multicast Forward enable
ipv6 Global Config enable

nmheartbeat disable
```

APPENDIX C

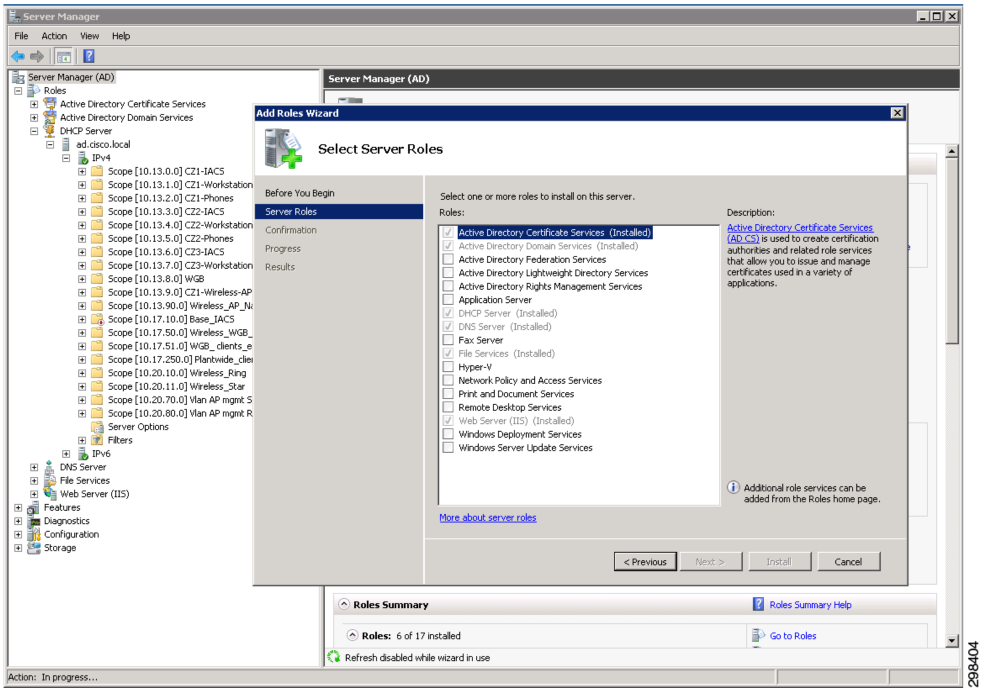
Server Infrastructure Configuration

This appendix includes the configurations for the DHCP, DNS, Active Directory, Root-CA and RADIUS servers.

DHCP Server Setup

Step 1 Enable DHCP service: Windows 2008 Server DHCP service is located in *Start > Administrative Tools > Server Manager (CPWE-AD) > Roles*. Right-click *Roles > Add Roles Wizard > DHCP service* and then follow the instructions to enable DHCP. Figure C-1 shows the window where the DHCP service is enabled.

Figure C-1 DHCP Server Role Setup


Server Manager
File
Action
View
Help
Server Manager (AD)
Roles
Active Directory Certificate Services
Active Directory Domain Services
DHCP Server
ad.cisco.local
IPv4
Scope [10.13.0.0] CZ1-IACS
Scope [10.13.1.0] CZ1-Workstation
Scope [10.13.2.0] CZ1-Phones
Scope [10.13.3.0] CZ2-IACS
Scope [10.13.4.0] CZ2-Workstation
Scope [10.13.5.0] CZ2-Phones
Scope [10.13.6.0] CZ3-IACS
Scope [10.13.7.0] CZ3-Workstation
Scope [10.13.8.0] WGB
Scope [10.13.9.0] CZ1-Wireless-AP
Scope [10.13.90.0] Wireless_AP_N
Scope [10.17.10.0] Base_IACS
Scope [10.17.50.0] Wireless_WGB_
Scope [10.17.51.0] WGB_ clients_e
Scope [10.17.250.0] Plantwide_clie
Scope [10.20.10.0] Wireless_Ring
Scope [10.20.11.0] Wireless_Star
Scope [10.20.70.0] Vlan AP mgmt S
Scope [10.20.80.0] Vlan AP mgmt R
Server Options
Filters
IPv6
DNS Server
File Services
Web Server (IIS)
Features
Diagnostics
Configuration
Storage
Server Manager (AD)
Add Roles Wizard
Select Server Roles
Before You Begin
Server Roles
Confirmation
Progress
Results
More about server roles
< Previous
Next >
Install
Cancel
Roles Summary
Roles Summary Help
Go to Roles
298404

Select one or more roles to install on this server.

Roles:

- ☑ Active Directory Certificate Services (Installed)
- ☑ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ☑ File Services (Installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Desktop Services
- ☑ Web Server (IIS) (Installed)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

Description:

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Additional role services can be added from the Roles home page.

Roles: 6 of 17 installed

Refresh disabled while wizard in use

Action: In progress...

Step 2 Create DHCP server: Once DHCP service is enabled, right-click it and select *Add Role Services* to create DHCP server. Name it *ad.cisco.local* or any other preferred name.

Step 3 Add scopes: Click DHCP server and expand "IPv4" to add DHCP scopes as below:

a. WLC Primary (10.20.80.x scope)

b. WLC backup (10.20.70.x scope) and its corresponding local VLAN

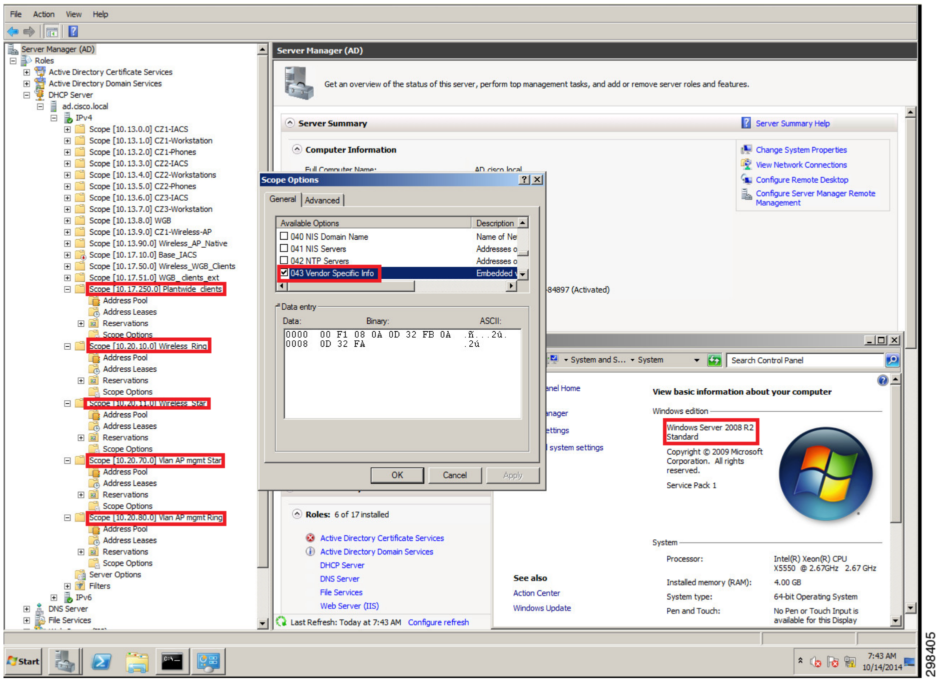
c. Ring topology (10.20.10.x scope) and Star topology (10.20.11.x scope) for plant-wide inter-cell roaming

d. The IACS devices has the requirement to keep its original IP address while roaming across plant-wide. Normally, static IP addresses are used for IACS devices and WGBs. If DHCP method is preferred, a separate DHCP scope (10.17.250.x subnet) has been created for this purpose.

Note Once DHCP scope has been created, make sure to activate the scope. Also, it is recommended to reserve some portion of the scope for management purposes.

Step 4 Configure DHCP Option 43: WLCs are located in the industrial zone server farm and connect to Cell/Area Zone LWAPs and WGBs via Layer 3 routing protocol. In this scenario, DHCP option 43 is required for the LWAP to locate the WLC in the Layer 3 domain. DHCP option 43 is a hex string assembled by concatenating the Type + Length + Value into a TLV value pair. Type is 00 F1. Length is the number of WLC management interface IP addresses times 4 in hex (for example, in the Unified WLAN setup with primary and backup WLCs, this value will be 2 * 4 = 8, or in hex, 08 as shown in Figure C-2.) Values correspond to each WLC management IP address (for example, 0A 0D 32 FB and 0A 0D 32 FA correspond to IP addresses of 10.13.50.251 and 10.13.50.252, respectively).

Figure C-2 Central DHCP Server Setup



Server Manager (AD)
- Roles
  - Active Directory Certificate Services
  - Active Directory Domain Services
  - DHCP Server
    - ad.cisco.local
      - IPv4
        - Scope [10.13.0.0] CZ1-IACS
        - Scope [10.13.1.0] CZ1-Workstation
        - Scope [10.13.2.0] CZ1-Phones
        - Scope [10.13.3.0] CZ2-IACS
        - Scope [10.13.4.0] CZ2-Workstations
        - Scope [10.13.5.0] CZ2-Phones
        - Scope [10.13.6.0] CZ3-IACS
        - Scope [10.13.7.0] CZ3-Workstation
        - Scope [10.13.8.0] WGB
        - Scope [10.13.9.0] CZ1-Wireless-AP
        - Scope [10.13.90.0] Wireless_AP_Native
        - Scope [10.17.10.0] Base_IACS
        - Scope [10.17.50.0] Wireless_WGB_Clients
        - Scope [10.17.51.0] WGB_ clients_ext
        - Scope [10.17.250.0] Plantwide_clients
        - Scope [10.20.10.0] Wireless_Ring
        - Scope [10.20.11.0] Wireless_Star
        - Scope [10.20.70.0] Vlan AP mgmt Star
        - Scope [10.20.80.0] Vlan AP mgmt Ring

Scope Options

Available Options	Description
□ 040 NIS Domain Name	Name of Ne
□ 041 NIS Servers	Addresses o
□ 042 NTP Servers	Addresses o
☑ 043 Vendor Specific Info	Embedded v

Data entry

