Enterprise Mobility 4.1 Design Guide

Cisco Validated Design I

Revised: April 13, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number:
Text Part Number: OL-14435-01

Cisco Validated Design

The Cisco Validated Design Program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit www.cisco.com/go/validateddesigns.

Enterprise Mobility 4.1 Design Guide

CONTENTS

Preface

Document Purpose

The purpose of this document is to describe the design and implementation of the Cisco Unified Wireless Network solution for the enterprise, using the features incorporated in the Wireless LAN Controller software Release 4.1.

Intended Audience

This publication is for experienced network administrators who are responsible for design and implementation of wireless networks.

Document Organization

The following table lists and briefly describes the chapters of this guide.

Section	Description
Chapter 1, "Cisco Unified Wireless Network Solution Overview."	Summarizes the benefits and characteristics of the Cisco Unified Wireless Network for the enterprise.
Chapter 2, "Cisco Unified Wireless Technology and Architecture."	Discusses the key design and operational considerations in an enterprise Cisco Unified Wireless Deployment.
Chapter 3, "WLAN Radio Frequency Design Considerations."	Describes the basic radio frequency (RF) information necessary to understand RF considerations in various wireless local area network (WLAN) environments.
Chapter 4, "Cisco Unified Wireless Network Architecture—Base Security Features."	Describes the natively available 802.11 security options and the advanced security features in the Cisco Unified Wireless solution, and how these can be combined to create an optimal WLAN solution.
Chapter 5, "Cisco Unified Wireless QoS."	Describes quality-of-service (QoS) in the context of WLAN implementations.

Section	Description
Chapter 6, "Cisco Unified Wireless Multicast Design."	Describes the improvements that have been made in IP multicast forwarding and provides information on how to deploy multicast in a wireless environment.
Chapter 7, "Cisco Unified Wireless Hybrid REAP."	Describes the Cisco Centralized WLAN architecture and its use of H-REAP.
Chapter 8, "Cisco Wireless Mesh Networking."	Describes the use of wireless mesh.
Chapter 9, "VoWLAN Design Recommendations."	Provide design considerations when deploying voice over WLAN (VoWLAN) solutions.
Chapter 10, "Cisco Unified Wireless Guest Access Services."	Describes the use of guest access services in the centralized WLAN architecture.
Chapter 11, "Mobile Access Router, Universal Bridge Client, and Cisco Unified Wireless."	Describes the use of the mobile access router, universal bridge client, and mesh networks.
Chapter 12, "Cisco Unified Wireless and Mobile IP."	Describes the inter-workings of the Cisco Mobile Client (CMC) over a Cisco Unified Wireless Network (WiSM).
Chapter 13, "Cisco Unified Wireless Location-Based Services."	Discusses the Cisco Location-Based Service (LBS) solution and the areas that merit special consideration involving design, configuration, installation, and deployment.
Glossary	Lists and defines key terms used in the guide.

CHAPTER 1

Cisco Unified Wireless Network Solution Overview

This chapter summarizes the benefits and characteristics of the Cisco Unified Wireless Network for the enterprise.The Cisco Unified Wireless Network solution offers secure, scalable, cost-effective wireless LANs for business critical mobility.The Cisco Unified Wireless Network is the industry's only unified wired and wireless solution to cost-effectively address the wireless LAN (WLAN) security, deployment, management, and control issues facing enterprises. This powerful indoor and outdoor solution combines the best elements of wired and wireless networking to deliver high performance, manageable, and secure WLANs with a low total cost of ownership.

WLAN Introduction

The mobile user requires the same accessibility, security, quality-of-service (QoS), and high availability currently enjoyed by wired users. Whether you are at work, at home, on the road, locally or internationally, there is a need to connect. The technological challenges are apparent, but to this end, mobility plays a role for everyone. Companies are deriving business value from mobile and wireless solutions. What was once a vertical market technology is now mainstream, and is an essential tool in getting access to voice, real-time information, and critical applications such as e-mail and calendar, enterprise databases, supply chain management, sales force automation, and customer relationship management.

WLAN Solution Benefits

WLANs provide the user with a new way to communicate while accommodating the way business is done now. The following benefits are achieved by WLANs:

- *Mobility within building or campus*—Facilitates implementation of applications that require an always-on network and that tend to involve movement within a campus environment.
- *Convenience*—Simplifies networking of large, open people areas.
- *Flexibility*—Allows work to be done at the most appropriate or convenient place rather than where a cable drop terminates. Getting the work done is what is important, not where you are.
- *Easier to set-up temporary spaces*—Promotes quick network setup of meeting rooms, war rooms, or brainstorming rooms tailored to variations in the number of participants.
- *Lower cabling costs*—Reduces the requirement for contingency cable plant installation because the WLAN can be employed to fill the gaps.

- *Easier adds, moves, and changes and lower support and maintenance costs*—Temporary networks become much easier to set up, easing migration issues and costly last-minute fixes.
- *Improved efficiency*—Studies show WLAN users are connected to the network 15 percent longer per day than hard-wired users.
- *Productivity gains*—Promotes easier access to network connectivity, resulting in better use of business productivity tools. Productivity studies show a 22 percent increase for WLAN users.
- *Easier to collaborate*—Facilitates access to collaboration tools from any location, such as meeting rooms; files can be shared on the spot and requests for information handled immediately.
- *More efficient use of office space*—Allows greater flexibility for accommodating groups, such as large team meetings.
- *Reduced errors*—Data can be directly entered into systems as it is being collected, rather than when network access is available.
- *Improved efficiency, performance, and security for enterprise partners and guests*—Promoted by implementing guest access networks.
- *Improved business resilience*—Increased mobility of the workforce allows rapid redeployment to other locations with WLANs.

Requirements of WLAN Systems

WLAN systems run either as an adjunct to the existing wired enterprise network or as a free-standing network within a campus or branch, individual teleworker, or tied to applications in the retail, manufacturing, or healthcare industries. WLANs must permit secure, encrypted, authorized communication with access to data, communication, and business services as if connected to the resources by wire.

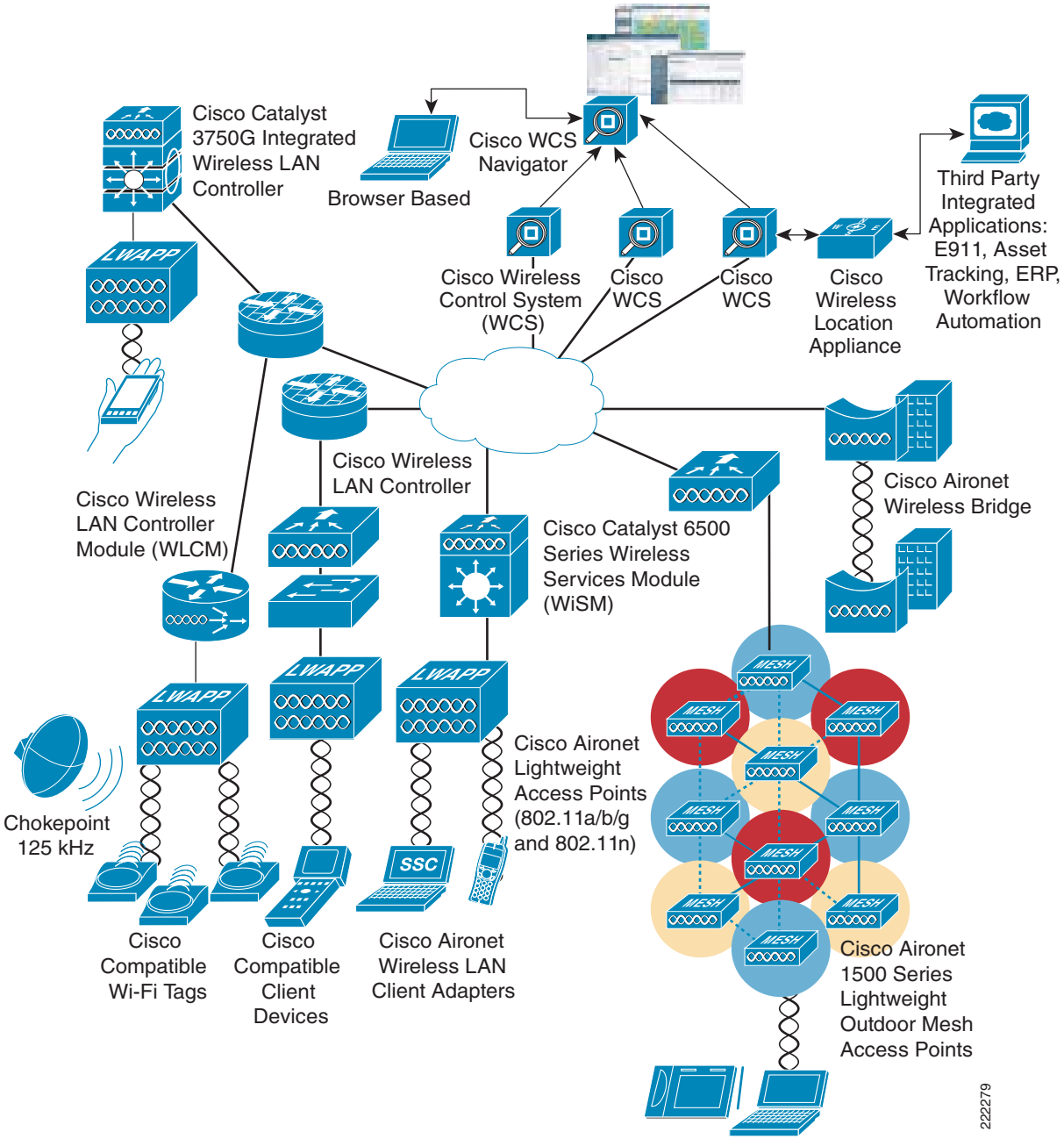
WLANs must be able to do the following:

- *Maintain accessibility to resources while employees are not wired to the network*—This accessibility enables employees to respond more quickly to business needs regardless of whether they are meeting in a conference room with a customer, at lunch with coworkers in the company cafeteria, or collaborating with a teammate in the next building.
- *Secure the enterprise from unauthorized, unsecured, or "rogue" WLAN access points*—IT managers must be able to easily and automatically detect and locate rogue access points and the switch ports to which they are connected, active participation of both access points, and client devices that are providing continuous scanning and monitoring of the RF environment.
- *Extend the full benefits of integrated network services to nomadic users*—IP telephony and IP video-conferencing are supported over the WLAN using QoS, which by giving preferential treatment to real-time traffic, helps ensure that the video and audio information arrives on time. Firewall and Intruder Detection that are part of the enterprise framework are extended to the wireless user.
- *Segment authorized users and block unauthorized users*—Services of the wireless network can be safely extended to guests and vendors. The WLAN must be able to configure support for a separate public network—a guest network.
- *Provide easy, secure network access to visiting employees from other sites*—There is no need to search for an empty cubicle or an available Ethernet port. Users should securely access the network from any WLAN location. Employees are authenticated through IEEE 802.1x and Extensible Authentication Protocol (EAP), and all information sent and received on the WLAN is encrypted.

- *Easily manage central or remote access points*—Network managers must be able to easily deploy, operate, and manage hundreds to thousands of access points within the WLAN campus deployments and branch offices or retail, manufacturing, and health care locations. The desired result is one framework that provides medium-sized to large organizations the same level of security, scalability, reliability, ease of deployment, and management that they have come to expect from their wired LANs.
- *Enhanced Security Services*—WLAN Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) control to contain wireless threats, enforce security policy compliance, and safeguard information.
- *Voice Services*—Brings the mobility and flexibility of wireless networking to voice communications via the Cisco Unified Wired and Wireless network and the Cisco Compatible Extensions voice-enabled client devices.
- *Location Services* — Simultaneous tracking of hundreds to thousands of Wi-Fi and active RFID devices from directly within the WLAN infrastructure for critical applications such as high-value asset tracking, IT management, location-based security, and business policy enforcement.
- *Guest Access*— Provides customers, vendors, and partners with easy access to a wired and wireless LANs, helps increase productivity, facilitates real-time collaboration, keeps the company competitive, and maintains full WLAN security.

WLANs in the enterprise have emerged as one of the most effective means for connecting to a network. Figure 1-1 shows the elements of the Cisco Unified Wireless Network.

Figure 1-1 Cisco Unified Wireless Network Architecture in the Enterprise



The following five interconnected elements work together to deliver a unified enterprise-class wireless solution:

- Client devices
- Access points
- Network unification
- World-class network management
- Mobility services

Beginning with a base of client devices, each element adds capabilities as the network needs evolve and grow, interconnecting with the elements above and below it to create a comprehensive, secure WLAN solution.

The Cisco Unified Wireless Network cost-effectively addresses the WLAN security, deployment, management, and control issues facing enterprises. This framework integrates and extends wired and wireless networks to deliver scalable, manageable, and secure WLANs with the lowest total cost of ownership. The Cisco Unified Wireless Network provides the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations expect from their wired LANs.

For more information about the Cisco Unified Wireless Network, see the following URL: http://www.cisco.com/go/unifiedwireless

Cisco Unified Wireless Network

The core feature set of the Cisco Unified Wireless Network includes Cisco Aironet access points (APs), the Wireless Control System (WCS), and Wireless LAN Controllers (WLC), including the Cisco Catalyst 6500 Wireless Services Module (WiSM), the 440X, the 2106 WLC, the WLCM ISR module, and the WS-C3750G integrated controller.

The core feature set is currently deployable in the following configurations:

- APs and WLC
- APs, WLCs, and WCS
- APs, WLC, WCS, and LBS

Adding optional Cisco Compatible Extensions client devices and the Cisco Secure Services Client provides additional benefits, including advanced enterprise-class security, extended RF management, and enhanced interoperability.

CHAPTER 2

Cisco Unified Wireless Technology and Architecture

This chapter discusses the key design and operational considerations associated with an enterprise Cisco Unified Wireless deployment.

This chapter examines the following:

- LWAPP
- Roaming
- Broadcast and multicast handling
- Product choices
- Deployment considerations

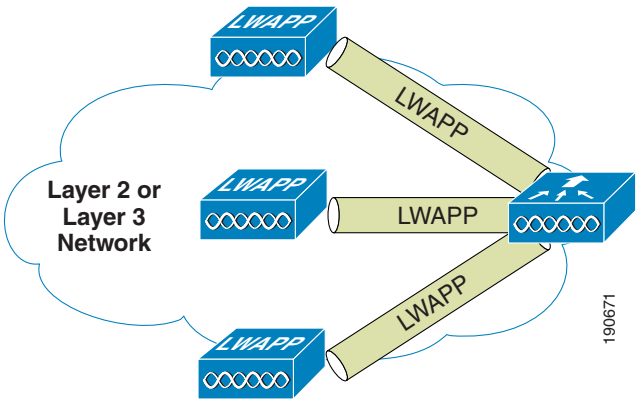
Much of the material in this chapter is explained in more detail in later chapters of the document. Recommended reading for more detail on the Cisco Unified Wireless Technology is *Deploying Cisco 440X Series Wireless LAN Controllers* at the following URL: http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html.

LWAPP Overview

Lightweight Access Point Protocol (LWAPP) is the underlying protocol used in Cisco's centralized WLAN architecture. It provides for the configuration and management of WLAN(s), in addition to tunneling WLAN client traffic to and from a centralized WLAN controller (WLC). Figure 2-1 shows a high level diagram of a basic centralized WLAN architecture, where LWAPP APs connect to a WLC via LWAPP.

Note Because the foundational WLAN features are the same, the term WLC is used generically to represent all Cisco WLAN Controllers, regardless of whether the controller is a standalone appliance, an ISR with a WLC module; or a Catalyst switch with a service module or integrated WLC.

Figure 2-1 LWAPP APs Connected to a WLC



The LWAPP protocol comprises of a number of functional components; however, only those that influence the design and operation of a centralized WLAN network are discussed in this document.

The key features of LWAPP are:

- Split MAC tunnel
- L2 or L3 based tunnels
- WLC discovery process.

Split MAC

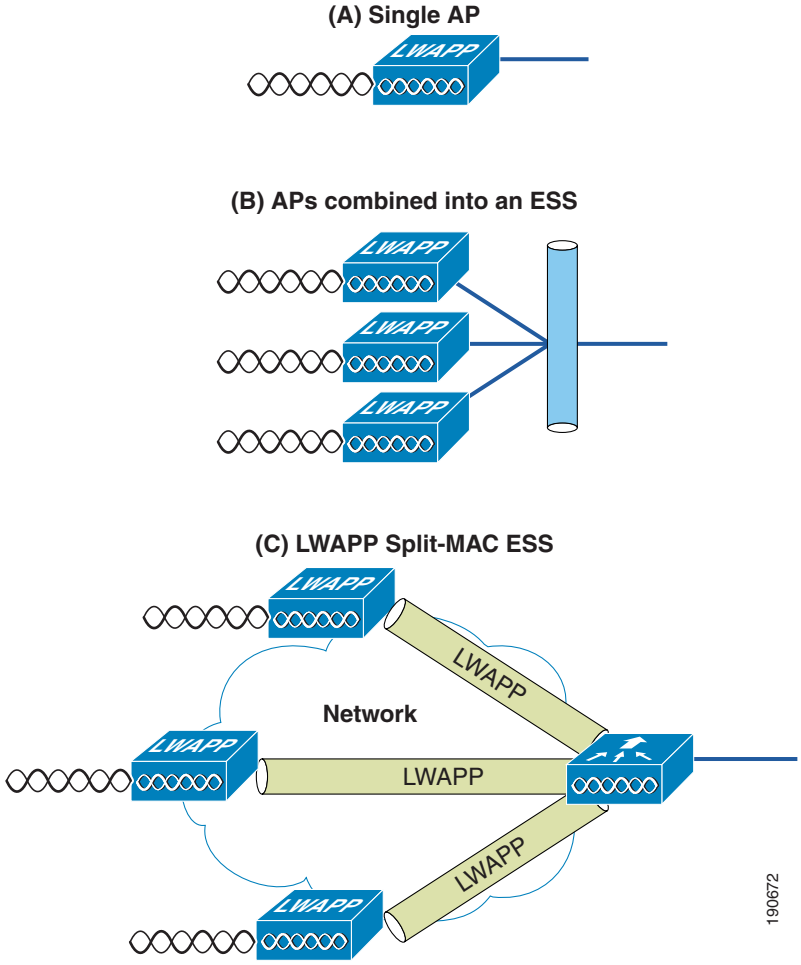
A key component of the LWAPP protocol is the concept of split MAC, where part of the 802.11 protocol operation is managed by the LWAPP AP, while the remaining parts are managed by the WLC. A diagram of the split MAC concept is shown in Figure 2-2c.

A generic 802.11 AP, at the simplest level, is nothing more than an 802.11 MAC-layer radio that bridges WLAN clients to a wired network based on association to a Basic Service Set Identifier (BSSID). See Figure 2-2a. The 802.11 standard extends the single AP concept (above) to allow multiple APs to provide an extended service set (ESS), where multiple APs use the same ESS identifier (ESSID, commonly referred to as an SSID) to allow a WLAN client to connect to a common network via more than one AP. See Figure 2-2b.

The LWAPP split MAC concept takes all of the functions normally performed by individual APs and distributes them between two functional components: an LWAPP AP and a WLC. The two are linked across a network by the LWAPP protocol and together provide equivalent radio/bridging services in a manner that is simpler to deploy and manage than individual APs.