```
0000   00 F1 08 0A 0D 32 FB 0A   .ñ...2û.
0008   0D 32 FA                  .2ú
```

Windows edition: Windows Server 2008 R2 Standard

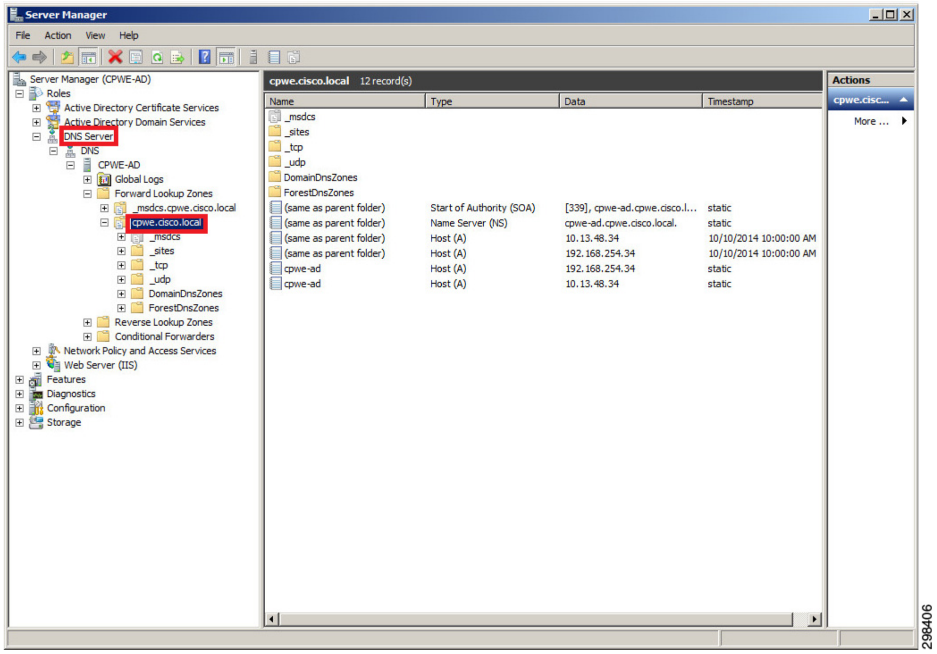
File
Action
View
Help
Address Pool
Address Leases
Reservations
Scope Options
Server Options
Filters
IPv6
DNS Server
File Services
Server Manager (AD)
Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.
Server Summary
Server Summary Help
Computer Information
Full Computer Name:
AD.cisco.local
Change System Properties
View Network Connections
Configure Remote Desktop
Configure Server Manager Remote Management
84897 (Activated)
General
Advanced
Data:
Binary:
ASCII:
OK
Cancel
Apply
System and S... System
Search Control Panel
View basic information about your computer
Copyright © 2009 Microsoft Corporation. All rights reserved.
Service Pack 1
System
Processor: Intel(R) Xeon(R) CPU X5550 @ 2.67GHz 2.67 GHz
Installed memory (RAM): 4.00 GB
System type: 64-bit Operating System
Pen and Touch: No Pen or Touch Input is available for this Display
See also
Action Center
Windows Update
Roles: 6 of 17 installed
Active Directory Certificate Services
Active Directory Domain Services
DHCP Server
DNS Server
File Services
Web Server (IIS)
Last Refresh: Today at 7:43 AM Configure refresh
Start
7:43 AM
10/14/2014
298405

DNS Server Setup

Step 1 Enable DNS service: Windows 2008 Server DNS service is located in *Start > Administrative Tools > Server Manager (CPWE-AD) > Roles*. Right-click *Roles* to select *Add Roles Wizard* to enable DNS service, and follow the instructions.

Step 2 Create DNS server: Once the DNS service is enabled, right-click on DNS server and select *Add Role Services* to create DNS server. Name it *CPWE-AD* or any other name preferred. Under this DNS server, create a new *forward lookup zone* such as *cpwe.cisco.local*. The completed setup is shown in Figure C-3.

Figure C-3 Central DNS Server Setup



cpwe.cisco.local 12 record(s)

Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[339], cpwe-ad.cpwe.cisco.l...	static
(same as parent folder)	Name Server (NS)	cpwe-ad.cpwe.cisco.local.	static
(same as parent folder)	Host (A)	10.13.48.34	10/10/2014 10:00:00 AM
(same as parent folder)	Host (A)	192.168.254.34	10/10/2014 10:00:00 AM
cpwe-ad	Host (A)	192.168.254.34	static
cpwe-ad	Host (A)	10.13.48.34	static

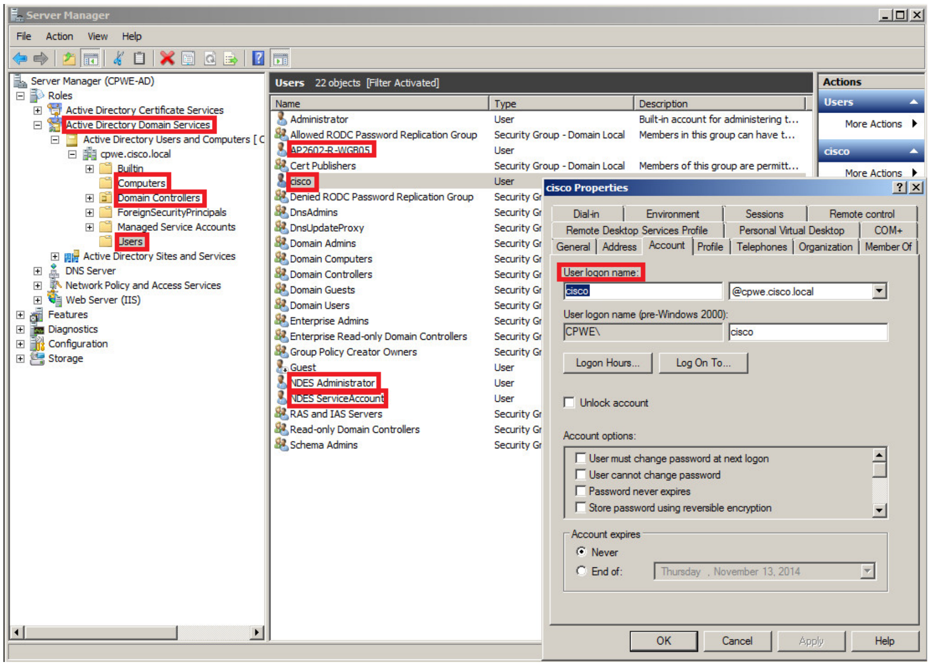
Active Directory Server Setup

Step 1 Enable Active Directory (AD) service: Windows 2008 Server Active Directory service is located in *Start > Administrative Tools > Server Manager (CPWE-AD) > Roles*. Right-click *Roles* to select *Add Roles Wizard* and enable Active Directory Domain Services, and then follow the instructions.

Step 2 Create AD server: Once AD service is enabled, right-click on AD server and select *Add Role Services* to create AD server and name it *CPWE-AD.cpwe.cisco.local* or any other name preferred.

Step 3 Add AD users: Right-click this AD server *Users* drop-down directory to add users in Users group (for example, *cisco*) with necessary information. Also, assign these users to the correct AD domain service with right privileges; repeat the same steps for users *NDES Administrator* and *NDES ServiceAccount* for Root-CA certification server, and any users needed for WGB clients (for example, *AP2602-R-WGB05*). Refer to Figure C-4 through Figure C-6 for more details.

Figure C-4 Central AD User Overview


Server Manager
File Action View Help
Server Manager (CPWE-AD)
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Users and Computers [C
cpwe.cisco.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Active Directory Sites and Services
DNS Server
Network Policy and Access Services
Web Server (IIS)
Features
Diagnostics
Configuration
Storage
Actions
Users
More Actions
cisco
More Actions
cisco Properties
Dial-in Environment Sessions Remote control
Remote Desktop Services Profile Personal Virtual Desktop COM+
General Address Account Profile Telephones Organization Member Of
Logon Hours... Log On To...
OK Cancel Apply Help
298407

Users 22 objects [Filter Activated]

Name	Type	Description
Administrator	User	Built-in account for administering t…
Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group can have t…
AP2602-R-WGB05	User	
Cert Publishers	Security Group - Domain Local	Members of this group are permitt…
cisco	User	
Denied RODC Password Replication Group	Security Gr	
DnsAdmins	Security Gr	
DnsUpdateProxy	Security Gr	
Domain Admins	Security Gr	
Domain Computers	Security Gr	
Domain Controllers	Security Gr	
Domain Guests	Security Gr	
Domain Users	Security Gr	
Enterprise Admins	Security Gr	
Enterprise Read-only Domain Controllers	Security Gr	
Group Policy Creator Owners	Security Gr	
Guest	User	
NDES Administrator	User	
NDES ServiceAccount	User	
RAS and IAS Servers	Security Gr	
Read-only Domain Controllers	Security Gr	
Schema Admins	Security Gr	

User logon name: cisco @cpwe.cisco.local

User logon name (pre-Windows 2000): CPWE\ cisco

□ Unlock account

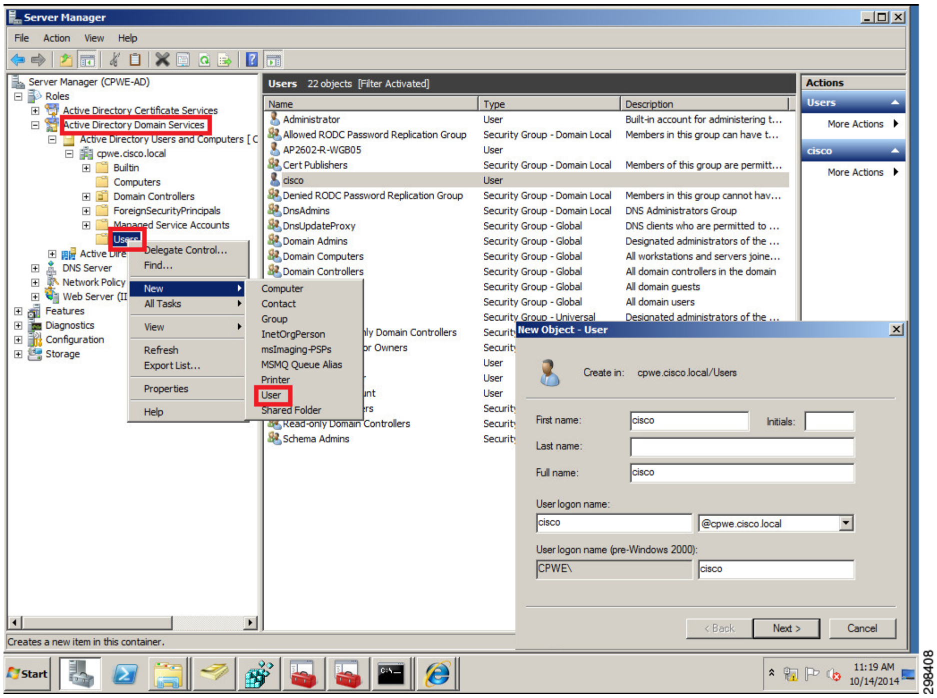
Account options:

- □ User must change password at next logon
- □ User cannot change password
- □ Password never expires
- □ Store password using reversible encryption

Account expires

- ● Never
- ○ End of: Thursday , November 13, 2014

Figure C-5 Central AD Server User Setup



Users 22 objects [Filter Activated]

Name	Type	Description
Administrator	User	Built-in account for administering t…
Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group can have t…
AP2602-R-WGB05	User	
Cert Publishers	Security Group - Domain Local	Members of this group are permitt…
cisco	User	
Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group cannot hav…
DnsAdmins	Security Group - Domain Local	DNS Administrators Group
DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to …
Domain Admins	Security Group - Global	Designated administrators of the …
Domain Computers	Security Group - Global	All workstations and servers joine…
Domain Controllers	Security Group - Global	All domain controllers in the domain
	Security Group - Global	All domain guests
	Security Group - Global	All domain users
	Security Group - Universal	Designated administrators of the …
ly Domain Controllers	Securit	
r Owners	Securit	
	User	
	User	
nt	User	
rs	Securit	
Read-only Domain Controllers	Securit	
Schema Admins	Securit	

Create in: cpwe.cisco.local/Users

First name: cisco Initials:

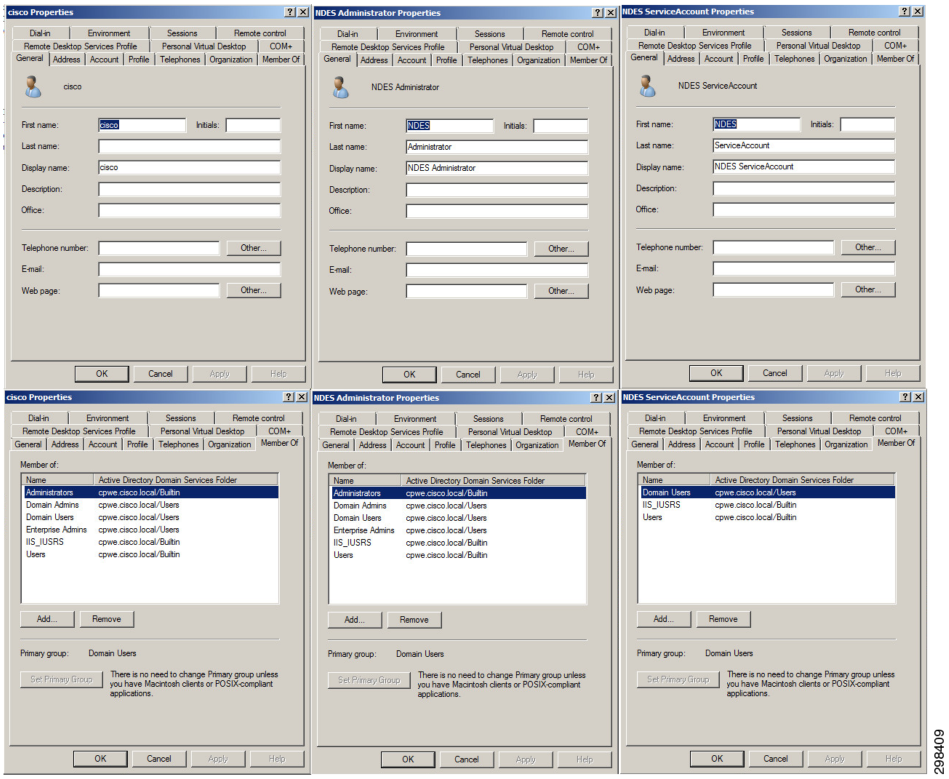
Last name:

Full name: cisco

User logon name: cisco @cpwe.cisco.local

User logon name (pre-Windows 2000): CPWE\ cisco

Figure C-6 Central AD Server Users Properties



cisco Properties

cisco

First name: cisco Initials:
Last name:
Display name: cisco
Description:
Office:
Telephone number:
E-mail:
Web page:

NDES Administrator Properties

NDES Administrator

First name: NDES Initials:
Last name: Administrator
Display name: NDES Administrator
Description:
Office:
Telephone number:
E-mail:
Web page:

NDES ServiceAccount Properties

NDES ServiceAccount

First name: NDES Initials:
Last name: ServiceAccount
Display name: NDES ServiceAccount
Description:
Office:
Telephone number:
E-mail:
Web page:

cisco Properties

Member of:

Name	Active Directory Domain Services Folder
Administrators	cpwe.cisco.local/Builtin
Domain Admins	cpwe.cisco.local/Users
Domain Users	cpwe.cisco.local/Users
Enterprise Admins	cpwe.cisco.local/Users
IIS_IUSRS	cpwe.cisco.local/Builtin
Users	cpwe.cisco.local/Builtin

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

NDES Administrator Properties

Member of:

Name	Active Directory Domain Services Folder
Administrators	cpwe.cisco.local/Builtin
Domain Admins	cpwe.cisco.local/Users
Domain Users	cpwe.cisco.local/Users
Enterprise Admins	cpwe.cisco.local/Users
IIS_IUSRS	cpwe.cisco.local/Builtin
Users	cpwe.cisco.local/Builtin

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

NDES ServiceAccount Properties

Member of:

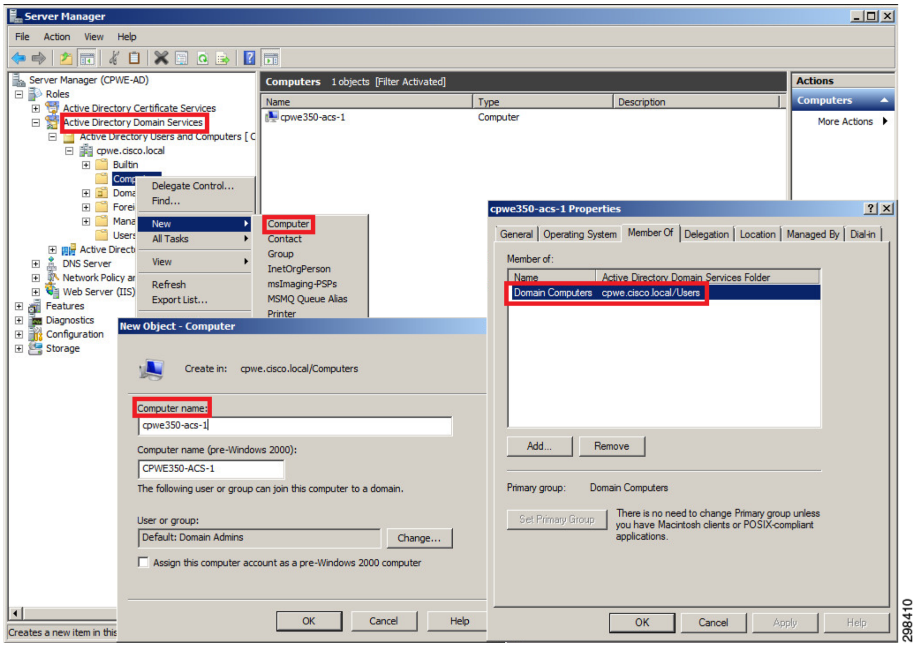
Name	Active Directory Domain Services Folder
Domain Users	cpwe.cisco.local/Users
IIS_IUSRS	cpwe.cisco.local/Builtin
Users	cpwe.cisco.local/Builtin

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Step 4 Configure server authentication: Right-click the AD server's *Computers* drop-down directory, adding any servers requiring authentication (for example, *cpwe350-acs-1*) in computer group, with necessary information as shown in Figure C-7. Assign the servers to the correct AD domain service with right privileges.

Figure C-7 Central AD Server Computers Properties



Computers 1 objects [Filter Activated]

Name	Type	Description
cpwe350-acs-1	Computer	

New Object - Computer

Create in: cpwe.cisco.local/Computers

Computer name: cpwe350-acs-1

Computer name (pre-Windows 2000): CPWE350-ACS-1

The following user or group can join this computer to a domain.

User or group: Default: Domain Admins — Change...

☐ Assign this computer account as a pre-Windows 2000 computer

cpwe350-acs-1 Properties

Member of:

Name	Active Directory Domain Services Folder
Domain Computers	cpwe.cisco.local/Users

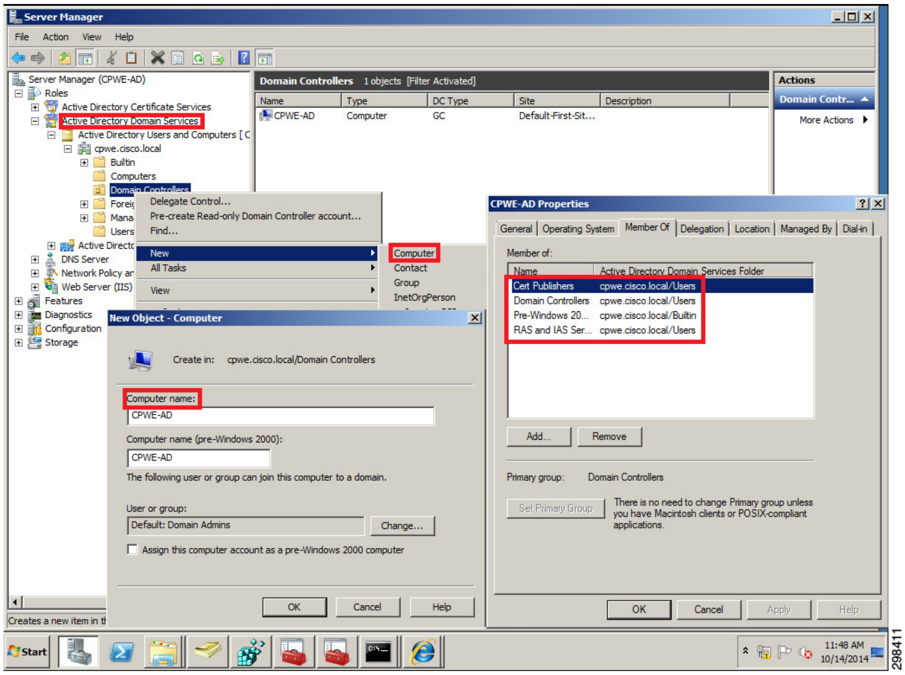
Primary group: Domain Computers

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

298410

Step 5 Configure domain controller: Right-click the AD server *Domain Controller* drop-down directory and add the AD server hostname (for example, *CPWE-AD*) as a domain controller, with necessary information as shown in Figure C-8, Assign this server to correct AD domain service with write privileges.

Figure C-8 Central AD Server Domain Controller Properties



Domain Controllers 1 objects [Filter Activated]

Name	Type	DC Type	Site	Description
CPWE-AD	Computer	GC	Default-First-Sit...	

New Object - Computer

Create in: cpwe.cisco.local/Domain Controllers

Computer name: CPWE-AD

Computer name (pre-Windows 2000): CPWE-AD

The following user or group can join this computer to a domain.

User or group: Default: Domain Admins — Change...

☐ Assign this computer account as a pre-Windows 2000 computer

CPWE-AD Properties

Member of:

Name	Active Directory Domain Services Folder