Note Although ‘split MAC’ facilitates Layer 2 connectivity between the WLAN clients and the wired interface of the WLC; this does not mean that the LWAPP tunnel will pass all traffic. The WLC forwards only IP Ethertype frames, and its default behavior is to not forward broadcast and multicast traffic. This is important to keep in mind when considering multicast and broadcast requirements in a WLAN deployment.

Figure 2-2 Split MAC Concept



The simple timing-dependent operations are generally managed locally on the LWAPP AP, while more complex, less time-dependent operations are managed on the WLC.

For example, the LWAPP AP handles the following:

- Frame exchange handshake between a client and AP
- Transmission of beacon frames
- Buffering and transmission of frames for clients in power save mode
- Response to probe request frames from clients; the probe requests are also sent to the WLC for processing
- Forwarding notification of received probe requests to the WLC
- Provision of real-time signal quality information to the switch with every received frame
- Monitoring each of the radio channels for noise, interference, and other WLANs
- Monitoring for the presence of other APs
- Encryption and decryption of 802.11 frames

Other functionality is handled by the WLC. Some of the MAC-layer functions provided by the WLC include the following:

- 802.11 authentication
- 802.11 association and reassociation (mobility)
- 802.11 frame translation and bridging
- 802.1X/EAP/RADIUS processing
- Termination of 802.11 traffic on a wired interface, except in the case of REAP and H-REAP configured APs, which are discussed later in this guide

An LWAPP tunnel supports two categories of traffic:

- LWAPP control messages—Used to convey control, configuration, and management information between the WLC and APs.
- Wireless client data encapsulation—Transports Layer 2 wireless client traffic in IP Ethertype encapsulated packets from the AP to the WLC.

When encapsulated client traffic reaches the WLC, it is mapped to a corresponding VLAN interface/port at the WLC. This interface mapping is defined as part of a WLAN's configuration settings on the WLC. The interface mapping is usually static, but a WLAN client can be dynamically mapped to a specific VLAN based on parameters sent by an upstream AAA server upon successful EAP authentication. In addition to the VLAN assignment, other WLAN configuration parameters include: SSID, operational state; authentication and security method; and QoS.

Layer 2 and Layer 3 Tunnels

LWAPP allows tunneling within Ethernet frames (Layer 2) or within UDP packets (Layer 3). This is configurable on the WLC. Only one method can be supported at a time and not all WLCs support the Layer 2 method.

Layer 2 Tunnel

When deploying Layer 2 LWAPP, the WLC and the LWAPP APs require IP addresses even though the LWAPP tunnel uses Ethertype 0xBBBB to encapsulate traffic between them. All communication between the LWAPP AP and the WLC is encapsulated using Ethertype 0xBBBB.

Although Layer 2 LWAPP is one of the simplest ways to establish AP connectivity and configuration, it is generally not recommended for enterprise deployments, and therefore will not be discussed further in this document.

The primary reasons why the Layer 2 method is not a current Cisco best practice recommendation:

- Layer 2 connectivity between the LWAPP APs and the WLC potentially limits the location of where the APs or WLC can be positioned within the overall network. Extending Layer 2 transport across an enterprise network to get around this limitation is not a current Cisco best practice recommendation.
- Layer 2 LWAPP is not supported on all LWAPP APs and WLC platforms.
- Even though client traffic DSCP values are preserved within the tunnel, Layer 2 LWAPP does not provide corresponding CoS marking for the Ethertype frames, and therefore is not able to provide transparent, end-to-end QoS for the tunneled traffic.

Layer 3 Tunnel

Layer 3 LWAPP is the recommended tunnel type. This method uses IP UDP packets to facilitate communication between the LWAPP AP, and the WLC. L3 LWAPP is able to perform fragmentation and reassembly of tunnel packets; thereby allowing client traffic to make use of a full 1500 byte MTU and not have to adjust for any tunnel overhead.

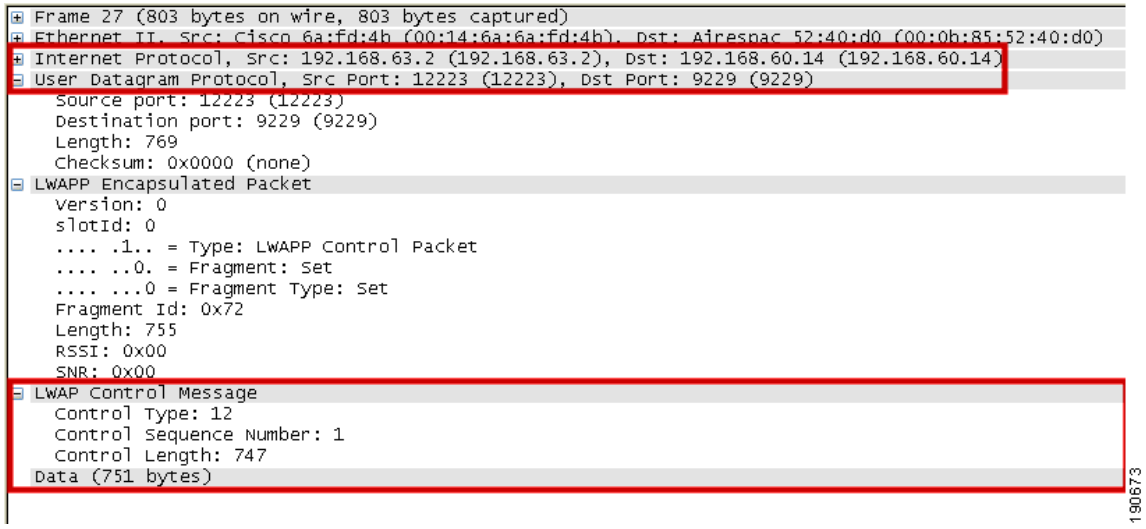
Note In order to optimize the fragmentation and reassembly process, the number of fragments that the WLC or AP expect to receive is limited. The ideal supported MTU size for deploying the Cisco Unified Wireless network is 1500, but the solution operates successfully over networks where the MTU is as small as 500 bytes.

The following are some Layer 3 LWAPP packet captures to illustrate LWAPP operation. The sample decodes were captured using a Wireshark Network Analyzer.

Note The Wireshark's default configuration does not decode Cisco LWAPP packets correctly. This can be corrected by using the "SWAP Frame Control" option under protocol preferences.

Figure 2-3 shows a decode of an LWAPP control packet. This packet originates from the WLC using UDP source port 12223 (as do all LWAPP control packets from the WLC). Control Type 12 represents a configuration command used to pass AP configuration information to the LWAPP AP by the WLC. Control packet payloads are AES encrypted, using keys derived from the PKI authentication process that is performed when an LWAPP AP first establishes a connection with the WLC.

Figure 2-3 LWAPP Control Packet



802.11 Probe Request in LWAPP shows a decode of an LWAPP packet containing an 802.11 probe request. This packet originates from the LWAPP AP to the WLC using UDP port 12222, as do all LWAPP-encapsulated 802.11 frames. In this example, RSSI and SNR values are also included in the LWAPP packet to provide RF information to the WLC.

Figure 2-4 802.11 Probe Request in LWAPP

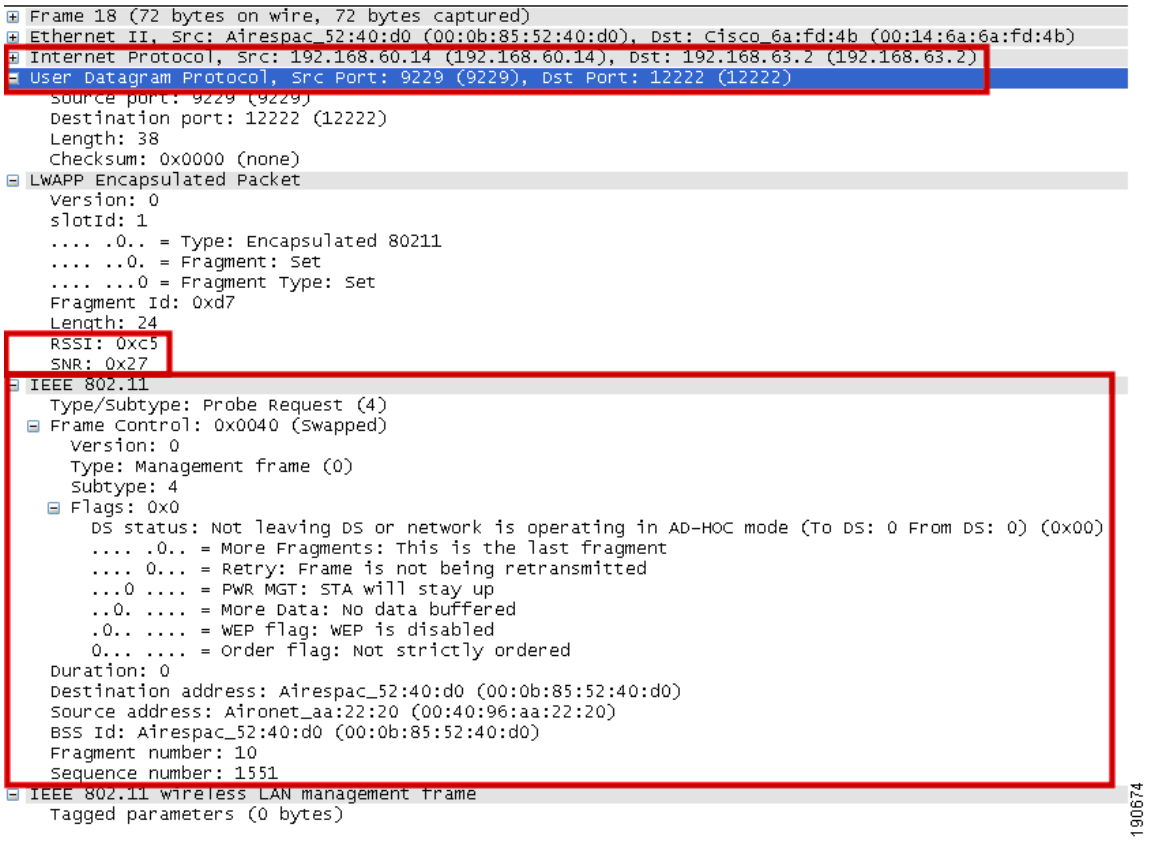
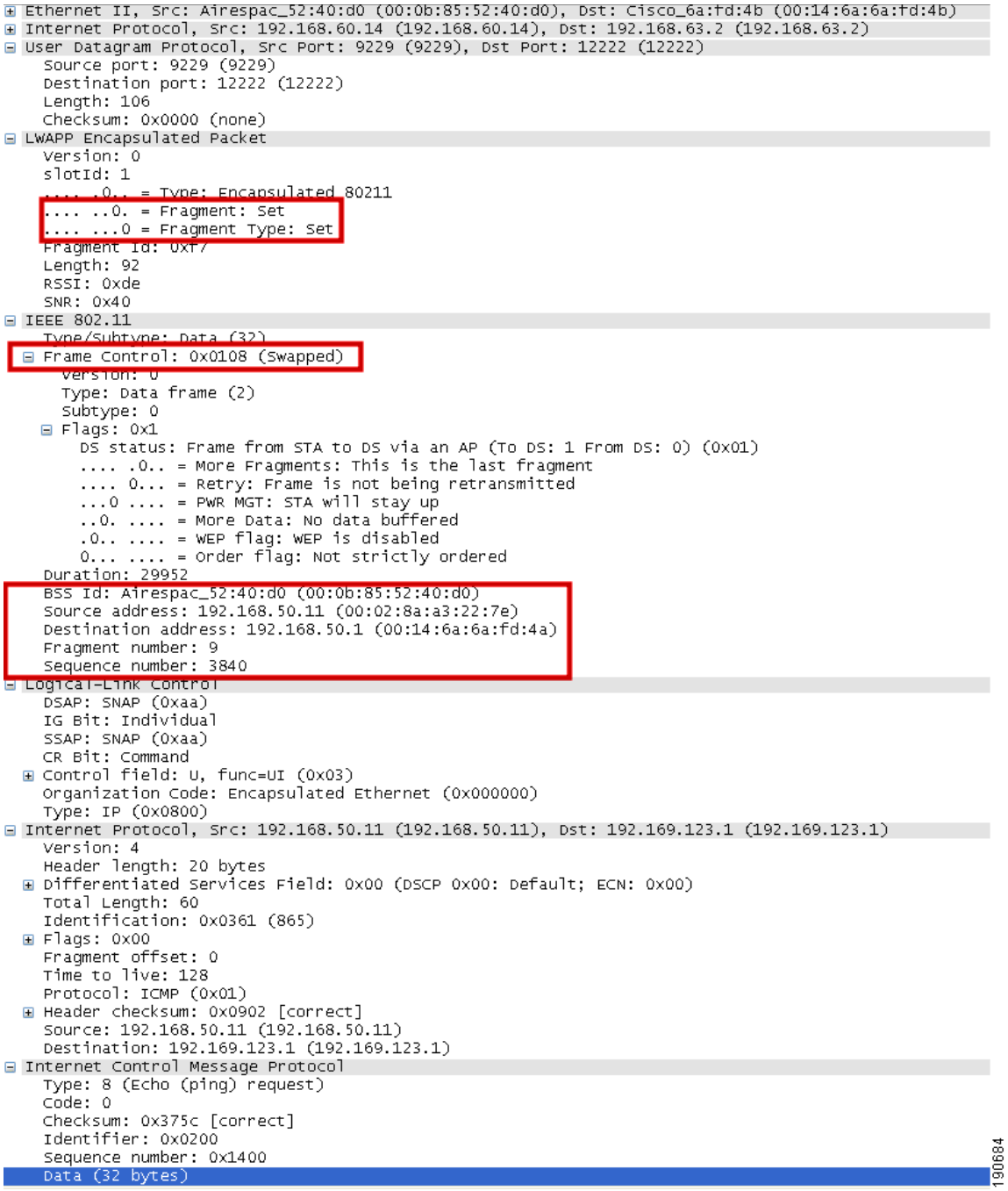


Figure 2-5 shows another LWAPP-encapsulated 802.11 frame, but in this case it is an 802.11 data frame, like that shown in Figure 2-4. It contains a complete 802.11 frame, as well as RSSI and SNR information for the WLC. This capture is being shown to illustrate that an 802.11 data frame is treated the same by LWAPP as the other 802.11 frames. Figure 2-5 highlights that fragmentation is supported, in order for LWAPP packets to accommodate the minimum MTU size between the LWAPP AP and the WLC. Note in the Wireshark decode that the frame control decode bytes have been swapped; this is accomplished during Wireshark's protocol analysis of the LWAPP packet to take into account that some LWAPP APs swap these bytes.

Figure 2-5 802.11 Data Frame in LWAPP



WLC Discovery and Selection

The following section highlights the typical behavior of a Layer 3 LWAPP AP upon being reset. For a comprehensive description of the discovery/join process, see the *440X Series Wireless LAN Controllers Deployment Guide* at the following URL: http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html.

Upon reset, the following sequence takes place:

Step 1 The AP broadcasts a Layer 3 LWAPP discovery message on the local IP subnet. Any WLC configured for Layer 3 LWAPP mode that is connected to the same IP subnet will see the discovery message. Each of the WLCs receiving the LWAPP discovery message will in turn reply with a unicast LWAPP discovery response message to the AP.

Step 2 If a feature called 'Over-the-Air Provisioning' (OTAP) is enabled on a WLC, APs that are already joined to that WLC will advertise their known WLCs in neighbor messages sent to other APs 'over the air'. Any new AP attempting to 'discover' WLCs for the first time will receive these messages and in turn unicast an LWAPP discovery request to each WLC advertised in the OTAP message. (OTAP is not supported by IOS APs in their initial state. In other words, a new IOS-based AP cannot use OTAP to discover a WLC.) WLCs that receive LWAPP discovery request messages unicast an LWAPP discovery response to the AP.

Step 3 The AP maintains previously learned WLC IP addresses locally in NVRAM. The AP sends a unicast LWAPP discovery request to each of these WLC IP addresses. Any WLC receiving an LWAPP discovery request responds by sending an LWAPP discovery response to the AP. As stated earlier, WLC IP addresses can be learned via OTAP messages sent from existing APs already joined to WLCs. The information stored in NVRAM also includes address information for any previously joined WLC that was a member of another mobility group. (The mobility group concept is discussed in greater detail later in this document.)

Step 4 If OTAP is not used, DHCP servers can be programmed to return WLC IP addresses using vendor specific DHCP options. In this case "Option 43" is used in a "DHCP offer" to "advertise" WLC addresses to LWAPP APs. When an AP receives its IP address via DHCP, it checks for WLC IP address information in the Option 43 field of the DHCP 'offer'. The AP sends a unicast LWAPP discovery message to each WLC listed in the DHCP Option 43. WLCs receiving the LWAPP discovery request messages unicast an LWAPP discovery response to the AP.

Step 5 In lieu of Option 43 information, the AP attempts to resolve the following DNS name: "CISCO-LWAPP-CONTROLLER.localdomain". If the AP is able to resolve this, it sends a unicast LWAPP discovery message to each IP address returned in the DNS reply. As described above, each WLC that receives an LWAPP discovery request message replies with a unicast LWAPP discovery response to the AP.

Step 6 If after Steps 1 through 5 no LWAPP discovery response is received, the AP resets and restarts the search algorithm.

Typically, either the DHCP or DNS discovery mechanism is used to provide one or more seed WLC addresses, and then a subsequent WLC discovery response provides a full list of WLC mobility group members.

An LWAPP AP is normally configured with a list of up to 3 WLCs that represent preferred WLCs. If these WLCs become unavailable or are over-subscribed, the AP chooses another WLC from the list of WLCs learned in the discover response and chooses the least-loaded WLC.

Components

There are three primary components that make up Cisco's Unified Wireless Architecture: the Lightweight APs, the WLC, and the WCS. This section describes the AP and WLC product options.

The Cisco WCS is an optional network component that works in conjunction with Cisco Aironet Lightweight APs, Cisco wireless LAN controllers and the Cisco Wireless Location Appliance. With Cisco WCS, network administrators have a single solution for RF prediction, policy provisioning, network optimization, troubleshooting, user tracking, security monitoring, and wireless LAN systems management. Robust graphical interfaces make wireless LAN deployment and operations simple and cost-effective. Detailed trending and analysis reports make Cisco WCS vital to ongoing network operations. More information on Cisco WCS can be found at the following URls:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html

http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

WLCs

For convenience, this document refers to all Cisco Unified Wireless controllers as WLCs due to the general uniformity and commonality of features across all of Cisco's WLC platforms.