Cert Publishers	cpwe.cisco.local/Users
Domain Controllers	cpwe.cisco.local/Users
Pre-Windows 20...	cpwe.cisco.local/Builtin
RAS and IAS Ser...	cpwe.cisco.local/Users

Primary group: Domain Controllers

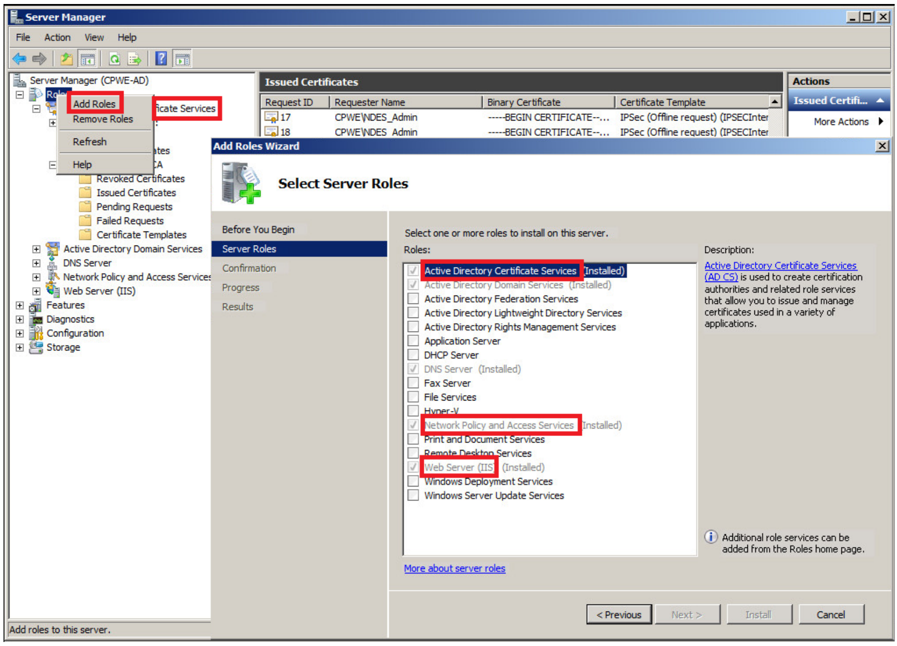
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

298411

Root-CA Server Setup

Step 1 Enable Root-CA service: Windows 2008 Server Class-3 Root-CA Server service is located in *Start > Administrative Tools > Server Manager (CPWE-AD) > Roles*. Right-click *Roles* to select *Add Roles Wizard* and to enable Root-CA certification authority service (as shown in Figure C-9 and follow the instructions.

Figure C-9 Root-CA Certificate Server Installations



Request ID	Requester Name	Binary Certificate	Certificate Template
17	CPWE\NDES_Admin	-----BEGIN CERTIFICATE--...	IPSec (Offline request) (IPSECInter
18	CPWE\NDES_Admin	-----BEGIN CERTIFICATE--...	IPSec (Offline request) (IPSECInter

Select one or more roles to install on this server.

Roles:

- ☑ Active Directory Certificate Services (Installed)
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- □ File Services
- □ Hyper-V
- ☑ Network Policy and Access Services (Installed)
- □ Print and Document Services
- □ Remote Desktop Services
- ☑ Web Server (IIS) (Installed)
- □ Windows Deployment Services
- □ Windows Server Update Services

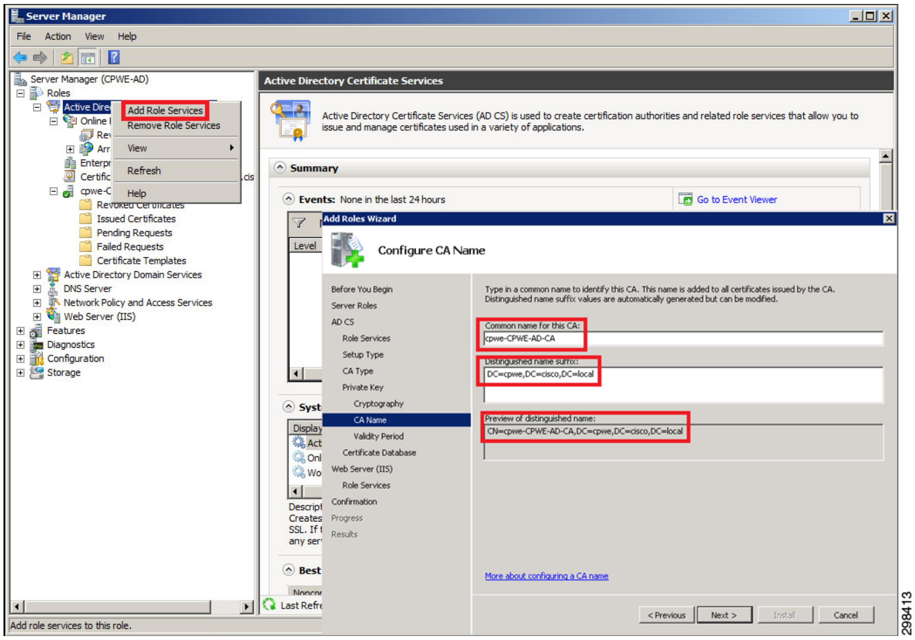
Description:

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Additional role services can be added from the Roles home page.

Step 2 Create Root-CA server and define X.509 parameters: Once Root-CA service is enabled, right-click *Root-CA server*. Right-click *Add Role Service*s to create Root-CA certificate authority server and name it *cpwe-CPWE-AD-CA* or any other name preferred. In the configuration wizard, fill in class 3 ROOT-CA X.509 V3 information (for example, CN=cpwe-CPWE-AD-CA, DC=cpwe, DC=cpwe, DC=cisco, DC=local meaning cpwe-CPWE-AD-CA.cpwe.cisco.local) as shown in Figure C-10

Figure C-10 Root-CA Certificate Authority Server Setup



Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Events: None in the last 24 hours

Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA: cpwe-CPWE-AD-CA

Distinguished name suffix: DC=cpwe,DC=cisco,DC=local

Preview of distinguished name: CN=cpwe-CPWE-AD-CA,DC=cpwe,DC=cisco,DC=local

Step 3 Set up manual certificate enrollment: Web Server (IIS) can provide manual "CerEnroll" and "CertSrv" certification manual enrollment service from certification authority GUI interface as shown in Figure C-11 and Figure C-12. Certification manual enrollment and installation can be preceded in Root-CA server itself (https://localhost/certsrv) or through network service IP (https://Root-CA-IP/certsrv) from remote site which is highlighted in Figure C-11

Figure C-11 Root-CA Web Server (IIS) Setup

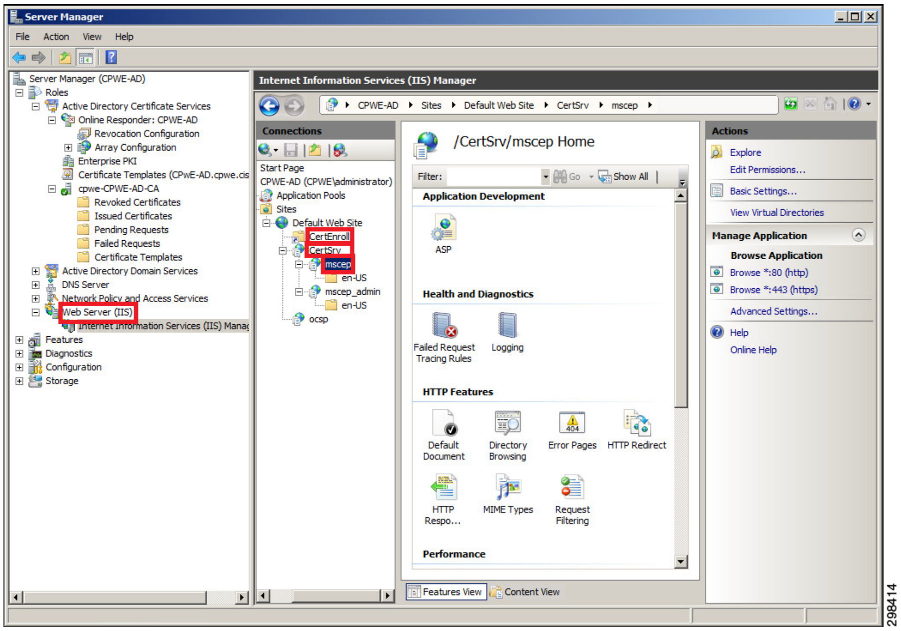
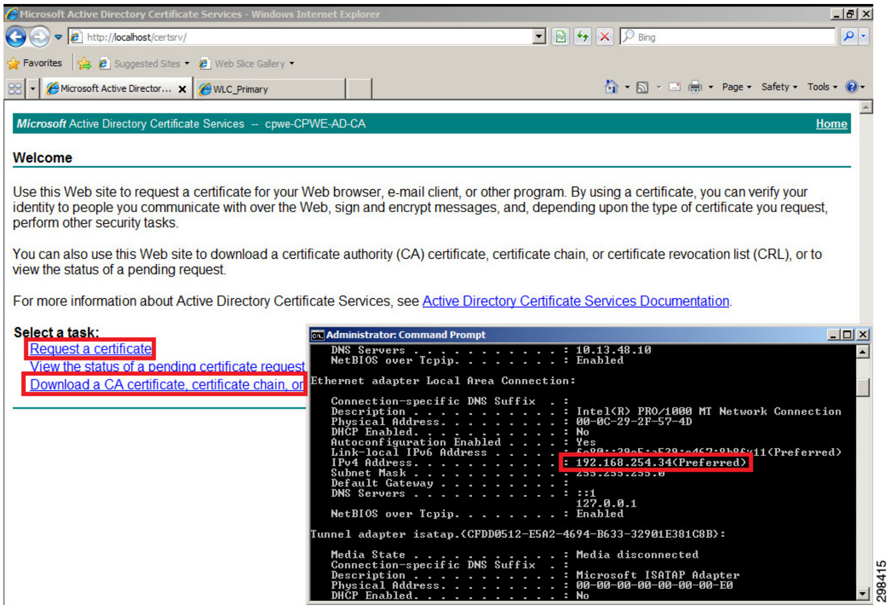


Figure C-12 Root-CA Web Server (IIS) Certification Manual Enrollment



Microsoft Active Directory Certificate Services - Windows Internet Explorer
http://localhost/certsrv/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Director...
WLC_Primary
Page
Safety
Tools
Administrator: Command Prompt
298415

Microsoft Active Directory Certificate Services -- cpwe-CPWE-AD-CA Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or

```
   DNS Servers . . . . . . . . . . . : 10.13.48.10
   NetBIOS over Tcpip. . . . . . . . : Enabled
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-2F-57-4D
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::38c5:a539:e467:8b8f%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.254.34(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DNS Servers . . . . . . . . . . . : ::1
                                       127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{CFDD0512-E5A2-4694-B633-32901E381C8B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
```

Step 4 Set up automated certificate enrollment (optional): A more scalable way for certification auto enrollment and management is through MSCEP Network Device Enrollment Services (NDES). NDES is the Microsoft implementation of the Simple Certificate Enrollment Protocol (SCEP). SCEP is an Internet-Draft standard developed by Cisco Systems and submitted to the Internet Engineering Task Force (IETF) that helps solve the problem of manually requesting and installing certificates by enabling devices to enroll for X.509 v3 certificates from any CA that supports SCEP. Distributing certificates to Windows® OSs from an Active Directory (AD) enterprise Certification Authority (CA) is relatively simple and can be automated using Group Policy Certificate Auto enrollment after a PKI is in place. To issue certificates to devices that don't have accounts in AD, system admins must manually create Public-Key Cryptography Standards (PKCS) requests and install certificates on those devices. This can be a time-consuming task in organizations that have hundreds of devices that aren't part of AD. Figure C-13 illustrates the Certificate enrollment process in details. Step 1 to Step 3 is the default behavior for MSCEP password challenge before NDES start certificate enrollment process. This step can be disabled through Windows 2008 server registry edit as shown in Figure C-14.

Figure C-13 Root-CA Network Device Certificate Enrollment Process

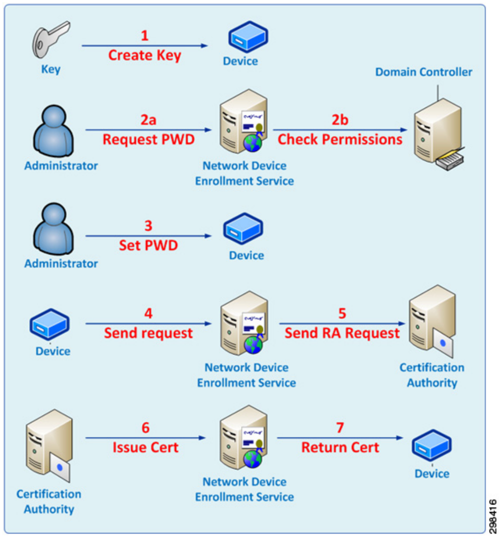
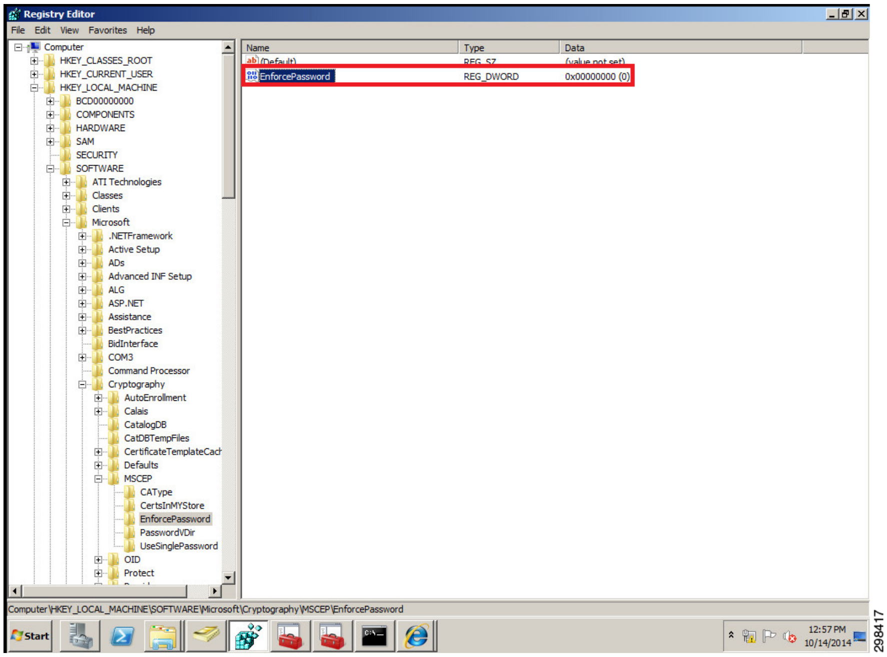


Figure C-14 Root-CA Disable NDES Password Challenge



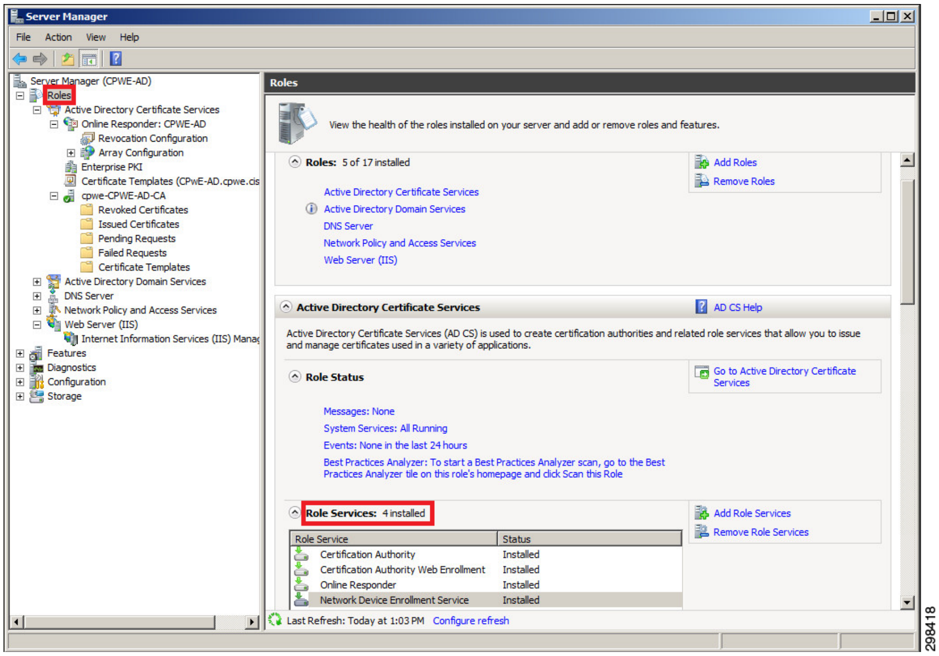
```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    BCD00000000
    COMPONENTS
    HARDWARE
    SAM
    SECURITY
    SOFTWARE
      ATI Technologies
      Classes
      Clients
      Microsoft
        .NETFramework
        Active Setup
        ADs
        Advanced INF Setup
        ALG
        ASP.NET
        Assistance
        BestPractices
        BidInterface
        COM3
        Command Processor
        Cryptography
          AutoEnrollment
          Calais
          CatalogDB
          CatDBTempFiles
          CertificateTemplateCach
          Defaults
          MSCEP
            CAType
            CertsInMYStore
            EnforcePassword
            PasswordVDir
            UseSinglePassword
          OID
          Protect
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
EnforcePassword	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