The following summarizes the various Cisco Unified Wireless WLCs and their features:

- 2106—Is a standalone WLC that supports up to six APs, with eight Fast Ethernet interfaces. Two of the Fast Ethernet interfaces can be used to power (802.3af) directly connected APs. The interface can be configured as dot1q trunks to provide connection into the wired network. The 2106 is ideal for a small-to-medium size offices, where an H-REAP would otherwise be unsuitable because of the number of users, WAN requirements, and/or client roaming requirements.
- 4402—Is a standalone WLC that supports either 12, 25, or 50 APs. It comes with two SFP-based Gigabit Ethernet ports that can be configured as dot1q trunks to provide connection into the wired network, or the Gigabit ports can be link-aggregated to provide an EtherChannel connection to the switched network. This is ideal for medium-size offices or buildings.
- 4404—Is a standalone WLC that supports 100 APs. It comes with four SFP-based Gigabit Ethernet ports that can be configured as dot1q trunks to provide connection into the wired network. The Gigabit ports can be link aggregated to provide an EtherChannel connection to the switched network. This is ideal for large offices, buildings, and even a small campus.
- WLCM—The WLC module is specifically designed for Cisco's Integrated Service Router (ISR) series. It's currently available in a 6, 8 or 12 AP version. The WLCM appears as an interface on the ISR router that can be configured as a dot1q trunk to provide a routed connectivity to the wired network. This is ideal for small-to-medium size offices requiring an integrated solution.
- WS-C3750G—Is a WLC that supports either 25 or 50 APs that comes integrated with the Catalyst 3750 switch. The WLC's backplane connections appear as two Gig Ethernet ports, that can be configured separately as dot1q trunks to provide connection into the 3750. Or, the Gig ports can be link aggregated to provide a single EtherChannel connection to the 3750. Because the WLC is integrated directly it has access to all of the advanced routing and switching features available in the 3750 stackable switch. It is ideal for medium-size offices or buildings. The '50 AP' version can scale up to 200 APs when four 3750s are stacked together as a virtual switch.

- WiSM—Is a WLC module that is designed specifically for Cisco's Catalyst 6500 switch series. It supports up to 300 APs per module. Depending on the 6500 platform, multiple WISMs can be installed to offer significant scaling capabilities. The WiSM appears as a single aggregated link interface on the 6500 that can be configured as a dot1 trunk to provide connection into the 6500 backplane. This is ideal for large buildings or campuses.

Table 2-1 summarizes the Cisco Unified Wireless Controllers.

Table 2-1 Cisco Unified Wireless Controller Summary

Product	Number of APs	Interfaces	Comments
2106	6	8x Fast Ethernet	Cannot be a Mobility Anchor, does not support Layer 2 LWAPP, 2 of the Fast Ethernet interfaces support 802.3af for PoE.
4402	12 or 25	2x Gig Ethernet	
4404	50 or 100	4x Gig Ethernet	
WLCM	6, 8 or 12	ISR backplane	Cannot be a Mobility Anchor, does not support Layer 2 LWAPP. Layer 3 sub-interface termination of static and dynamic WLC interfaces only, no support for dot1q trunking.
WS-C3750G	25 or 50	3750 backplane	Full featured 3750 stackable switch with integrated WLC
WiSM	300	6500 backplane	Module directly connecting to the 6500 backplane

APs

Within the Cisco Unified Wireless Architecture, there are two categories of APs: standalone and LWAPP. This section briefly discusses the various models of AP products available within each category, and contrasts features, functionality, and applications. Cisco's 1500 series MESH APs are mentioned briefly below; however, this design guide does not address wireless MESH applications or deployment guidelines. Refer to the following guides for further information about the Cisco MESH solution:

- Cisco Mesh Networking Solution Deployment Guide: http://www.cisco.com/en/US/docs/wireless/access_point/mesh/4.0/deployment/guide/overview.html
- Cisco Aironet 1500 Series Wireless Mesh AP Version 5.0 Design Guide: http://www.cisco.com/en/US/docs/wireless/technology/mesh/design/guide/MeshAP.html

Cisco Standalone APs

APs in this category consist of the original Aironet product line. The following select models are available in or are capable of being field-upgraded to LWAPP mode of operation. This feature permits an enterprise to standardize on a common AP platform that can be deployed in mixed wireless topologies.

First generation standalone APs are as follows:

- AP 1100—This single band 802.11b/g AP. It has an integrated antenna and is considered an entry-level AP for enterprise deployments. The part number for the LWAPP AP is AIR-LAP1121G-x-K9 where x= the regional code.

- AP 1200—A single band 802.11b/g AP that is targeted for enterprise deployments. Unlike the 1100 series, the 1200 supports connections to external antennas for more flexibility. It can be field-upgraded to support an 802.11a radio as well as upgradeable for lightweight (LWAPP) operation. The part number for the LWAPP AP is AIR-LAP1231G-x-K9 where x= the regional code.
- AP 1230AG—Dual band 802.11a/b/g AP with external connectors for antennas in both bands. It does not have all of the features (most notably 802.3af PoE standard) and RF performance of the 1240AG. It also comes in a lightweight (LWAPP) version or can be upgraded later to lightweight mode of operation. The part number for the LWAPP AP is AIR-LAP1232G-x-K9 where x= the regional code.

Second generation standalone APs are as follows:

- AP 1130AG—The AG version is dual band (a/b/g) AP with integrated antennas. It is designed to be wall-mounted and makes use of an integrated dual-band antenna. The 1130AG is available in a lightweight (LWAPP) version for implementation in centralized (WLC)-based deployments. The standalone version can be upgraded for lightweight operation. The part number for the LWAPP AP is AIR-LAP1131AG-x-K9 where x = the regional code.
- AP 1240AG—A dual band 802.11 a/b/g AP designed for deployments in challenging RF environments such as retail and warehousing. The 1241AG possesses external connections for antennas in both bands. It is the most feature-rich AP in the standalone category and is also available in a lightweight (LWAPP) version. For greatest flexibility, the standalone version can be upgraded later to lightweight mode of operation. Other notable features include pre-installed certificates for LWAPP operation mode and the ability to support hybrid REAP. The part number for the LWAPP AP is AIR-LAP1242AG-x-K9 where x = the regional code,
- AP 1300—A single band 802.11b/g AP/bridge designed for outdoor deployments. It comes with an integrated antenna or can be ordered with RP-TNC connectors to support external antenna applications. The LWAPP AP part number is AIR-LAP1310G-x-K9 where x = the regional code.

A new third generation AP, the Cisco 1252, is a business class AP that supports draft 2 of the emerging 802.11n standard. 802.11n offers combined data rates up to 600Mbps using Multiple-Input Multiple-Output (MIMO) technology. The Cisco 1252 is available in a dual-band a/b/g or a single-band b/g radio configuration and can be deployed as a stand alone AP (standalone) or as part of a unified (controller) wireless deployment. In order to offer maximum deployment flexibility, the Cisco 1252 is equipped with RP-TNC connectors for use with a variety of external 2.4 and 5Ghz antennas. In order to support the greater throughput rates offered by 802.11n, the Cisco 1252 incorporates a gigabit 10/100/1000 interface. The Cisco 1252 is designed to be deployed in challenging RF environments where high bandwidths are needed. Part numbers for the standalone version include: AIR-AP1252AG-x-K9 (Dual Band) and AIR-AP1252G-x-K9 (single band). Part numbers for the Cisco Unified Wireless versions include: AIR-LAP1252AG-x-K9 (dual band) and AIR-LAP1252G-x-K9 (single band).

Cisco LWAPP APs

APs in this category consist of the original Airespace product line, but also include the standalone AP models noted above. The following models can be used only in WLC topologies:

- AP 1010—Dual band, zero touch, 802.11a/b/g AP intended for basic enterprise LWAPP/WLC deployments. The 1010 comes with internal dual sector antennas. The part number is AIR-AP1010-x-K9 where x = the regional code.
- AP 1020—Similar to the 1010, but in addition to its internal sector antennas, it also includes RP-TNC connectors for external 2.4 and 5 GHz antennas. The part number is AIR-AP1020-x-K9 where x = the regional code.

- AP 1030—Also referred to as the REAP AP or Remote Edge AP, the 1030 possesses the same capabilities, features, and performance as the 1020, in addition to being able to be deployed in environments where it is not practical to deploy a WLC, such as in small branch offices. The part number is AIR-AP1030-x-K9 where x = the regional code.
- AP 1500—A dual band AP specifically designed for outdoor, point-to-point, and multipoint MESH deployments. The 802.11a band is used for backhaul while the b/g band is used for wireless client access. The 1500 uses (patent pending) Adaptive Wireless Path Protocol (AWPP) for optimal routing through MESH topologies.

Table 2-2 and Table 2-3 provide a comparison summary of the APs discussed above.

Table 2-2 AP Comparison (1)

Cisco Series	802.11b/g	802.11a	802.11n	Standalone	LWAPP	# Broadcasted SSIDs	Preinstalled Cert?
1000	YES	YES	NO	NO	YES	16	YES
1100	YES	NO	NO	YES	YES	8[1]	NO
1130AG	YES	YES	NO	YES	YES	8[1]	YES[2]
1200	YES	Optional	NO	YES	YES	8[1]	YES[2]
1230AG	YES	YES	NO	YES	YES	8[1]	YES[2]
1240AG	YES	YES	NO	YES	YES	8[1]	YES[2]
1252AG	YES	YES	YES	YES	YES	8[1]	YES
1252G	YES	NO	YES	YES	YES	8[1]	YES
1300	YES	NO	NO	YES	YES	8[1]	NO
1500	YES	YES	NO	NO	YES	16	YES

1. 16 BSSIDs to be supported in future Releases.
2. Units shipped prior to August 2005 require a Cisco-provided utility to load self-signed certificate, and an 11g radio is required.

Table 2-3 AP Comparison (2)

Cisco Series	Office and similar environments	Challenging Indoor environments	Outdoors
1010	Recommended[1]	Not Recommended	Not Recommended
1020	Recommended[1]	Recommended[1]	Not Recommended
1100	Recommended	Not Recommended	Not Recommended
1130AG	Ideal	Not Recommended	Not Recommended
1200	Recommended[2]	Recommended	Recommended[2]
1230AG	Recommended	Recommended	Recommended[2]
1240AG	Recommended[2]	Ideal	Recommended[2]
1300	Not Recommended	Not Recommended	Ideal[3]
1500	Not Recommended	Not recommended	Ideal[1]

1. Or 1030 for Remote offices. LWAPP Deployments Only.

2. Can be used outdoors when deployed in weatherproof NEMA rated enclosure. Particularly for deployments above suspended ceilings.
3. Standalone Deployments Only.

For further detailed information, see the following link:
http://www.cisco.com/en/US/products/ps6108/prod_brochure0900aecd8035a015.html

Mobility Groups, AP Groups, and RF Groups

Within the Cisco Unified Wireless Architecture, there are three important 'group' concepts:

- Mobility groups
- AP groups
- RF groups

This section describes the purpose and application of these groups within the Cisco Unified Wireless Architecture. For more details on operation and configuration, see the following URLs:

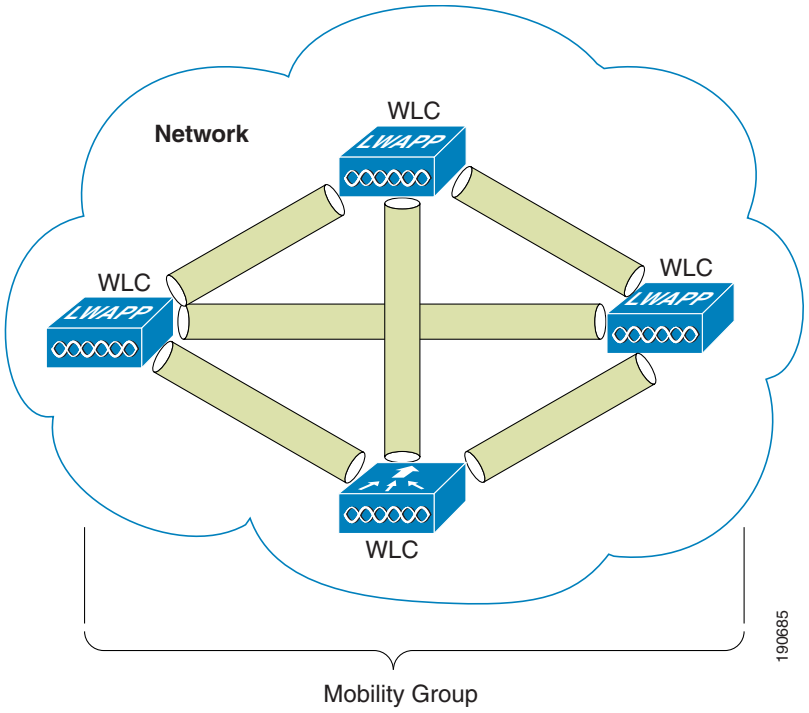
- Deploying Cisco 440X Series Wireless LAN Controllers—
http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html
- Cisco Wireless LAN Controller Configuration Guide, Release 4.1—
http://www.cisco.com/en/US/docs/wireless/controller/4.1/configuration/guide/ccfig41.html

Mobility Groups

A mobility group is a group of WLCs that together, act as a single virtual WLC by sharing essential end client, AP, and RF information. A given WLC within a mobility domain, is able to make decisions based on data received from other members of the entire mobility group, rather than relying solely on the information learned from its own directly connected APs and clients.

A mobility group forms a mesh of authenticated tunnels between member WLCs, thereby allowing any WLC to directly contact another WLCs within the group, as shown in Figure 2-6.

Figure 2-6 WLC Mobility Group



Mobility Group Definition

Creating a mobility group is simple and well documented; however, there are some important considerations to keep in mind:

- Up to 24 WLAN controllers and 3600 APs are supported per mobility group. An enterprise may consist of more WLAN controllers and APs, but they must be configured as members of another mobility group.
- The WLCs do not have to be of the same model/type to be a member of a mobility group. For example, a group may comprise of any combination of the following: 4402, 4404, WiSM, WLCM, 3750G, and 2106; however, they should all be running the same software version. With that said, a mobility group will not be broken simply because of software differences, but a common software version is strongly recommend in order to ensure feature and functional parity across a unified wireless deployment.
- A mobility group requires all WLCs in the group to use the same virtual IP address.
- Each WLC must use the same ‘mobility domain name’ and be defined as a peer in each others ‘Static Mobility Members’ list.
- In order for a wireless client to seamlessly roam between mobility group members (WLCs), a given WLAN's SSID and security configuration must be configured identically across all WLCs comprising the mobility group.

Mobility Group Application

Mobility groups are used to help facilitate seamless client roaming between APs that are joined to different WLCs. The primary purpose of a mobility group is to create a virtual WLAN domain (across multiple WLCs) in order to provide a comprehensive view of a wireless coverage area. The use of mobility groups are beneficial only when a deployment comprises of 'overlapping' coverage established by two or more APs that are connected to different WLCs. A mobility group is of no benefit when two APs, associated with different controllers, are in different physical locations with no overlapping (contiguous) coverage between them (for example, Campus and Branch or between two or more buildings within a campus).

Mobility Group—Exceptions

The Cisco Unified Wireless solution offers network administrators the ability to define static mobility tunnel (Auto Anchor) relationships between an ‘anchor’ WLC and other WLCs in the network. This option, among other things, is used when deploying wireless guest access services.

If the auto anchor feature is used, no more than 24 (foreign) WLCs can be mapped to a designated anchor WLC. Foreign WLCs do not, by virtue of being connected to the auto anchor, establish mobility relationships between each other. The anchor WLC must have a ‘static mobility group member’ entry defined for each foreign WLC where a static mobility tunnel is needed. Likewise for each foreign WLC where a static mobility tunnel is being configured, the anchor WLC must be defined as a ‘static mobility group member’ in the foreign WLC.

A WLC can only be member of one mobility group for the purpose of supporting dynamic inter-controller client roaming. A WLC that is configured as an ‘auto anchor’, does not have to be in the same mobility group as the foreign WLCs. It is possible for a WLC to be a member of one mobility group whilst at the same time, act as an auto anchor for a WLAN originating from foreign WLCs that are members of other mobility groups.

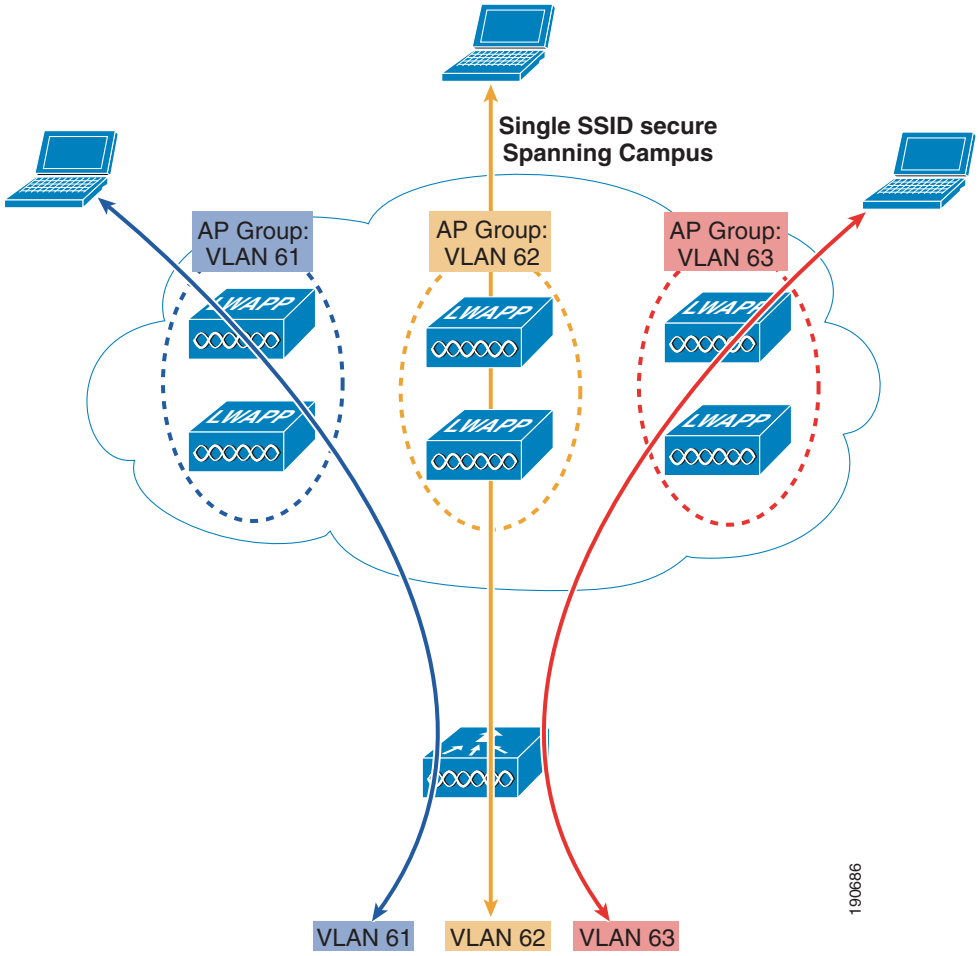
For a discussion on mobility anchor configuration, see Chapter 10, “Cisco Unified Wireless Guest Access Services.”

AP Groups

In typical deployment scenarios, each WLAN is mapped to a single dynamic interface per WLC. However, consider a deployment scenario where there is a 4404-100 WLC supporting the maximum number of APs (100). Now consider a scenario where 25 users are associated to each AP. That would result in 2500 users sharing a single VLAN. Some customer designs may require substantially smaller subnet sizes. One way to deal with this is to break up the WLAN into multiple segments. The WLC’s AP grouping feature allows a single WLAN to be supported across multiple dynamic interfaces (VLANs) on the controller. This is done by taking a group of APs and mapping them to a specific dynamic interface. APs can be grouped logically by employee workgroup or physically by location. Figure 2-7 illustrates the use of AP groups based on site-specific VLANs.

Note AP groups do not allow multicast roaming across group boundaries; this is discussed in more detail later in this design guide.

Figure 2-7 AP Groups and Site-Specific VLANS



In Figure 2-7, there are three dynamic interfaces configured, each mapping to a site-specific VLAN: VLAN 61, 62, and 63. Each site specific VLAN and associated APs are mapped to the same WLAN SSID using the AP grouping feature. A corporate user associating to the WLAN on an AP in the AP Group corresponding to VLAN 61 gets an IP address on the VLAN 61 IP subnet. Likewise, a corporate user associating to the WLAN on an AP in the AP Group corresponding to VLAN 62 gets an IP address on the VLAN 62 IP subnet and so on. Roaming between the site-specific VLANs is handled internally by the WLC as a Layer 3 roaming event and as such, the wireless LAN client maintains its original IP address.

RF Groups

RF groups, also known as RF domains, represent another important deployment consideration. An RF group is a cluster of WLCs that collectively coordinate and calculate their dynamic radio resource management (RRM) settings based on 802.11 PHY type (for example, 802.11b/g and 802.11a).

An RF group exists for each 802.11 PHY type. Grouping WLCs into RF domains allows the solution's dynamic RRM algorithms to scale beyond a single WLC, thereby allowing RRM for a given RF domain to extend between floors, buildings, and even across campuses. RF Groups and RRM is discussed in more detail in a later chapter of this document, but can be summarized as follows:

- LWAPP APs periodically send out neighbor messages over the air that includes the WLC's IP address and a hashed message integrity check (MIC) derived from a timestamp and the BSSID of the AP.
- The hashing algorithm uses a shared secret (the RF Group Name) that is configured on the WLC and is pushed out to each AP. APs sharing the same secret are able to validate messages from each other using the MIC. When APs belonging to other WLCs hear validated neighbor messages at a signal strength of -80 dBm or stronger, their WLCs dynamically become members of the RF group.
- Members of an RF group elect an RF domain leader to maintain a "master" power and channel scheme for the RF group.
- The RF group leader analyzes real-time radio data collected by the system and calculates a master power and channel plan.
- The RRM algorithms:
  - Try to achieve a uniform (optimal) signal strength of -65 dBm across all APs
  - Attempt to avoid 802.11 co-channel interference and contention
  - Attempt to avoid non-802.11 interference.
- The RRM algorithms employ dampening calculations to minimize system-wide dynamic changes. The end result is dynamically calculated, near-optimal power and channel planning that is responsive to an ever changing RF environment.
- The RF group leader and members exchange RRM messages at a specified update interval, which is 600 seconds by default. Between update intervals, the RF group leader sends keep alive messages to each of the RF group members and collects real-time RF data. Note that the maximum number of controllers per RF group is 20.

Roaming

Roaming in an enterprise 802.11 network can be described as when an 802.11 client changes its AP association from one AP within an ESS to another AP in the same ESS. Depending on network features and configuration, several events can occur between the client, WLCs, and upstream hops in the network, but at the most basic level, roaming is simply a change in AP association.

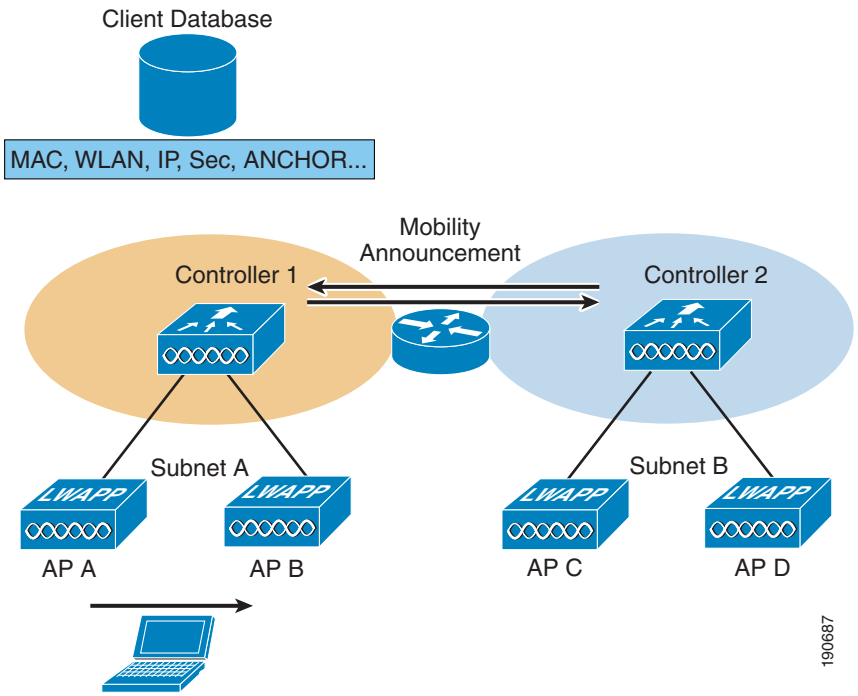
When a wireless client authenticates and associates with an AP, the corresponding WLC (to which the AP is connected) creates an entry for that client in its client database. This entry includes the client MAC and IP addresses, security context and associations, QoS context, WLAN, and associated AP. The WLC uses this information to forward frames and manage traffic to and from the wireless client.

When the wireless client moves its association from one AP to another, the WLC simply updates the client database with information about the new AP. If necessary, new security context and associations are established as well.

A Layer 2 roam occurs when a client leaves one AP and re-associates with a new AP, in the same client subnet. In most cases, the 'roamed to' AP is connected to the same WLC as the original AP.

The description above represents the simplest roaming scenario because a single WLC database maintains all information about the client. Network elements upstream from the WLC are unaffected by the client moving from one AP to another as illustrated in Figure 2-8.

Figure 2-8 Layer 2 Roam



When there are multiple WLCs connecting a WLAN to the same subnet and a client roams between APs connected to different WLCs, a mobility announcement is exchanged between the WLCs. The mobility announcement passes client-context information between WLCs.

WLC to WLC Roaming Across Client Subnets

In cases where a client roams between APs that are connected to different WLCs and the client subnet/VLAN is not the same between the WLCs, then a Layer 3 roam is performed. A mobility announcement is exchanged between the 'roamed to' (foreign) WLC's mobility database and the home (anchor) WLC's mobility database.

A Layer 3 roam is more complex because the wireless client is moving from one VLAN/subnet to another. Unless the WLAN system takes action to make the client subnet change transparent, the Layer 3 roam event has an adverse impact on client communication with upstream services. Existing client sessions will either hang or eventually timeout and disconnect. The Cisco Unified Wireless solution uses mobility tunnels to facilitate Layer 3 roaming that is transparent to the upstream network There are two types of mobility tunnels:

- Asymmetrical (default behavior – WLC Releases 4.0 and earlier)
- Symmetrical (new option beginning with WLC Releases 4.1 and later)

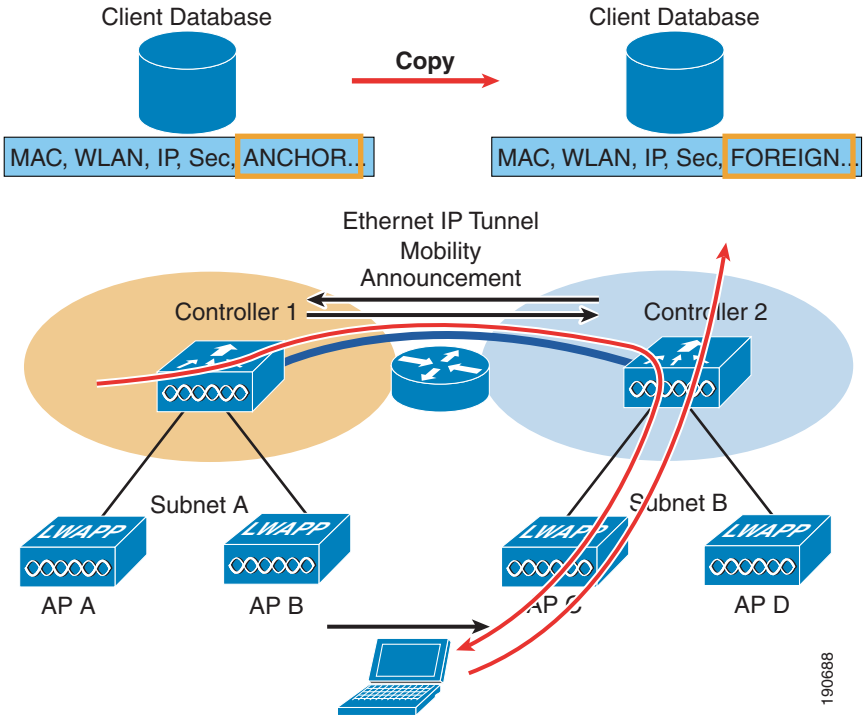
Note In WLC Release 4.1, asymmetrical tunneling is still the default behavior. Administrators must explicitly configure symmetrical tunnel behavior.

Layer 3 Roam—Asymmetrical Mobility Tunnel

In a Layer 3 roaming scenario, traffic returning to the wireless client goes through the anchor WLC. The anchor WLC establishes an Ethernet-over-IP (EoIP) tunnel to forward client traffic to the foreign WLC where it is then delivered to the client. All traffic originated by the client is forwarded out the corresponding VLAN interface to which the WLAN is mapped to at foreign WLC. The client's original IP address and default gateway IP (MAC) address remain the same. All traffic, other than that which is destined for the local subnet, is forwarded to the default router where the foreign WLC substitutes the client's default gateway MAC address with the MAC address of the default gateway associated with dynamic interface/VLAN at the foreign controller.

Figure 2-9 illustrates a client Layer 3 roam using an asymmetrical mobility tunnel.

Figure 2-9 Layer 3 Roaming



Using Figure 2-9, the following occurs when a client roams across a Layer 3 boundary:

1. The client begins with a connection to AP B on WLC 1.
2. This creates an ANCHOR entry in WLC 1's client database.
3. As the client moves away from AP B and begins association with AP C, WLC 2 sends a mobility announcement to its peers in the mobility group looking for the WLC with information for the client MAC address.
4. WLC 1 responds to the announcement, handshakes, and ACKs.
5. The client database entry for the roaming client is copied to WLC 2, and marked as FOREIGN. PMK data (master key data from the RADIUS server) is also copied to WLC 2. This facilitates fast roaming for WPA2/802.11i clients because there is no need to undergo full re-authentication with the RADIUS server.

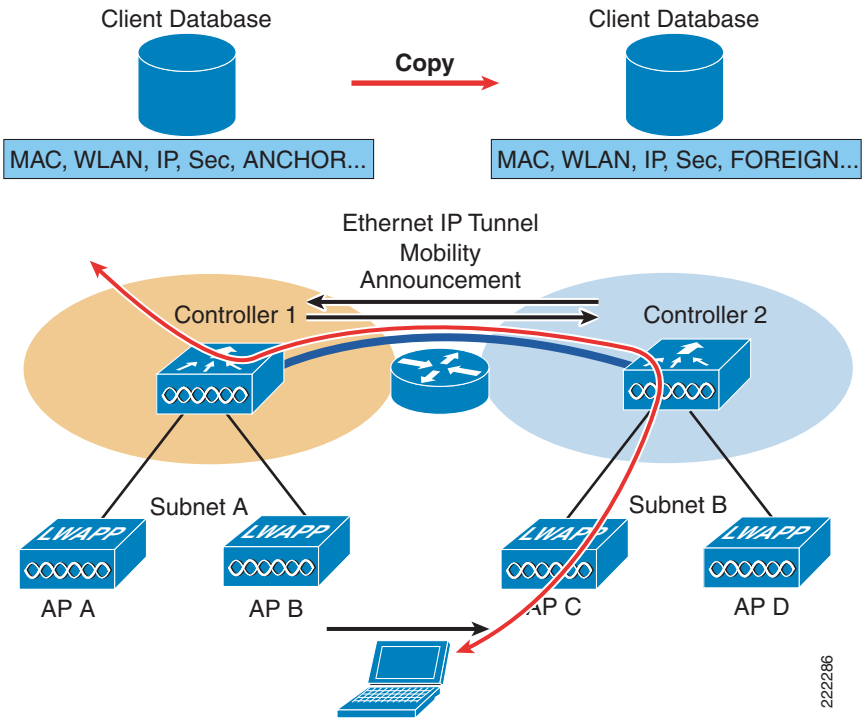
6. A simple key exchange is made between the client and AP, the client is added to WLC 2's database, which is similar to the anchor controller's entry, except that the client entry is marked as FOREIGN.
7. Data being sent to the WLAN client is now EoIP tunneled from the anchor WLC to the foreign WLC.
8. Data sent by the WLAN client is sent out a local interface VLAN at the foreign controller.

The 'asymmetrical' Layer 3 roaming procedure described above solves the challenge of roaming transparently across Layer 3 boundaries; however, the asymmetric flows can cause other issues in the upstream network. This is especially true if wireless client traffic is expected to flow bi-directionally through adjacent appliances or modules such as firewalls, NAC and or IPS/IDS appliances. Or, for example, if uRPF checks are enabled on next hop routed interfaces, traffic is dropped after the client roams to a different subnet. This is the reason why a symmetrical mobility tunnel capability was introduced to the Cisco Unified Wireless solution.

Layer 3 Roam—Symmetrical Mobility Tunnel

Beginning with WLC Release 4.1 and later, the WLCs can be configured to support dynamic, bi-directional tunneling between the foreign AP/WLC and the anchor WLC as shown in Figure 2-10.

Figure 2-10 Layer 3 Roam—Symmetrical Mobility Tunnel



The WLC's Layer 3 mobility handoff procedure remains unchanged. However, WLC Release 4.1 makes use of existing capabilities associated with the solution's auto anchor tunneling mechanism to create a dynamic symmetrical tunnel when a client performs a Layer 3 roam.

Symmetrical tunneling is not enabled by default. It must be explicitly configured either through the controller's web configuration interface, WCS template or the controller's CLI. Symmetrical mobility tunnel operation must be enabled for each controller that is a member of a given mobility group, otherwise unpredictable behavior can occur.

Figure 2-11 and Figure 2-12 show Wireshark protocol traces of a bidirectional mobility tunnel.

Figure 2-11 Bi-directional Mobility Tunnel(1)

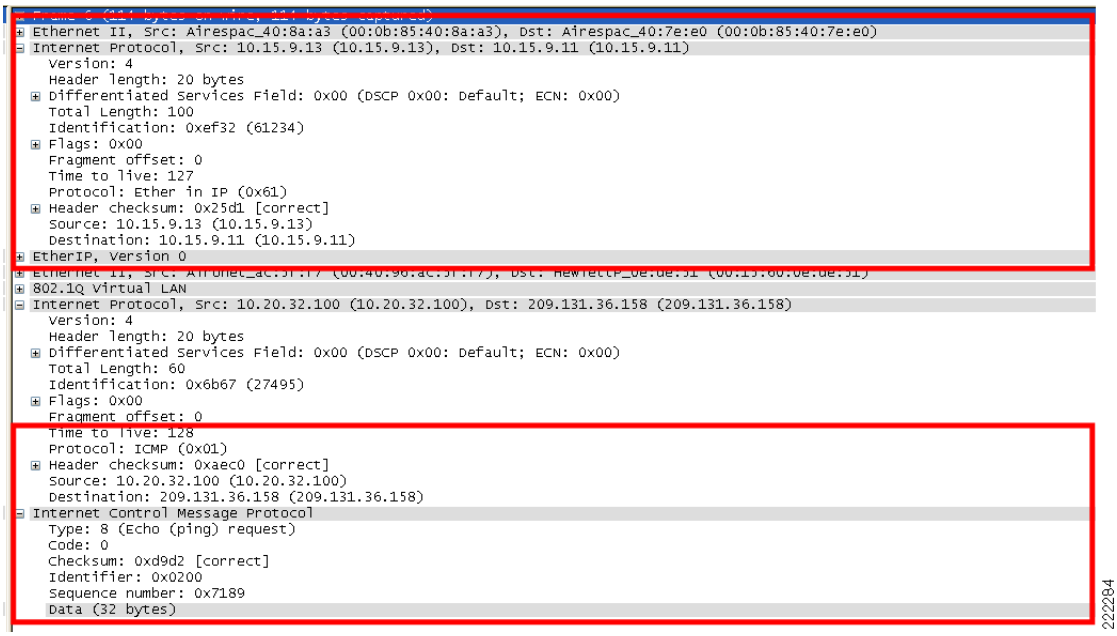
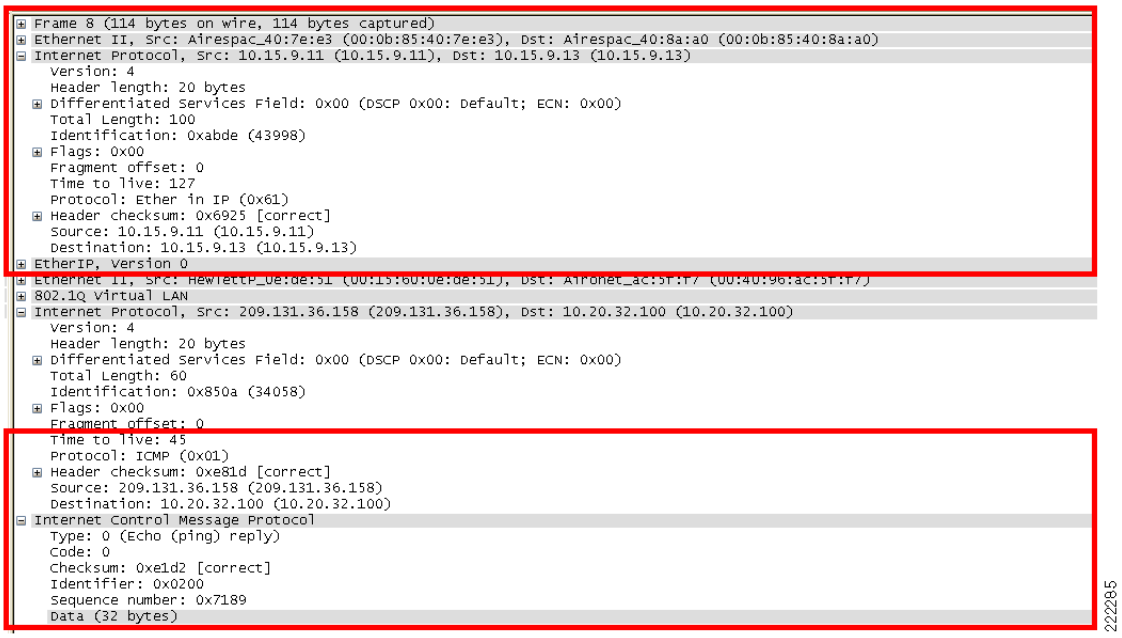


Figure 2-12 Bi-directional Mobility Tunnel(2)



In the protocol traces above, a symmetrical mobility tunnel (EtherIP) is established between two WLCs, 10.15.9.11 (anchor) and 10.15.9.13 (foreign). In Figure 2-11, client 10.20.32.100, which has roamed to an AP on controller 10.15.9.13, is sending an ICMP ping request to Internet site 208.131.36.158 (yahoo.com). Note that the foreign controller tunnels the client's packet to the anchor controller. If the controllers were configured for asymmetrical mobility tunneling, this packet would not appear in the

trace because the foreign controller would have forwarded it locally out the VLAN interface associated with the WLAN. In Figure 2-12, the ping reply is received by the anchor controller and forwarded to the foreign controller via same the mobility tunnel, which is the same as the asymmetrical tunnel.