Step 5 Confirm that all services are running: The completed class-3 Root-CA certification server should include required role service as shown in Figure C-15: *Certification Authority, Certification Authority Web Enrollment*, *Online Responder* and *Network Device Enrollment Service*.

Figure C-15 Root-CA Certificate Server Role Services



View the health of the roles installed on your server and add or remove roles and features.

Roles: 5 of 17 installed

Active Directory Certificate Services
Active Directory Domain Services
DNS Server
Network Policy and Access Services
Web Server (IIS)

Active Directory Certificate Services

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Role Status

Messages: None
System Services: All Running
Events: None in the last 24 hours
Best Practices Analyzer: To start a Best Practices Analyzer scan, go to the Best Practices Analyzer tile on this role's homepage and click Scan this Role

Role Services: 4 installed

Role Service	Status
Certification Authority	Installed
Certification Authority Web Enrollment	Installed
Online Responder	Installed
Network Device Enrollment Service	Installed

Last Refresh: Today at 1:03 PM

RADIUS Server Setup

EAP-TLS is recommended as the security method for plant-wide device-to-device AAA service. EAP-TLS requires both RADIUS and certification services.

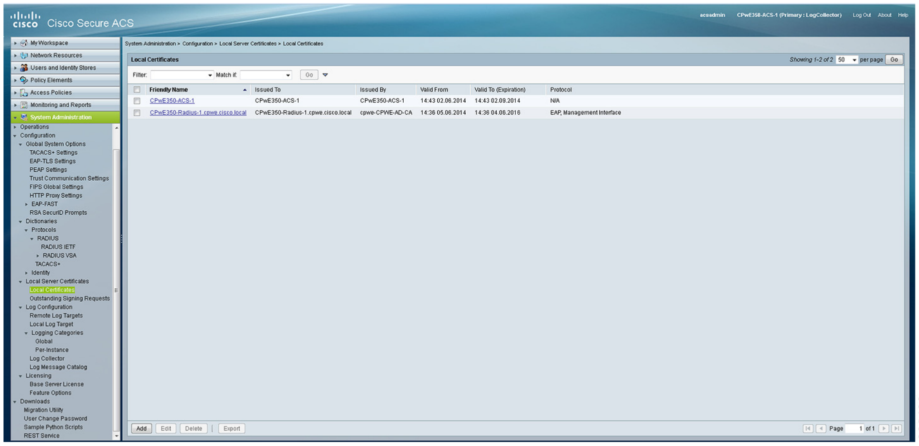
Cisco Access Control System (ACS) 5.5 was used as a dedicated RADIUS server for the CPwE WLAN. ACS 5.5 software runs on a dedicated Cisco 3415 / 3495 Security Access Control System Series Appliance, Cisco 1121 Security Access Control System Series Appliance, or a VMware virtual machine. CPwE WLAN choose VMware server as its AAA server. The ACS functionality can be further integrated into Cisco Identity Security Services (ISE) infrastructure which is not the part of this CVD.