Important Notes About Layer 3 Roaming

Layer 3 roaming is a highly useful capability, but when deploying with the 4.1 software release, remember the following points:

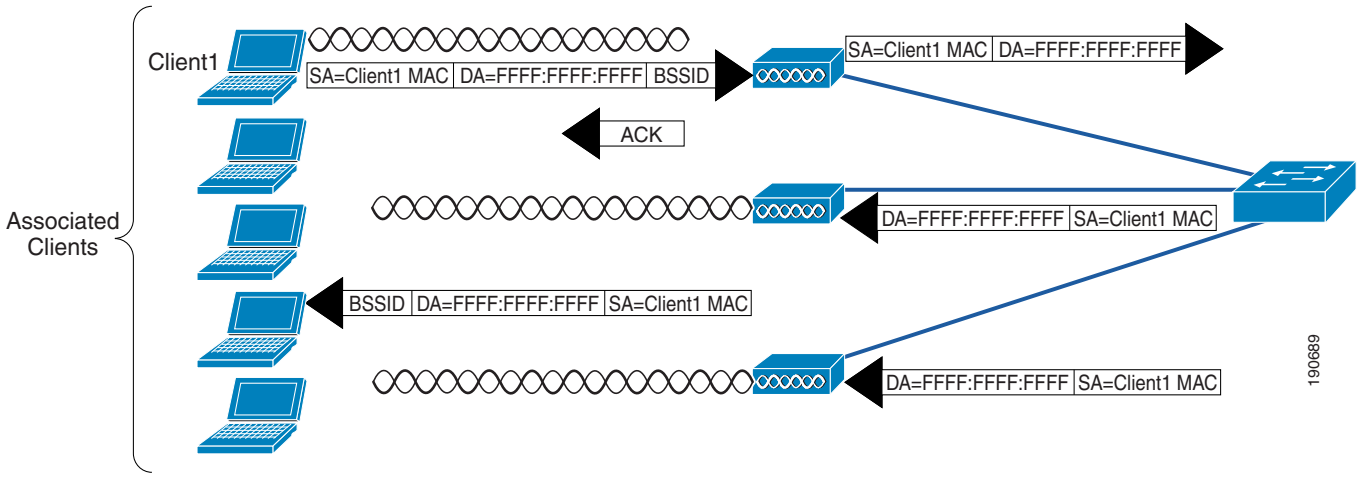
- Multicast group membership is not currently transferred during the client roam; that is, if a client is receiving a multicast stream and roams to a foreign WLC that multicast stream is broken, and must be re-established.
- The foundation for facilitating Layer 3 roaming within the Unified Wireless solution is based on the concept of mobility anchors and EoIP tunnels. An 'anchor WLC' is that WLC through which a client first associates to a WLAN. The client is then assigned an address, via DHCP, that corresponds to the interface/subnet assigned to the WLAN at the anchor controller. Currently, the Unified Wireless solution does not permit clients to connect to a WLAN with a static IP address that is outside the subnet defined for the WLAN. In deployment scenarios where static client addressing is necessary, Mobile IP should be investigated as a potential solution. For more details concerning Mobile IP and its compatibility with the Cisco Unified Wireless architecture, see Chapter 12, "Cisco Unified Wireless and Mobile IP."

Broadcast and Multicast on the WLC

The section discusses the handling of broadcast and multicast traffic by a WLC and its impact on design.

Figure 2-13 depicts basic 802.11 broadcast/multicast behavior. When client 1 in this example sends an 802.11 broadcast frame, it is unicasted to the AP. The AP then sends the frame as a broadcast out both its wireless and wired interfaces.

Figure 2-13 802.11 Broadcast/Multicast

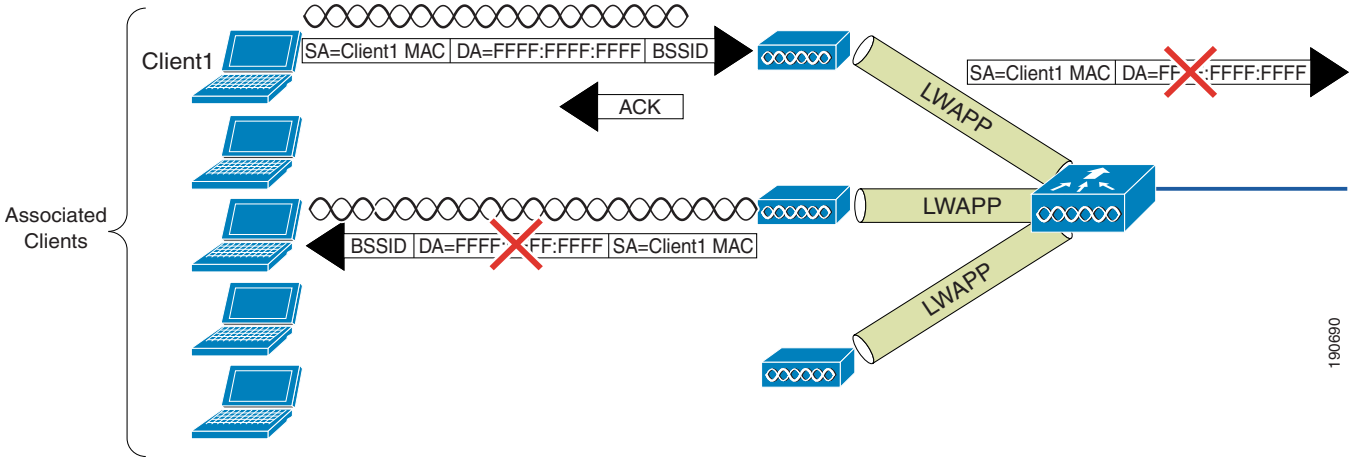


If there are other APs on the same wired VLAN as the AP as depicted in Figure 2-13, they forward the wired broadcast packet out their wireless interface.

The WLC's LWAPP split MAC method treats broadcast traffic differently, as shown in Figure 2-14. In this case, when a broadcast packet is sent by a client, the AP/Controller does not forward it back out the WLAN, and a only subset of all possible broadcast messages are forwarded out a given WLAN's wired interface at the WLC.

Note Which protocols are forwarded under which situations is discussed in the following section.

Figure 2-14 Default WLC Broadcast Behavior



WLC Broadcast and Multicast Details

Broadcast and multicast traffic often require special treatment within a WLAN network because of the additional load placed on then WLAN as a result of this traffic having to be sent at the lowest common bitrate. This is done to ensure that all associated wireless devices are able to receive the broadcast/multicast information.

The default behavior of the WLC is to block broadcast and multicast traffic from being sent out the WLAN to other wireless client devices. The WLC can do this without impacting client operation because most IP clients do not send broadcast/multicast type traffic for any reason other than to obtain network information (DHCP) and resolve IP addresses to MAC addresses (ARP).

DHCP

The WLC acts as a DHCP relay agent for associated WLAN clients. It unicasts client DHCP requests to a locally configured or upstream DHCP server except during L3 client roaming, which will be discussed in more detail below. DHCP server definitions are configured for each dynamic interface, which in turn is associated with one or more WLANs. DHCP relay requests are forwarded via the dynamic interfaces using the source IP address of a given dynamic interface. Because the WLC knows which DHCP server to use for a given interface/WLAN, there is no need to broadcast client DHCP requests out its wired and wireless interfaces.

The method above accomplishes the following:

- It eliminates the need for DHCP requests to be broadcasted beyond the WLC.

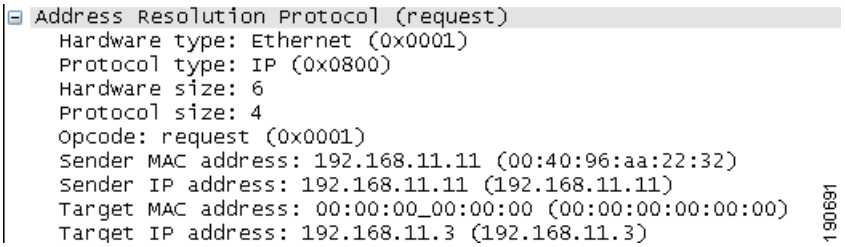
- The WLC becomes part of the DHCP process, thereby allowing it to learn the MAC / IP address relationships of connected WLAN clients, which in turn allows the WLC to enforce DHCP policies and mitigate against IP spoofing or denial-of-service (DoS) attacks.
- It allows the WLC to relay DHCP reply messages using a virtual DHCP server IP address rather than the actual IP address of a DHCP server The aforementioned behavior is configured via the WLC's CLI, and is enabled by default. The virtual address is shared by all WLCs that comprise a mobility group. The benefit of DHCP proxy is realized during L3 client roaming or when a client roams across an AP group boundary. In these cases, the WLC will receive a client DHCP renewal request upon which it will verify the client is roaming within the mobility group and allow the client to renew (keep) it's existing IP address/subnet assignment even though the client roamed to a new subnet on the foreign WLC. See Roaming, page 2-17.

Note The virtual IP/Proxy DHCP behavior described above is required if the asymmetrical mobility tunnel method is configured (default), see Roaming section above. Otherwise, if the symmetrical tunnel method is used, WLC based DHCP proxy is not necessary because client traffic and DHCP requests are always tunneled back to the anchor controller.

ARP

Before a WLAN client can send IP packets to any other IP address, it needs to know the MAC address of the target client to forward the frame to. To accomplish this, a client will broadcast an ARP query, requesting the MAC address for the IP host that it wishes to communicate with, see Figure 2-15.

Figure 2-15 ARP Frame



Upon seeing a wireless client ARP request, the WLC will either respond directly, acting as an ARP proxy in behalf of the other wireless clients, or it will forward the request out it's wired interface to have it resolved by another WLC. The WLC will not forward the ARP broadcast back out to the WLAN.

The default behavior of the WLC is to respond to ARP queries directly based on its local ARP cache. The WLC CLI command**: network arpunicast enable** can be used to override this behavior. In this case the WLC will unicast an ARP request directly to the target host rather than responding in behalf of the target. The target will unicast its ARP reply back to the requesting host. The purpose of this command is to avoid excessive retries by IP clients looking for a WLAN client that may have roamed from the WLAN network.

Other Broadcast and Multicast Traffic

As mentioned earlier the WLC (by default) will not forward broadcasts or multicasts toward the wireless users. If multicast forwarding is explicitly enabled as described in Chapter 6, "Cisco Unified Wireless Multicast Design," steps should be taken to minimize the multicast traffic generated on those interfaces that the WLC connects to.

All normal precautions should be taken to limit the multicast address groups explicitly supported by a WLAN. When multicast is enabled, it is global in nature, meaning it is enabled for every WLAN configured regardless if multicast is needed by that WLAN or not. The unified wireless solution is not able to distinguish between data link layer versus network layer multicast traffic neither is the WLC capable of filtering specific multicast traffic. Therefore, the following additional steps should be considered:

- Disable CDP on interfaces connecting to WLCs.
- Port filter incoming CDP and HSRP traffic on VLANs connecting to the WLCs.
- Remember that multicast is enabled for all WLANs on the WLC, including the Guest WLAN, therefore multicast security including link layer multicast security must be considered.

Design Considerations

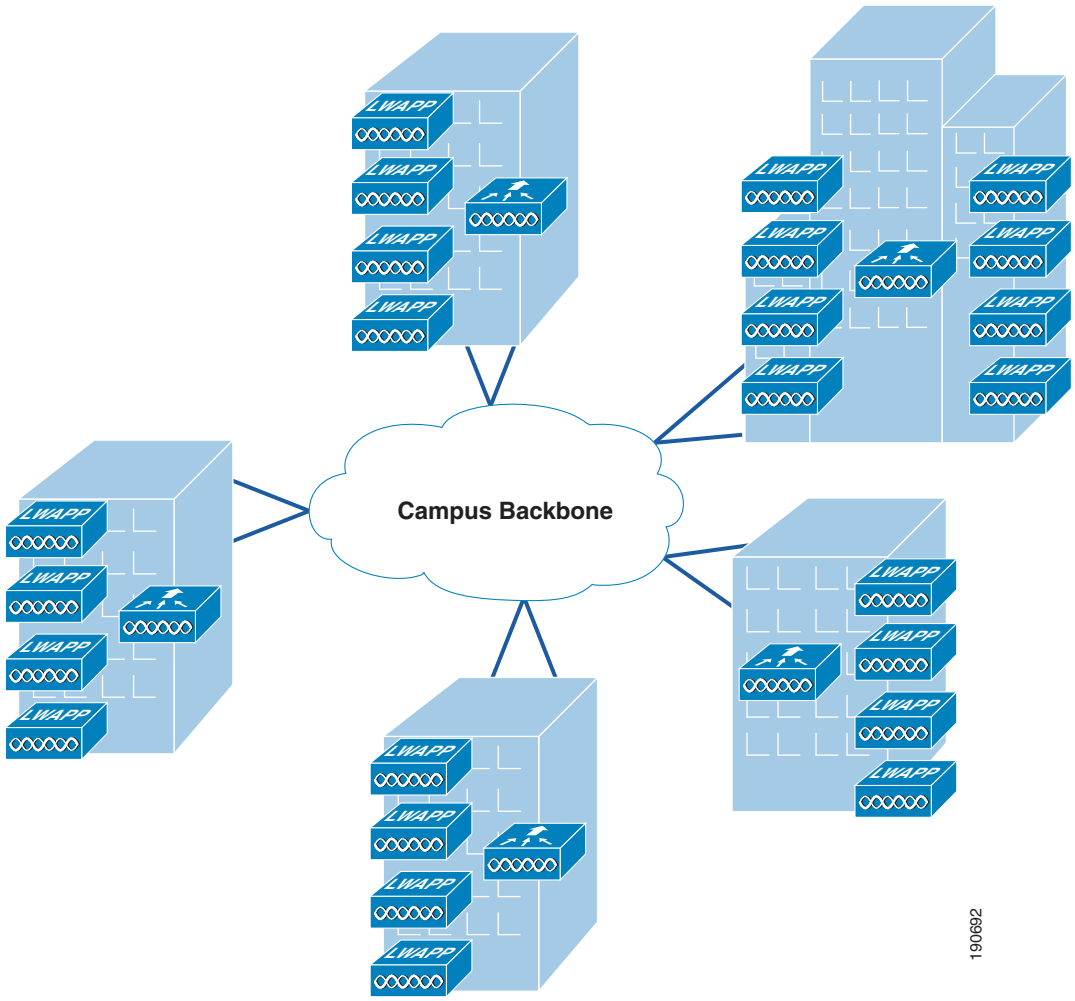
Within a Cisco Unified Wireless deployment, the primary design considerations are: AP connectivity, and WLC location and connectivity. This section will briefly discuss these topics and make general recommendations where appropriate.

WLC Location

The flexibility of Cisco Unified Wireless LAN solution leads to the following choices about where to locate WLCs:

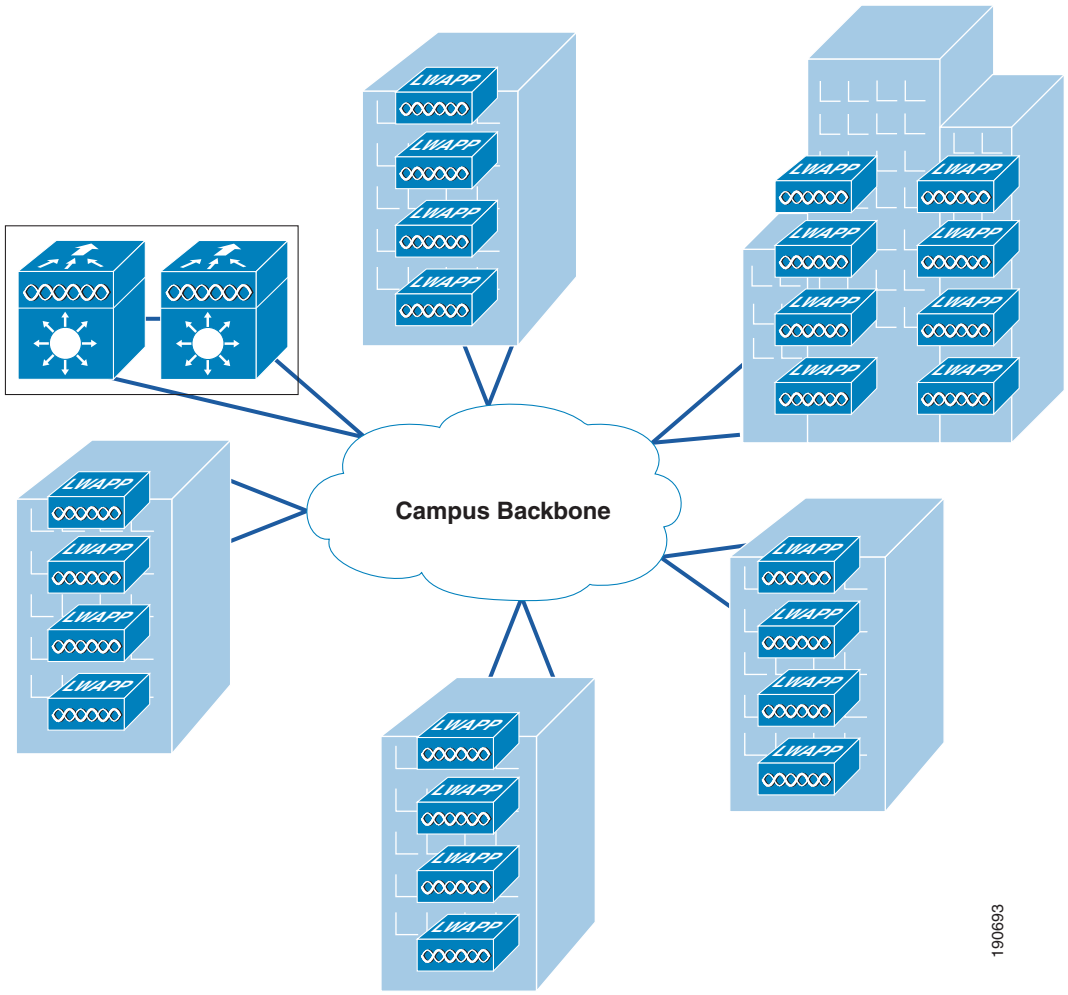
- Distributed WLC deployment—In the distributed model, WLCs are located throughout the campus network, typically on a per building basis, managing the APs that are resident in a given building. The WLC(s) is connected to the campus network using the distribution routers within the building. In this scenario the LWAPP tunnels, between APs and the WLC typically stay within the building. Figure 2-13 shows a distributed WLC deployment.
- Each of the distributed WLCs could be configured with as a separate RF group and mobility group, so long as the WLAN coverage is not overlapping between buildings.

Figure 2-13 WLCs Distributed



- Centralized WLC deployment—In this model, WLCs are placed at a centralized location in the enterprise network. This deployment model requires the AP/WLC LWAPP tunnels to traverse the campus backbone network. An example of a centralized WLC deployment is shown in Figure 2-14. Note in the example below that the centralized WLCs (a pair of WiSMs in Catalyst 6500's) are not shown in a specific building. A centralized WLC cluster is connected via a dedicated switch block to the campus core, which is typically located in the same building where the data center resides. The WLCs should not be connected directly to the data center's switching block because the network and security requirements of a data center are generally different then that of a WLC cluster.

Figure 2-14 WLCs Centralized



Centralizing WLCs

The general recommendation of this design guide is to deploy the WLCs at a central location within the overall campus environment. The distributed deployment model (which would require mobility groups and Layer 3 roaming) is well proven, but it is not recommended because of current shortcomings with multicast support associated with Layer 3 roaming. When these are addressed, most of the barriers preventing consideration of a distributed deployment model will be removed. Prior to Release 4.1, there were other functionality shortcomings (tunnel QoS and asymmetrical tunneling) that made distributed deployments impractical, but these have since been resolved.

The best way to address Layer 3 roaming is to avoid deployment scenarios that would otherwise necessitate it. Currently, large mobility subnets are more feasible to implement due to the scaling capabilities of the WISM module coupled with the broadcast/multicast suppression features offered by the WLC.

By centralized the WLC infrastructure, capacity management becomes simpler and more cost effective. Also, as WLANs become more mission critical, centralized deployments make it easier to create a high availability WLC topology. Centralization reduces the number of locations where capacity management and high availability issues must be dealt with.

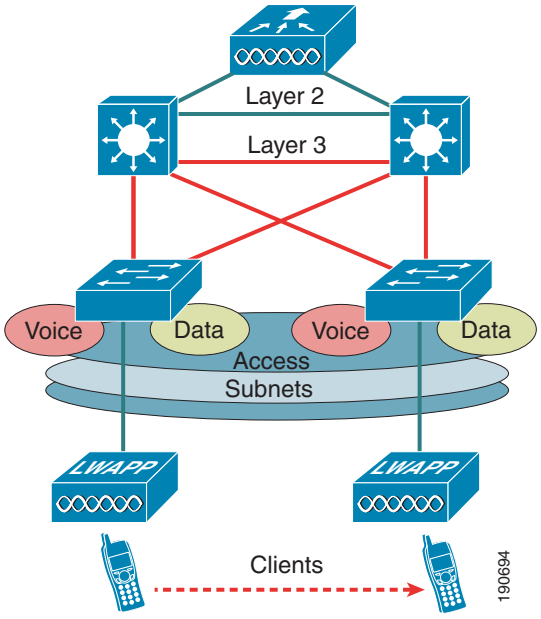
The same principle applies when integrating the WLC with other infrastructure components. Centralized WLCs minimize the number of integration points and integration devices. For example, if a decision is made to implement an inline security device such as a NAC appliance, the centralized WLC will have one integration point, whereas a distributed solution will have '*n'* integration points, where *n* equals the number of locations where WLCs are deployed.

In summary, a centralized WLC deployment is the preferred and recommended method. When planning any centralized WLC deployment, consideration must be given to the protection of the wired network infrastructure that directly connects to the WLC. The reason is because the WLC essentially attaches an 'access' network at a location within the overall enterprise topology that would not otherwise be exposed to 'access network' and its associated vulnerabilities. Therefore, all security considerations normally associated with an access layer network device must be considered. For example, in a WiSM based deployment, features such as denial-of-service protection and traffic storm protection should be considered because of the large scale role the WISM plays in providing diverse WLAN services to large numbers of end users while at the same time being directly connected to the backplane of a core multi-layer, multi-function Catalyst 6500 switching platform.

Distributed WLC Network Connectivity

As mentioned above, distributed WLCs are typically connected to the distribution layer router within the campus network. If this is the case, Cisco does *not* recommend the WLC connect to the distribution layer via a Layer 2 link, as shown in Figure 2-16.

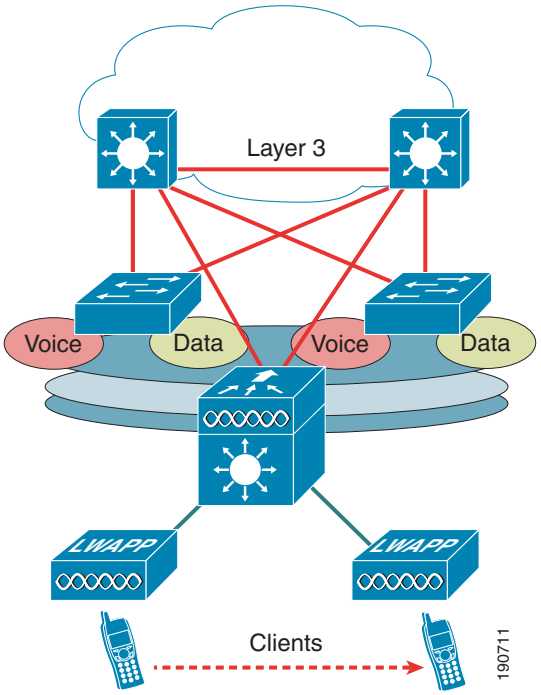
Figure 2-16 Layer 2 Connected WLC



This recommendation is made for a number of reasons, including the following:

- General best practice campus design recommends Layer 3 access and distribution connectivity to provide fast convergence and simplified operation; inserting a Layer 2 connected WLC breaks this model.
- Layer 2 WLC connectivity requires the introduction of access layer features at the distribution layer, such as HSRP, and access layer security features. This may be an issue if the distribution layer does not support all the preferred access switches, or needs to have its software version changed to support access features.
- A Layer 3 connected WLC, as shown in Figure 2-17 (in this case a 3750G), allows the WLAN-related software and configuration to be isolated to a single device and connects to the distribution layer using the same routing configuration as other the access layer routing devices.

Figure 2-17 Layer 3 Connected WLC



Traffic Load and Wired Network Performance

When deploying a Unified Wireless solution, questions often arise concerning:

- LWAPP traffic impact/load across the wired backbone.
- Minimum performance requirements to support a Unified Wireless deployment.
- Relative benefits of a distributed versus centralized WLC deployment in the context of traffic load on the network.

In examining the impact of the LWAPP traffic in relation to overall network traffic volume, there are three main points to consider:

- The volume of LWAPP control traffic—The volume of traffic associated with LWAPP control can vary depending on the actual state of the network. That is to say, it is usually higher during a software upgrade or WLC reboot situations. With that said, traffic studies have found that the

average load LWAPP control traffic places on the network is approximately 0.35 Kb/sec. In most campuses, this would be considered negligible, and would be of no consequence when considering a centralized deployment model over a distributed one.

- The overhead introduced by tunneling—A Layer 3 LWAPP tunnel adds 44 bytes to a typical IP packet to and from a WLAN client. Given that average packets sizes found on typical enterprises are approximately 300 bytes, this represents an overhead of approximately 15 percent. In most campuses, this overhead would be considered negligible, and again would be of no consequence when considering a centralized deployment model over a distributed one.
- Traffic engineering—Any WLAN traffic that is tunneled to a centralized WLC is then routed from the location of the WLC to its end destination in the network. Depending on the distance of the tunnel and location of the WLC, WLAN client traffic may not otherwise follow an optimal path to a given destination. In the case of a traditional access topology or distributed WLC deployment, client traffic enters the network at the edge and is optimally routed from that point based on destination address.

With that said, the longer tunnels and potentially inefficient traffic flows associated with a centralized deployment model can be partially mitigated by positioning the WLCs in that part of the network where most of the client traffic is destined (for example, a data center). Given the fact that most enterprise client traffic goes to servers in the data center and the enterprise backbone network is of low latency, any overhead associated with inefficient traffic flow would be negligible, and would be of no consequence when considering a centralized deployment model over a distributed one.

For most enterprises, the introduction of a WLAN does not result in the introduction of new applications, at least not immediately. Therefore, the addition of a Cisco Unified Wireless network alone is not likely to have a significant impact on campus backbone traffic volumes.

AP Connectivity

APs should be on different subnets from the end users. This is consistent with general best practice guidelines that specify that infrastructure management interfaces should be on a separate subnet from end users. Additionally, Cisco recommends that Catalyst Integrated Security Features (CISF) be enabled on the LWAPP AP switch ports to provide additional protection to the WLAN infrastructure. (H-REAP AP connectivity is discussed in Chapter 7, “Cisco Unified Wireless Hybrid REAP.”)

DHCP is generally the recommended method for AP address assignment, because it provides a simple mechanism for providing up-to-date WLC address information for ease of deployment. A static IP address can be assigned to APs, but requires more planning and individual configuration. Only APs with console ports permit static IP address configuration.

In order to effectively offer WLAN QoS within the Cisco Unified Wireless network, QoS should also be enabled throughout the ‘wired’ network that provides connectivity between LWAPP APs and the WLCs.

Operation and Maintenance

This section focuses on general deployment considerations and recommendations for easy operation and maintenance of a Cisco Unified Wireless deployment.

WLC Discovery

The different WLC discovery mechanisms for APs (discussed earlier) make initial deployment of LWAPP APs very simple. Options include:

- Staging (priming) LWAPP APs in advance using a WLC in a controlled environment
- Deploying them straight out of the box by using one of the auto discovery mechanisms (DHCP, DNS or OTP)

Although auto discovery is very useful, a network administrator will generally want to be able to control which WLC an AP will join once it is connected to the network for the first time. Subsequently then, an administrator will want to define which WLC will be the 'primary' for a given AP during normal operation in addition to configuring secondary and tertiary WLCs for backup purposes.

AP Distribution

The WLC discovery process was discussed earlier in this chapter. In a typical initial deployment, the APs will automatically distribute themselves across the available WLCs based on the load of each WLC. Although this process makes for an easy deployment, there are a number of operational reasons not to use the auto distribution method.

APs in the same physical location should be joined to the same WLC. This makes it easier for general management, operations and maintenance, allowing staff to control the impact that various operational tasks will have on a given location, and to be able to quickly associate WLAN issues with specific WLCs, whether it be roaming within a WLC, or roaming between WLCs.

The tools that are used to control AP distribution across multiple WLCs are:

- Primary, secondary, and tertiary WLC Names—Each AP can be configured with a primary, secondary, and tertiary WLC name, which in turn determine the first three WLCs in the mobility group that the AP will prefer to join, regardless of the load variations across WLCs in the mobility group.
- Master WLC—When an AP joins a WLC for the first time in the mobility group, it is not yet configured with a preferred primary, secondary, and tertiary WLC; therefore, it will be eligible to partner with any WLC (within the mobility group) depending upon the perceived WLC load. If a WLC is configured as a master WLC, all APs without primary, secondary, and tertiary WLC definitions will join with the master WLC. This allows operations staff to easily find newly joined APs and control when they go into production by defining the primary, secondary, and tertiary WLCs name parameters.

Firmware Changes

One key consideration in the operation of a Cisco Unified Wireless network is how to upgrade WLC firmware with minimal disruption to the overall WLAN network. Otherwise, a simple upgrade and reboot of a WLC can result in the loss of WLAN coverage in some locations while all the APs associated with that WLC download new software.

A better option is to migrate the APs to their secondary WLC, upgrade their primary WLC, and then migrate the APs back to the primary (upgraded) WLC in a controlled manner.

The process will vary slightly, if a deployment has been designed for high availability, in 1+1 scenario:

- APs are moved off the primary WLC to the secondary

- The primary WLC is upgraded
- All APs are then moved to the primary WLC
- The secondary WLC is upgraded
- Secondary APs are moved back to the secondary WLC.

In an N+1 scenario:

- Each WLC moves its APs to the +1 WLCs while the WLC is upgraded.
- APs are moved back to their primary WLC after it is upgraded.
- After all WLCs are upgraded, the +1 WLC is upgraded.

Note AP failback should be disabled to ensure that the APs return to their primary WLC in a controlled manner.

CHAPTER 3

WLAN Radio Frequency Design Considerations

This chapter describes the basic radio frequency (RF) information necessary to understand RF considerations in various wireless local area network (WLAN) environments. This chapter includes information on the following topics:

- Regulatory domains and frequencies
- Understanding the IEEE 802.11 standards
- RF spectrum implementations including 802.11b/g and 802.11a
- Planning for RF deployment
- Manually fine-tuning WLAN coverage
- Radio Resource Management (RRM)

RF Basics

In the United States, there are three bands allocated for unlicensed industrial, scientific, and medical (ISM) usage. These ISM bands are defined as follows:

- 900 MHz (902 to 928 MHz)
- 2.4 GHz (2.4 to 2.4835 GHz) (IEEE 802.11b/g operates in this frequency range)
- 5 GHz (5.15 to 5.35 and 5.725 to 5.825 GHz) (IEEE 802.11a operates in this frequency range)

Each range has different characteristics. The lower frequencies exhibit better range, but with limited bandwidth and thus lower data rates. The higher frequencies exhibit less range and are subject to greater attenuation from solid objects.

The following sections cover some of the specific RF characteristics used by 802.11 radios for improving communications in the 2.4 and 5 GHz frequency ranges.This section provides a summary of regulatory domains and their operating frequencies.

Regulatory Domains

Devices that operate in unlicensed bands do not require any formal licensing process, but when operating in these bands, the user is obligated to follow the government regulations for that region. The regulatory domains in different parts of the world monitor these bands according to different criteria, and the WLAN devices used in these domains must comply with the specifications of the relevant governing regulatory domain. Although the regulatory requirements do not affect the interoperability of IEEE 802.11b/g and 802.11a-compliant products, the regulatory agencies do set certain criteria in the

standard. For example, the emission requirements for WLAN to minimize the amount of interference a radio can generate or receive from another radio in the same proximity. It is the responsibility of the vendor to get the product certified from the relevant regulatory body. Table 3-1 summarizes the current regulatory domains for Wi-Fi products. The main regulatory domains are FCC, ETSI, and the MKK.

Besides following the requirements of the regulatory agencies, many vendors also ensure compatibility with other vendors through the Wi-Fi certification program (www.wi-fi.org).

Table 3-1 Regulatory Domains

Regulatory Domain	Geographic Area
Americas or FCC (United States Federal Communication Commission)	North, South, and Central America, Australia and New Zealand, various parts of Asia and Oceania
Europe or ETSI (European Telecommunications Standards Institute)	Europe (both EU and non EU countries), Middle East, Africa, various parts of Asia and Oceania
Japan (MKK)	Japan
China	People's Republic of China (Mainland China)
Israel	Israel
Singapore[1]	Singapore
Taiwan[1]	Republic of China (Taiwan)

[1] The regulations of Singapore and Taiwan for wireless LANs are particular to these countries only for operation in the 5 GHz band. Singapore and Taiwan are therefore only regulatory domains for 5 GHz operation; for operation in 2.4 GHz, they fall into the ETSI and FCC domains, respectively.

Note See the Cisco website for compliance information and also check with your local regulatory authority to find out what is permitted within your country. The information provided in Table 3-2 and Table 3-3 should be used as a general guideline.

Operating Frequencies

The 2.4 GHz band regulations have been relatively constant, given the length of time it has been operating. The FCC allows for 11 channels, ETSI allows for up to 13 channels, and Japan allows up to 14 channels, but requires a special license to operate in channel 14.

For 802.11a, countries are moving to open the frequency range 5.250–5.350 GHz (UNII-2) and the frequency range 5.470 to 5.780 GHz for additional 802.11a channels. These various frequencies are covered in more detail in the specific 802.11 sections in this chapter.

802.11b/g Operating Frequencies and Data Rates

Ratified in September 1999, the 802.11b standard operates in the 2.4 GHz spectrum and supports data rates of 1, 2, 5.5, and 11 Mbps. 802.11b enjoys broad user acceptance and vendor support. 802.11b technology has been deployed by thousands of enterprise organizations, which typically find its speed and performance acceptable for their current applications.

The 802.11g standard, which was ratified in June 2003, operates in the same spectrum as 802.11b and is backward-compatible with the 802.11b standard. 802.11g supports the additional data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

Table 3-2 lists the various 802.11b/g channel frequencies and specifies whether a regulatory agency allows their use in their domain. Note that not all of these frequencies are available for use in all regulatory domains.

Table 3-2 Operating Frequency Range for 802.11b and 802.11g

Channel Identifier	Center Frequency	FCC (America)	ESTI (EMEA)	TELEC (Japan)	MOC (Israel Outdoor)[1]
1	2412	X	X	X	
2	2417	X	X	X	
3	2422	X	X	X	
4	2427	X	X	X	
5	2432	X	X	X	X
6	2437	X	X	X	X
7	2442	X	X	X	X
8	2447	X	X	X	X
9	2452	X	X	X	X
10	2457	X	X	X	X
11	2462	X	X	X	X
12	2467		X	X	X
13	2472		X	X	X
14[2]	2484			X	

[1] Israel allows channels 1 through 13 indoors.

[2] Japan requires a special license for channel 14.

802.11a Operating Frequencies and Data Rates

Operating in the unlicensed portion of the 5 GHz radio band, 802.11a is immune to interference from devices that operate in the 2.4 GHz band, such as microwave ovens, many cordless phones, and Bluetooth (a short-range, low-speed, point-to-point, personal-area-network wireless standard). Because the 802.11a standard operates in a different frequency range, it is not compatible with existing 802.11b or 802.11g-compliant wireless devices, but it does mean that 2.4-GHz and 5-GHz equipment can operate in the same physical environment without interference.

Choosing between these two technologies (802.11b/g and 802.11a) does not involve a one-for-one trade-off. They are complementary technologies and will continue to coexist in future enterprise environments. Those responsible for implementing these technologies must be able to make an educated choice between deploying 2.4 GHz-only networks, 5 GHz-only networks, or a combination of both. Organizations with existing 802.11b networks cannot simply deploy a new 802.11a network for existing APs and expect to have their 802.11a 54 Mbps coverage in the same areas as their 11Mbps 802.11b coverage. The technical characteristics of both these bands simply do not allow for this kind of coverage interchangeability.

802.11a provides data rates of 6, 9, 12, 18, 24, 36, 48, with a maximum data rate of 54 Mbps, though generally at shorter ranges for a given power and antenna gain, but it has up to 23 nonoverlapping channels (depending on the geographic area) compared to the three nonoverlapping channels of 802.11b/g. This results in increased network capacity, improved scalability, and the ability to create microcellular deployments without interference from adjacent cells.

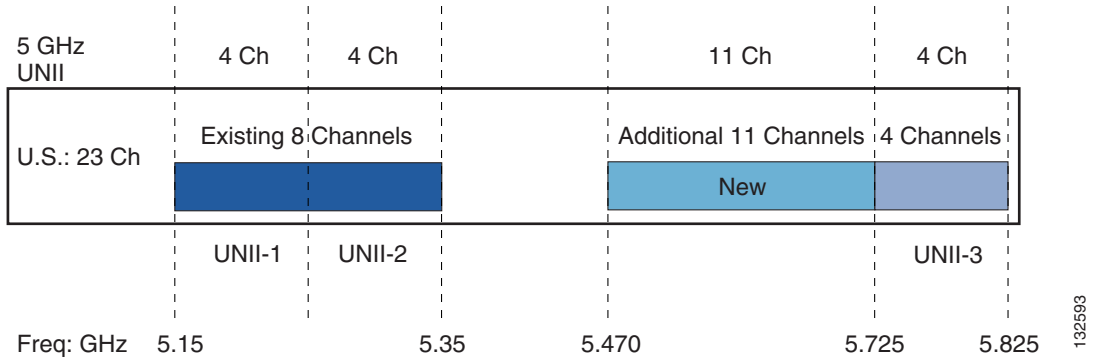
The 5 GHz band in which 802.11a operates is divided into several different sections. Each of the Unlicensed National Information Infrastructure (UNII) bands presented in Table 3-3 was originally intended for different uses, but all can currently be used by indoor 802.11a with appropriate power restrictions. Initially, the FCC defined only the UNII-1, UNII-2, and UNII-3 bands, each of which had four channels. The channels were spaced 20 MHz apart with an RF spectrum bandwidth of 20 MHz, thereby providing nonoverlapping channels.