Note For details about the installation and licensing process for Cisco ACS 5.5, refer to the following link:

- http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-5/installation/guide/csacs_book.html

Since ACS 5.5 is hosted on a separate machine from the Root-CA server, it requires a certificate from the Root-CA. Figure C-16 shows the ACS 5.5 certificate server setup.

Figure C-16 ACS 5.5 Certificate Setup



Showing 1-2 of 2 50 per page

□	Friendly Name	Issued To	Issued By	Valid From	Valid To (Expiration)	Protocol
□	CPwE350-ACS-1	CPwE350-ACS-1	CPwE350-ACS-1	14:43 02.06.2014	14:43 02.09.2014	N/A
□	CPwE350-Radius-1.cpwe.cisco.local	CPwE350-Radius-1.cpwe.cisco.local	cpwe-CPWE-AD-CA	14:36 05.06.2014	14:36 04.06.2016	EAP, Management Interface

Page 1 of 1

298420

APPENDIX D

Packet Rate Calculation Examples

The two examples below show how to quickly estimate the packet rate for the application using one of the common topologies (Fixed PAC to Wireless I/O and Fixed PAC to Wireless PAC). These results should be verified by looking at the actual packet rate from the switch, AP, or WGB statistics.

Example 1: Fixed PAC to Wireless I/O Packet Rate

In this example, a fixed safety PAC communicates to 6 wireless I/O chassis with digital, safety and analog modules. In addition, there are FactoryTalk ME stations (one per each wireless machine) and one PC running Studio 5000 online with trends. See Table D-1.

Table D-1 Fixed PAC to Wireless I/O Parameters

System Parameter / Size	Value
Number of I/O chassis (Rack Optimized)	6
Input safety modules (Input Data only)	6
Output safety modules	6
Analog modules	12
Safety Task scan rate	40 ms
Rack Optimized RPI	20 ms
Safety input RPI	20 ms
Analog RPI	100 ms
FTView ME stations	6
HMI tags (numeric / string)	100 / 10
HMI scan rate	500 ms

Using the above parameters, the application packet rate can be estimated as shown in Table D-2.

Table D-2 I/O Packet Rates

Data Type	Packet Rate
Standard I/O (rack optimized)	6 x 2 x 50 = 600
Safety input	12 x 50 = 600
Safety output	6 x 25 = 150
Analog I/O	12 x 2 x 10 = 240

Table D-2 I/O Packet Rates (continued)

Data Type	Packet Rate
Total I/O rate	1,590 pps
HMI tags (from IAB data)	6 x 18 = 108
Studio 5000 online with trends (from switch port statistics)	50
Total Rate (I/O + Class 3)	1.748 pps

This example shows that the estimated packet rate is below the recommended maximum of 2,200 pps. The remaining bandwidth can be reserved for the maintenance traffic such as Studio 5000 upload / download or device management via HTTP.

Example 2: Fixed PAC to Wireless PAC Packet Rate

In this example, a fixed safety PAC communicates to 10 wireless safety PAC using standard and safety Produced/Consumed tags. The fixed PAC produces two standard and one safety tag to all wireless PACs, and consumes one standard and one safety tag from each wireless PAC. There are also FactoryTalk SE clients (one per each wireless machine). See Table D-3.

Table D-3 Fixed PAC to Wireless PAC Parameters

System Parameter / Size	Value
Number of Wireless PACs	10
Standard P/C tags (Fixed to Wireless)	20
Standard P/C tags (Wireless to Fixed)	10
Safety P/C tags (both directions)	20
Standard P/C RPI (Fixed to Wireless)	20 ms
Standard P/C RPI (Wireless to Fixed)	50 ms
Safety P/C RPI	40 ms
FTView SE stations	10

Using the above parameters, the application packet rate can be estimated as shown in Table D-4.

Table D-4 P/C Packet Rate

Data Type	Packet Rate
Standard P/C	20 x 50 + 10 x 20 = 1200
Safety P/C	20 x 25 = 500
Total P/C rate	1,700 pps
FTView SE traffic (from switch port statistics)	25 x 10 = 250
Total rate (P/C + Class 3)	1,950 pps

The total rate is still below the recommended limit. However, by combining two produced tags into one, the packet rate can be reduced by 500 pps. The lower packet rate is always preferred for better performance in the channel.

For PAC to PAC communication, the Connection Type for remote Ethernet modules should be configured as None. The default setting of *Rack Optimization* would create an extra connection per module in each direction that is not necessary (no remote I/O modules). In the above example, the extra packet rate would be 20 x 50 = 1000 pps (with default RPI of 20 ms). The total rate would be beyond the limit.

APPENDIX E

Test Hardware and Software

The hardware and software components listed in Table E-1 were used in the Autonomous and Unified Architecture testing.

Table E-1 Test Hardware and Software

Role	Product	SW Version	Notes
Autonomous AP	Stratix 5100	15.2(4)JAZ	Autonomous testing only
Lightweight AP	Aironet 3602E	15.2(4)JB4	Unified testing only
Workgroup Bridge (WGB)	Aironet 2602E, Stratix 5100	15.2(4)JAZ	
Wireless LAN Controller (WLC)	Cisco 5508	7.6.110.0	Unified testing only
Access switch	Cisco IE 2000, Stratix 5700	15.2(1)EY, 15.2(1)EY1	With PoE
Access switch	Cisco IE 3000, Stratix 8000	15.2(1)EY, 15.2(1)EY1	With PoE
Distribution switch	Catalyst 3750-X	15.0(2)SE5, 15.0(2)SE6	Switch stack
Core switch	Catalyst 6500	15.1(2)SY1	Unified testing only
GuardLogix Safety PAC	1756-L73S	21.011	
GuardLogix Safety Partner processor	1756-L7SP	21.011	
ControlLogix PAC	1756-L75	21.011	
ControlLogix 2-port EtherNet/IP module	1756-EN2TR	5.028	
ControlLogix Fast Input Module	1756-IB16IF	1.01	
ControlLogix Fast Output Module	1756-OB16IEF	1.012	
POINT I/O 2-Port EtherNet/IP Module	1734-AENTR	4.003, 3.012	
POINT Digital input module	1734-IB8	3.022	
POINT Digital output module	1734-OB8	3.022	
POINT Digital safety input module	1734-IB8S	1.022, 3.01.02	
POINT Digital safety output module	1734-OB8S	1.022, 3.01.02	
PanelView Plus 6	2711P-T6C20D8	7.00	Autonomous testing only

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. For ongoing news, please go to 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

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.

Rockwell Automation is a leading provider of power, control and information solutions that enable customers to get products to market faster, reduce their total cost of ownership, better utilize plant assets, and minimize risks in their manufacturing environments.

www.rockwellautomation.com

Americas:
Rockwell Automation
1201 South Second Street
Milwaukee, WI 53204-2496 USA
Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

Asia Pacific:
Rockwell Automation
Level 14, Core F, Cyberport 3
100 Cyberport Road, Hong Kong
Tel: (852) 2887 4788, Fax: (852) 2508 1846

Europe/Middle East/Africa:
Rockwell Automation
NV, Pegasus Park, De Kleetlaan 12a
1831 Diegem, Belgium
Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

Publication ENET-TD006A-EN-P 11/2014
Updated: November 11, 2014