There are differing limitations on these three UNII bands. Restrictions vary between them for transmit power, antenna gain, antenna styles, and usage. The UNII-1 band is designated for indoor operations, and initially had a restriction of permanently attached antennas. The UNII-2 band was designated for indoor or outdoor operations, and permitted external antennas**.** The UNII-3 band was intended for outdoor bridge products and permitted external antennas, but the UNII-3 band can now be used for indoor or outdoor 802.11a WLANs as well.

The channels in UNII-1 (5.150 to 5.250 GHz) are 36, 40, 44, and 48. The channels in UNII-2 (5.250-5.350 GHz) are 52, 56, 60, 64 and require Dynamic Frequency Selection (DFS) and Transmitter Power Control (TPC). The channels in the new frequency range (5.470-5.725 GHz) are 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, and 140 also require DFS and TPC. The channels in UNII-3 are 149, 153, 157, 161, 165 (5.725-5.825) and do not require DFS and TPC. Not all channels in a given range can be used in all of the regulatory domains. Figure 3-1 shows the various channels in the UNII-1, 2, and 3 bands, along with the additional 11 new channels.

In February of 2004, the FCC released a revision to the regulations covering the 5 GHz 802.11a channel usage. This revision added 11 additional channels, bringing the available channels capacity to 23 channels (see Figure 3-1).

Figure 3-1 802.11 Channel Capacity



The new additional 11 channels are for indoor/outdoor use. To use the 11 new channels, however, radios must comply with two features that are part of the 802.11h specification: TPC and DFS. DFS is required to avoid radar that operates in this frequency range, but it can also be used for other purposes, such as dynamic frequency planning. 802.11h has been supported since Cisco Unified Wireless Network Software Release 3.1.

DFS dynamically instructs a transmitter to switch to another channel whenever a particular condition (such as the presence of a radar signal) is met. Before transmitting, the DFS mechanism of a device monitors its available operating spectrum, listening for a radar signal. If a signal is detected, the channel associated with the radar signal is vacated or flagged as unavailable for use by the transmitter. The

transmitting device continuously monitors the environment for the presence of radar, both prior to and during operation. Portions of the 5 GHz band are allocated to radar systems, which allows WLANs to avoid interference with incumbent radar users in instances where they are collocated.

TPC allows the AP to negotiate power levels with a WLAN client during that association process. The AP can inform that WLAN client of the range of allowable transmit power to be used with that AP, and may reject clients unable to meet those levels. The WLAN client is able to adjust its transmit power level within the range specified in the TPC negotiations. This ensures that interference from the WLAN is minimized and allows the WLAN client to optimize battery life.

For more information on FCC regulation updates, see the following URL: http://www.cisco.com/en/US/products/hw/wireless/ps469/products_white_paper0900aecd801c4a88.shtml.

Table 3-3 shows the standard 802.11a frequencies.

Table 3-3 Operating Frequency Range for 802.11a

Channel ID	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	149	153	157	161
Center Freq. MHz	5180	5200	5220	5240	5260	5280	5300	5320	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700	5745	5765	5785	5805
Band	UNII-1				UNII-2															UNNII-3			

Table 3-4 shows the specific frequency bands and channel numbers for a few specific regulatory domains.

Table 3-4 Additional Frequency Bands and Channel Numbers for Other Regulatory Domains

Regulatory Domain	Frequency Band	Channel Number	Center Frequency
Japan	U-NII lower bands	36	5.180
		40	5.200
		44	5.220
		48	5.240
Singapore	U-NII lower band	36	5.180
		40	5.200
		44	5.220
		48	5.240
Taiwan		52	5260
		56	5280
		60	5300
		64	5320

Table 3-4 Additional Frequency Bands and Channel Numbers for Other Regulatory Domains

EMEA 1 Australia New Zealand	Same as USA	Same as USA	Same as USA
EMEA 2 [1]	U-NII lower band	36 40 44	5.180 5.200 5.220

1. Some EMEA countries, such as Denmark and Germany, are limited to 20 mW.

Understanding the IEEE 802.11 Standards

IEEE 802.11 is the working group within the Institute for Electrical and Electronics Engineers (IEEE) responsible for wireless LAN standards at the physical and link layer (Layer 1 and Layer 2) of the OSI model, as compared to the Internet Engineering Task Force (IETF, which works on network layer (Layer 3) protocols. Within the 802.11 working group are a number of task groups that are responsible for elements of the 802.11 WLAN standard. Table 3-5 summarizes some of the task group initiatives.

For more information on these working groups, see the following URL: http://www.ieee802.org/11/

Table 3-5 IEEE 802.11 Task Group Activities

Task Group	Project
MAC	To develop one common MAC for WLANs in conjunction with a physical layer entity (PHY) task group
PHY	To develop three WLAN PHYs—Infrared, 2.4 GHz FHSS, 2.4 GHz DSSS
a	To develop PHY for 5 GHz UNII band
b	To develop higher rate PHY in 2.4 GHz band
c	To cover bridge operation with 802.11 MACs (spanning tree)
d	To define physical layer requirements for 802.11 operation in other regulatory domains (countries)
e	To enhance 802.11 MAC for QoS
f	To develop recommended practices for Inter Access Point Protocol (IAPP) for multi-vendor use
g	To develop higher speed PHY extension to 802.11b (54 Mbps)
h	To enhance 802.11 MAC and 802.11a PHY-Dynamic Frequency selection (DFS), Transmit Power control (TPC)
i	To enhance 802.11 MAC security and authentication mechanisms
j	To enhance the 802.11 standard and amendments to add channel selection for 4.9 GHz and 5 GHz in Japan
k	To define RRM enhancements to provide interfaces to higher layers for radio and network measurements
k	To define Radio Resource Measurement enhancements to provide interfaces to higher layers for radio and network measurements

Table 3-5 IEEE 802.11 Task Group Activities (continued)

m	To perform editorial maintenance, corrections, improvements, clarifications, and interpretations relevant to documentation for 802.11 family specifications
n	Focus on high throughput extensions (>100MB/s at MAC SAP) in 2.4GHz and/or 5GHz bands
o	To provide Fast Handoffs in Voice over WLAN (goal is around 50ms)
p	Focus on vehicular communications protocol aimed at vehicles, such as toll collection, vehicle safety services, and commerce transactions via cars
r	To develop a standard specifying fast BSS transitions and fast roaming
s	To define a MAC and PHY for meshed networks that improves coverage with no single point of failure
t	To provide a set of performance metrics, measurement methodologies, and test conditions to enable manufacturers, test labs, service providers, and users to measure the performance of 802.11 WLAN devices and networks at the component and application level
u	To provide functionality and interface between an IEEE 802.11 access network (Hotspot) and any external network
v	To provide extensions to the 802.11 MAC/PHY to provide network management for stations (STAs)
w	To provide mechanisms that enable data integrity, data origin authenticity, replay protection, and data confidentiality for selected IEEE 802.11 management frames including but not limited to: action management frames, deauthentication and disassociation frames

Direct Sequence Spread Spectrum

Direct sequence spread spectrum (DSSS) encodes redundant information into the RF signal. This provides the 802.11 radio with a greater chance of understanding the reception of a packet, given background noise or interference on the channel. Every data bit is expanded into a string of bits, or chips, called a chipping sequence or barker sequence. The chipping rate mandated by IEEE 802.11 is 11 chips per bit. It uses binary phase-shift keying (BPSK)/quadrature phase-shift keying (QPSK) at the 1 and 2 Mbps rates and 8 chips (complimentary code keying–CCK) at the 11 and 5.5 Mbps rate. This means that at 11 Mbps, 8 bits are transmitted for every one bit of data. The chipping sequence is transmitted in parallel across the spread spectrum frequency range.

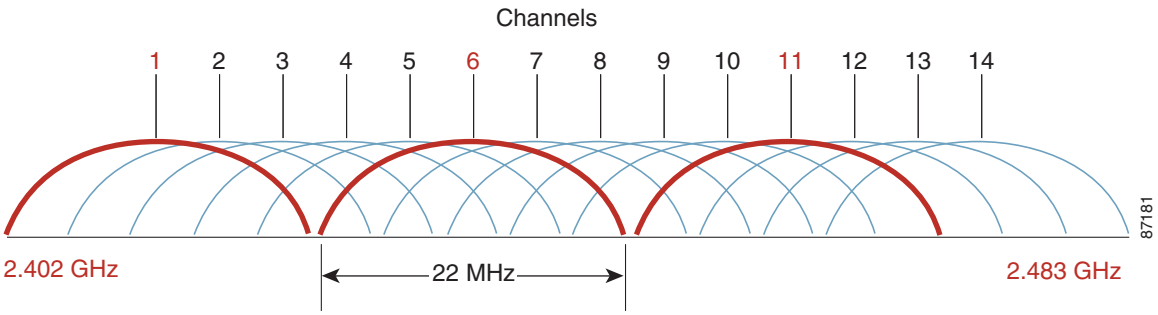
IEEE 802.11b Direct Sequence Channels

14 channels are defined in the IEEE 802.11b direct sequence (DS) channel set. Each DS channel transmitted is 22 MHz wide, but the channel separation is only 5 MHz. This leads to channel overlap such that signals from neighboring channels can interfere with each other. In a 14-channel DS system (11 usable channels in the US), only three nonoverlapping (and thus, non-interfering) channels 25 MHz apart are possible (channels 1, 6, and 11).

This channel spacing governs the use and allocation of channels in a multi-AP environment, such as an office or campus. APs are usually deployed in a cellular fashion within an enterprise, where adjacent APs are allocated nonoverlapping channels. Alternatively, APs can be co-located using channels 1, 6,

and 11 to deliver 33 Mbps bandwidth to a single area (but only 11 Mbps to a single client), if 802.11g was used in the same manner the aggregate bandwidth would be 162Mbps with a maximum data rate of 54Mbps). The channel allocation scheme is illustrated in Figure 3-2.

Figure 3-2 IEEE 802.11 DSS Channel Allocations



IEEE 802.11g

802.11g provides for a higher data rate (up to 54 Mbps) in the 2.4-GHz band, the same spectrum as 802.11b. 802.11g is backward-compatible with 802.11b and provides additional data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. At higher data rates, 802.11g uses the same modulation technique, orthogonal frequency division multiplexing (OFDM), as 802.11a (see IEEE 802.11a OFDM Physical Layer, page 3-9).

Table 3-6 lists 802.11g modulation and transmission types for the various data rates.

Table 3-6 802.11g Modulation and Transmission Types

Modulation	Transmission Type	Bits per Subchannel	Data Rate (Mbps)
BPSK	DSSS	NA	1
QPSK	DSSS	NA	2
CCK	DSSS	NA	5.5
BPSK	OFDM	125	6
BPSK	OFDM	187.5	9
CCK	DSSS	NA	11
QPSK	OFDM	250	12
QPSK	OFDM	375	18
16-QAM	OFDM	500	24
16-QAM	OFDM	750	36
64-QAM	OFDM	1000	48
64-QAM	OFDM	1125	54

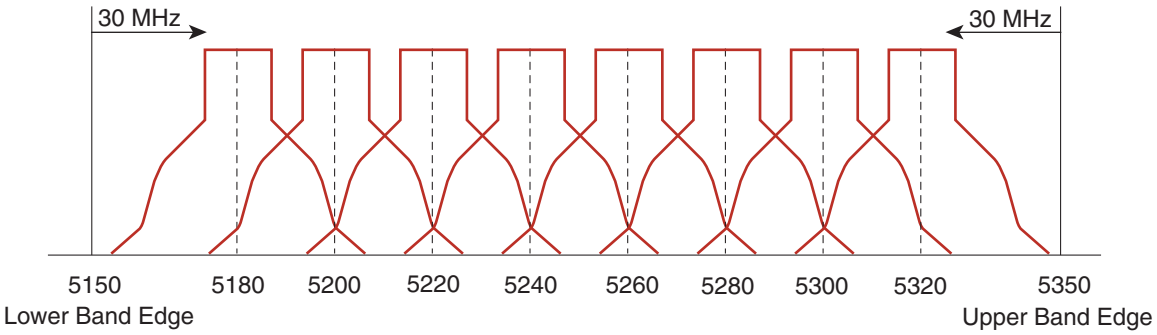
IEEE 802.11a OFDM Physical Layer

IEEE 802.11a defines requirements for the physical layer of the OSI model, operating in the 5.0 GHz UNII frequency, with data rates ranging from 6 Mbps to 54 Mbps. It uses Orthogonal Frequency Division Multiplexing (OFDM), which is a multi-carrier system (compared to single carrier systems). OFDM allows subchannels to overlap, providing a high spectral efficiency. The modulation technique allowed in OFDM is more efficient than spread spectrum techniques used with 802.11b.

IEEE 802.11a Channels

The 802.11a channel shows the center frequency of the channels. The frequency of the channel is 10 MHz on either side of the dotted line. There is 5 MHz of separation between channels, as shown in Figure 3-3.

Figure 3-3 Channel Set Example



For the US-based 802.11a standard, the 5 GHz unlicensed band covers 300 MHz of spectrum and supports 12 channels. As a result, the 5 GHz band is actually a conglomerate of three bands in the USA: 5.150-to-5.250 GHz (UNII 1), 5.250-to-5.350 GHz (UNII 2), and 5.725-to-5.875 GHz (UNII 3).

RF Power Terminology

Terms such as dB, dBi, and dBm are used to describe the amount of change in power measured at points in a system, as perceived by the radio or compared to a reference power level, respectively. The following sections cover their differences and provide a rule of thumb for their use, in addition to providing an explanation of effective isotropic radiated power (EIRP).

dB

The term *decibel* (*dB)* is mainly used for attenuation or amplification of the power level. dB is a logarithmic ratio of a signal to another standardized value. For example, dBm is where the value is being compared to 1 milliWatt, and dBw is where the value is being compared to 1 Watt.

The math is as follows:

Power (in dB) = 10 * log10 (signal/reference)

Plugging in some numbers (signal 100mW, reference 1mW) gives a value in dB of 20 (100 = 10 squared; taking the exponent 2 and multiplying by 10 gives you 20).

Remember that it is logarithmic (meaning that it increases or decreases exponentially and not linearly), and it is a ratio of some value to a reference. Also, remember that it is multiplied by 10.

Given that it is logarithmic, there are some general rules of thumb. An increase or decrease of 3 dB means that the signal doubled (double the power) or halved, respectively. An increase or decrease of 10dB means that the signal went up by 10 times or down to $1/10^{th}$ the original value.

Indoor WLAN and outdoor WLAN deployments both offer separate challenges in RF deployments, and need to be analyzed separately. However, there are some rules of thumb for indoor use. For every increase of 9dB, the indoor coverage area should double. For every decrease of 9dB, the indoor coverage area should be cut in half.

dBi

The term *dBi* is used to describe the power gain rating of antennas. The real antennas are compared to an isotropic antenna (a theoretical or imaginary antenna) that sends the same power density in all directions, thus the use of dBi.

Antennas are compared to this ideal measurement, and all FCC calculations use this measurement (dBi). For example, a Cisco omni-directional AIR-ANT4941 has a gain of 2.2 dBi, meaning that the maximum energy density of the antenna is 2.2 dB greater than an isotropic antenna.

dBm

The term *dBm* uses the same calculation as described in the dB section, but has a reference value of 1 milliWatt.

So, taking into consideration the example previously given in the dB section, if the power jumped from 1 mW to 100mW at the radio, the power level would jump from 0 dBm to 20 dBm.

Besides describing transmitter power, dBm can also describe receiver sensitivity. Receiver sensitivity is in minus dBm (-dBm), because the signal reduces in value from its point of transmission. The sensitivity indicates the lowest power the receiver can receive before it considers the signal unintelligible.

Effective Isotropic Radiated Power

Although transmitted power based on the radio setting is rated in either dBm or milliwatts, the maximum energy density coming from an antenna from a complete system is measured as effective isotropic radiated power (EIRP), which is a summation of the dB values of the various components. EIRP is the value that regulatory agencies, such as the FCC or ETSI, use to determine and measure power limits, expressed in terms of maximum energy density within the first Fresnel of the radiating antenna. EIRP is calculated by adding the transmitter power (in dBm) to antenna gain (in dBi) and subtracting any cable losses (in dB). For example, if you have a Cisco Aironet bridge connected to a solid dish antenna by a 50 foot length of coaxial cable, plugging in the numbers gives the following:

- Bridge—20 dBm
- 50 Foot Cable—3.3 dBm (negative because of cable loss)
- Dish Antenna—21 dBi
- EIRP—37.7dBm

For more information, see the following URL:
http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a00800e90fe.shtml

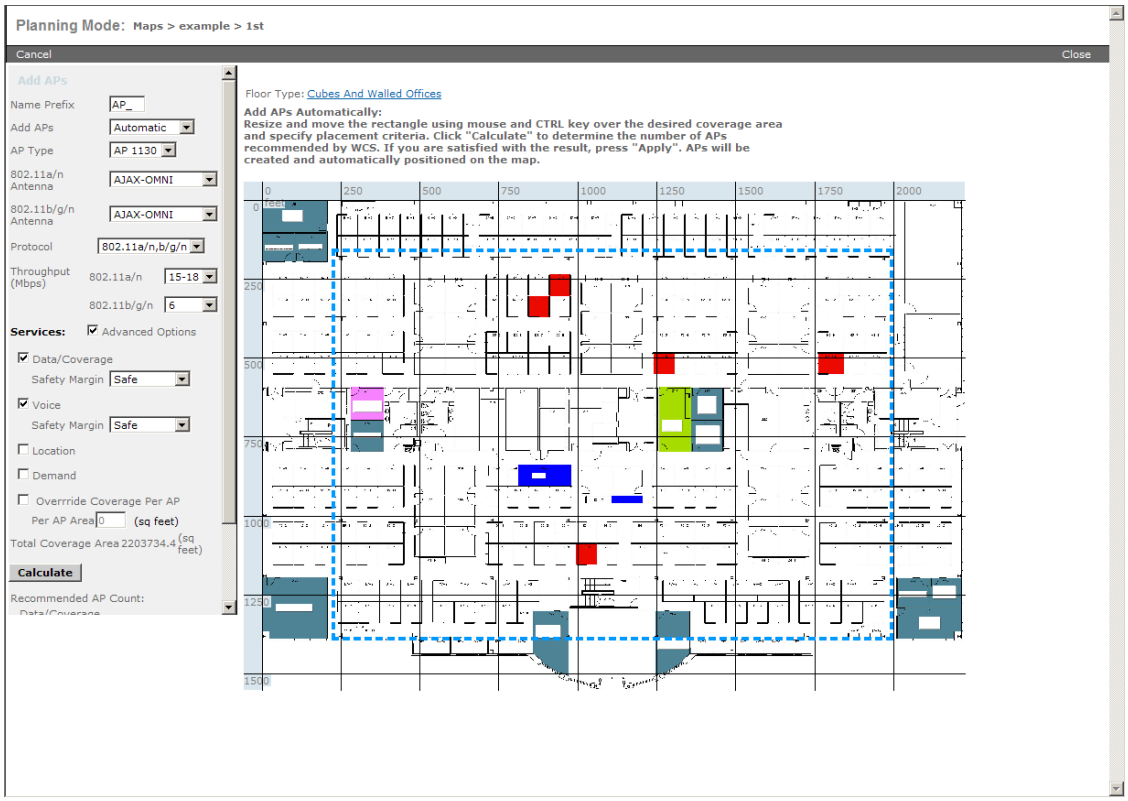
Planning for RF Deployment

Many of the RF-design considerations are interdependent or implementation-dependent. As a result, there is no “one-size-fits-all” template for the majority of requirements and environments.

Cisco Wireless Control System (WCS) provides integrated RF prediction tools that can be used to create a detailed wireless LAN design, including LWAPP AP placement, configuration, and performance/coverage estimates. IT staff can import real floor plans into Cisco WCS and assign RF characteristics to various building components to increase design accuracy.

Graphical heat maps help IT staff visualize anticipated wireless LAN behavior for easier planning and faster rollout. WCS also supports irregular shaped buildings by offering drawing tools to help organizations easily design and support WLAN deployments in such buildings. Figure 3-4 shows an example of the planning tool.

Figure 3-4 Planning Tool



Different Deployment Types of Overlapping WLAN Coverage

How much overlapping WLAN coverage you set in your wireless network depends on the usage, though with limited exceptions, all designs should be deployed to minimize retransmission and data rate shifting. Wireless networks can be deployed for location management, voice, or data-only networks, or a combination of all three. The difference is in the pattern in which the APs are laid out, and the amount of RF overlap in the coverage area. When planning a WLAN deployment consideration should be given to future uses of the WLAN deployment.

Converting a WLAN deployment to support additional services beyond a data-only deployment is not simply a matter of adding APs; it can require an additional site survey and the possible relocation of existing APs.

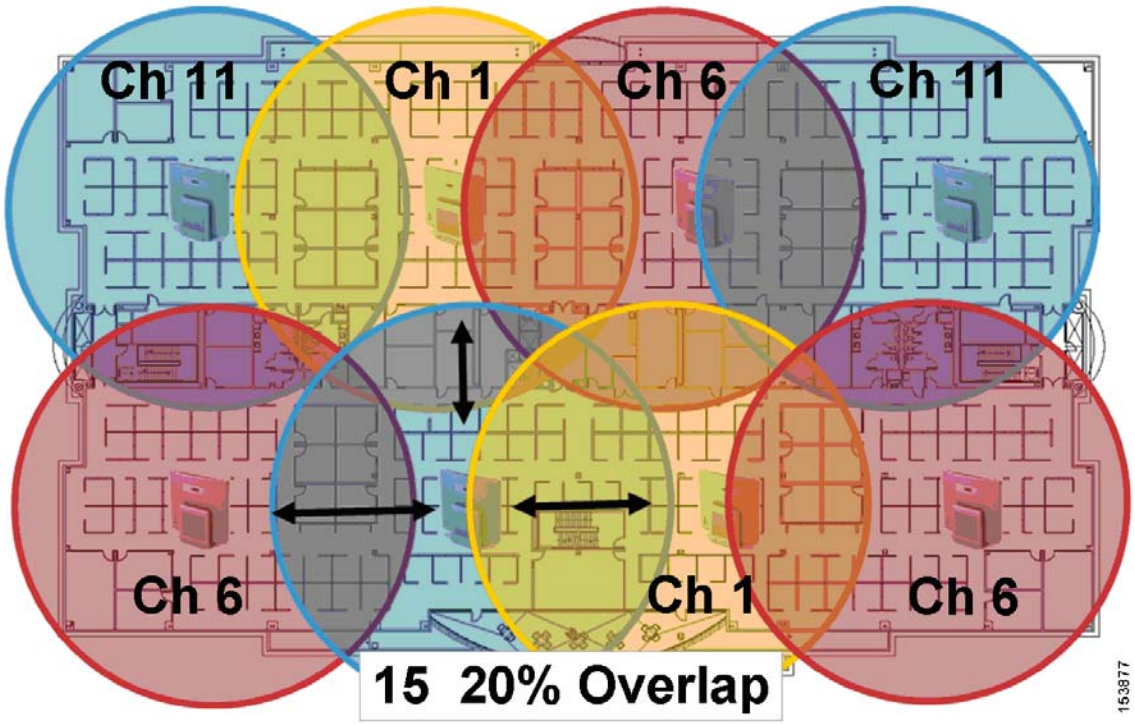
Data-Only Deployment

Data-only deployments do not require a large amount of overlap. This is because 802.11 clients respond to a lower signal from a nearby AP by stepping down their rate and taking a longer time to transmit. The required overlap is determined by the WLAN data rate requirement described in WLAN Data Rate Requirements, page 3-16. For data-only networks, the rule of thumb for separation of APs is typically 120–130 feet, but, when making your estimation for AP separation, remember to factor in objects that affect RF coverage, such as wall densities, machinery, elevators, or even wide-open space with steel cages, because your results can vary depending on the RF environment. RRM has been developed for this type of deployment and it is very useful for controlling the RF coverage.

Voice/Deployment

Figure 3-5 shows the voice network pattern and overlap.

Figure 3-5 Single Floor Site Survey for Voice



The APs are grouped closer together and have more overlap than a data-only installation, because voice clients should roam to a better AP before dropping packets. You generally also want to run smaller cells than in the past, and ensure the overlapping cell edges at or above -67 dBm. This accomplishes a number of things including greater homogeneity across a single cell and reducing processor load in the handheld, which increases link stability and reduces latency. Although only one AP might be required for a defined area, Cisco recommends that you have two APs on nonoverlapping channels with a received signal strength indication (RSSI) above 35 at all times in your installation, for redundancy and load balancing purposes. For the 7920 voice deployment, Cisco recommends that you have a Received Signal Strength Indication (RSSI) above 35 at all time in your installation. This is to ensure that the VoIP phone has good reception as well as allowing some over-subscription and enhances roaming choices for the phone.

Remember that designing for low noise background is as important as relatively high energy density within the cell. This means that a good baseline power setting for the AP is in the 35–50 mW range. This generally requires approximately 15 percent more APs than if you deployed a coverage model at 100 mW.

Pre-site surveys are useful for identifying and characterizing certain challenging areas and potential sources for interference, such as existing WLANs, rogues, and non-802.11 interference from sources such as microwave ovens and many cordless telephones. Following a design that should be reviewed and approved by all stakeholders, post-site surveys should be considered as an excellent audit mechanism to ensure that the coverage model complies with the intended functional requirements as set forth by the stakeholders.

When making your estimation for separation, remember to factor in objects that affect RF coverage such as wall densities, machinery, elevators, or even wide open spaces with steel cages, because your results may vary depending on the RF environment. Be sure to include transient dynamics such as forklifts, large groups of people, or large objects moved through the area by crane or similar load bearing devices. A WLC is often a very effective method for preliminary site evaluation, by allowing a fast deployment of a WLAN infrastructure that can then be used to make RF measurements of the area; a hand-walked site survey is also effective insurance for complex areas such as those commonly found in healthcare, retail, and manufacturing.

For more information on a wireless voice deployment, see Chapter 9, "VoWLAN Design Recommendations," as well as the 7920 deployment guide at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7920/5_0/english/design/guide/7920ddg.html

Location-Based Services Deployments

The third type of deployment is the location-based services (LBS) deployments, which may be the most complex of current applications because it relies not only on excellent cell coverage, but optimal location of APs. Location management deployments can simultaneously track thousands of devices by using the WLAN infrastructure. Examples include Wi-Fi tag type deployments or asset tracking deployments to locate equipment or devices via the wireless network and/or simply to indicate where wireless clients are throughout the wireless network in relation to a drawing or diagram. This can be used to make the wireless infrastructure more secure by providing the location of a rogue client or APs, and greatly improve client troubleshooting capabilities.

For a location management deployment, the APs are laid out in a staggered pattern. Figure 3-6 shows a typical pattern. The staggered pattern allows for more accurate estimation of the location of a device.

Figure 3-6 Example of a Single Floor Location Management Deployment

For a discussion of location-based services, see Chapter 13, "Cisco Unified Wireless Location-Based Services," and the whitepaper entitled *Wi-Fi Location Based Services 4.1 Design Guide*, which can be found at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/wifich1.html.

The Cisco 7921G and the Cisco 7920 are Cisco VoWLAN handsets. Their use is one of the most common reasons for deploying QoS on a WLAN.

For more information on the 7920 and 7921G handsets, see the following:

- Cisco Unified Wireless IP Phone 7921G Version 1.0(2)

  http://www.cisco.com/en/US/products/hw/phones/ps379/products_data_sheet0900aecd805e315d.html

- Cisco Unified Wireless IP Phone 7920 Version 3.0

  http://www.cisco.com/en/US/products/hw/phones/ps379/products_data_sheet09186a00801739bb.html

- Deploying VoWLAN infrastructure involves more than simply providing QoS on WLAN. A voice WLAN needs to consider site survey coverage requirements, user behavior, roaming requirements, and admission control. These are covered in the following guides:

  – Design Principles for Voice Over WLAN

    http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/net_implementation_white_paper0900aecd804f1a46.html

  – Cisco Unified Wireless IP Phone 7921G Adminstration Guide

    http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7921g/5_0_1/english/administration/guide/21adm501.html

- Cisco Wireless IP Phone 7920 Design and Deployment Guide

  http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7920/5_0/english/design/guide/7920ddg.html

WLAN Data Rate Requirements

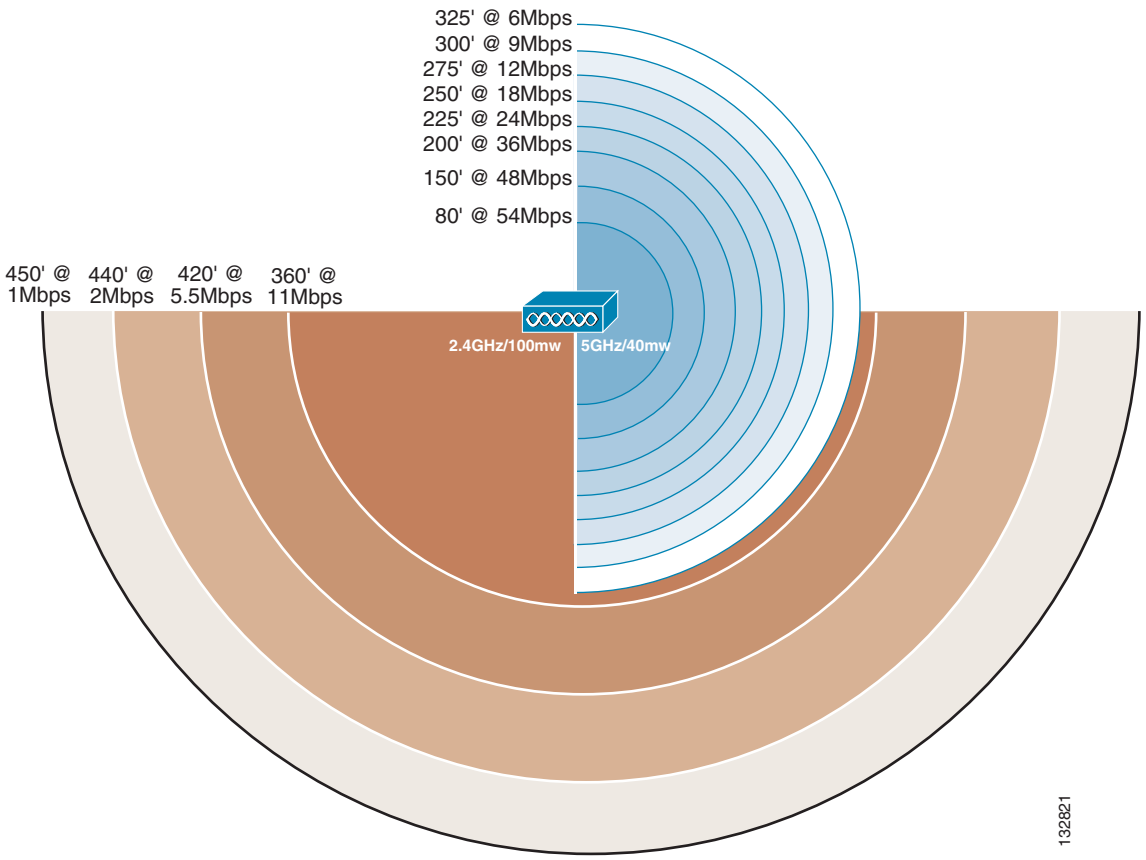
Data rates affect AP coverage areas. Lower data rates (such as 1 Mbps) can extend the coverage area farther from the AP than higher data rates (such as 54 Mbps) as illustrated in Figure 3-7 (which is not drawn to scale). Therefore, the data rate (and power level) affects coverage and consequently the number of APs required for the installation, as illustrated in Figure 3-8 for different data rates. As part of the planning process, consider the required data rates, the required range, and the required reliability.

Data Rate Compared to Coverage Area

Different data rates are achieved by the AP using different encoding techniques on the wireless link, allowing data to be more easily recovered from noise; this can be seen in the different receiver sensitivities for the different data rates. The number of symbols, or chips, sent out for a packet at the 1 Mbps data rate is greater than the number of symbols used for the same packet at 11 Mbps. This means that sending data at the lower bit rates takes more time than sending the equivalent data at a higher bit rate. And when there is more than one client associated to the radio, the lower rate client affects the higher rate clients' maximum data throughput by taking longer to transmit a packet of the same length.

The actual diameter of the coverage, as shown in Figure 3-7, depends on factors such as environment, power level, and antenna gain.

Figure 3-7 Data Rate Compared with Coverage

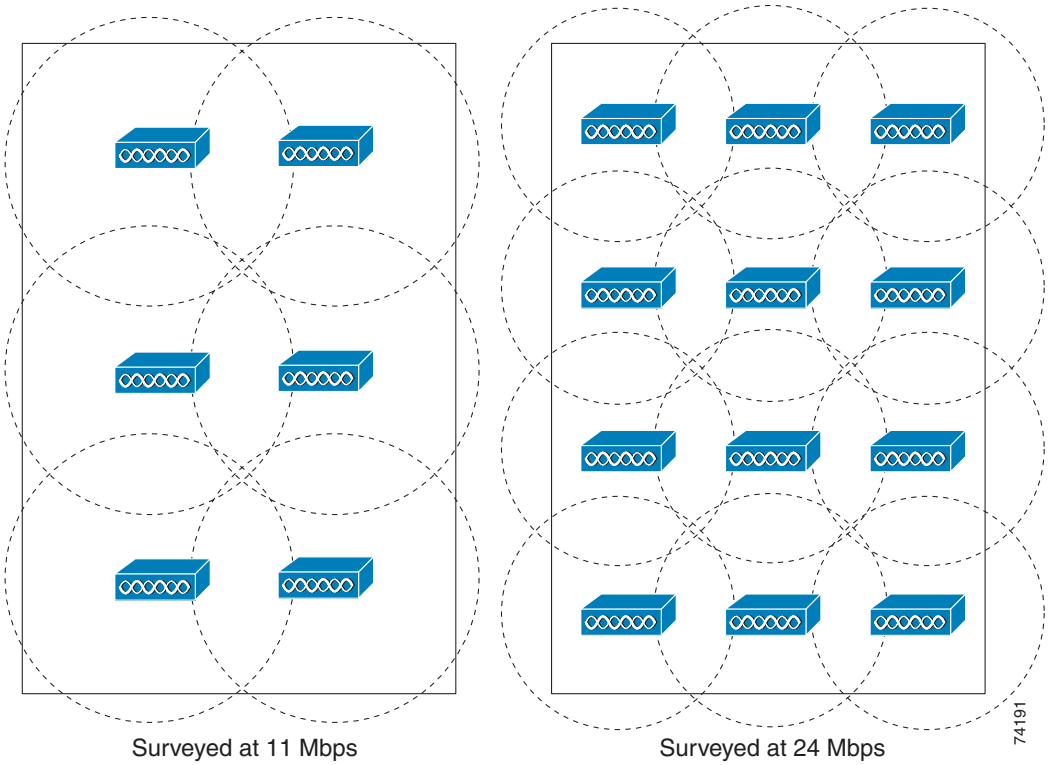


For example, indoors using the standard antennas on the NIC card and APs, the diameter of the 1 Mbps circle is approximately 700 feet (210 m), and the diameter of the 11 Mbps circle is about 200 feet (60 m). This does depend upon the type of indoor environment. An open office plan building is different from one with offices and solid walls. Increasing the gain of the antenna can increase the distance and change the shape of the radiation pattern to be focused in specific directions rather than being radiated evenly.

AP Density for Different Data Rates

The minimum required reliable data rate has a direct impact upon the number of APs needed in the design, along with power setting, antenna gain, and location. Figure 3-8 shows coverage comparison and AP density for different data rates. Although six APs with a minimum data rate of 11 Mbps might adequately service an area, it might take twice as many APs to support a minimum data rate of 24 Mbps, and more again to support a minimum data rate of 48 Mbps for the same coverage area.

Figure 3-8 Coverage Comparison and AP Density for Different Data Rates



The data rate you choose depends on the type of application to be supported, but should not be greater than the typical requirements because there is trade-off in coverage. In a typical WLAN environment, the higher data rates give maximum throughput and should minimize performance-related support issues. The physical facility and/or whether the network is client-centric generally dictates range requirements; some clients might not support the higher data rates, longer ranges, or the delay and jitter rates of an infrastructure element such as an AP.

It might seem logical to choose the default configuration of APs and clients, thereby allowing all data rates. However, there are three key reasons for limiting the data rate to the *highest* rate at which full coverage is obtained:

- Broadcast and multicast (if enabled) are sent at the lowest associated data rate (to ensure that all clients can receive the packets). This reduces the throughput of the WLAN because traffic must wait until frames are processed at the slower rate.
- Clients that are farther away, and therefore accessing the network at a lower data rate, decrease the overall throughput by causing delays while the lower bit rates are being serviced. It might be better to force the clients to roam to a closer AP so as not to impact the performance of the rest of the network.
- If a 54 Mbps service is specified and provisioned with APs to support *all* data rates (for example), clients at lower rates can associate with the APs that can create a coverage area greater than planned, thereby increasing the security exposure (by allowing association from outside the building) and potentially interfering with other WLANs.

Client Density and Throughput Requirements

Wireless APs have two characteristics that make actual client data throughput slower than the data rate:

- APs have an aggregate throughput less than the data rate because 802.11 provides a reliable transport mechanism that ACKs all packets, thereby halving the throughput on the channel.
- APs are similar to shared hubs. That is, the channel is shared by all the clients associated to that AP on that channel, thus collisions slow data throughput.

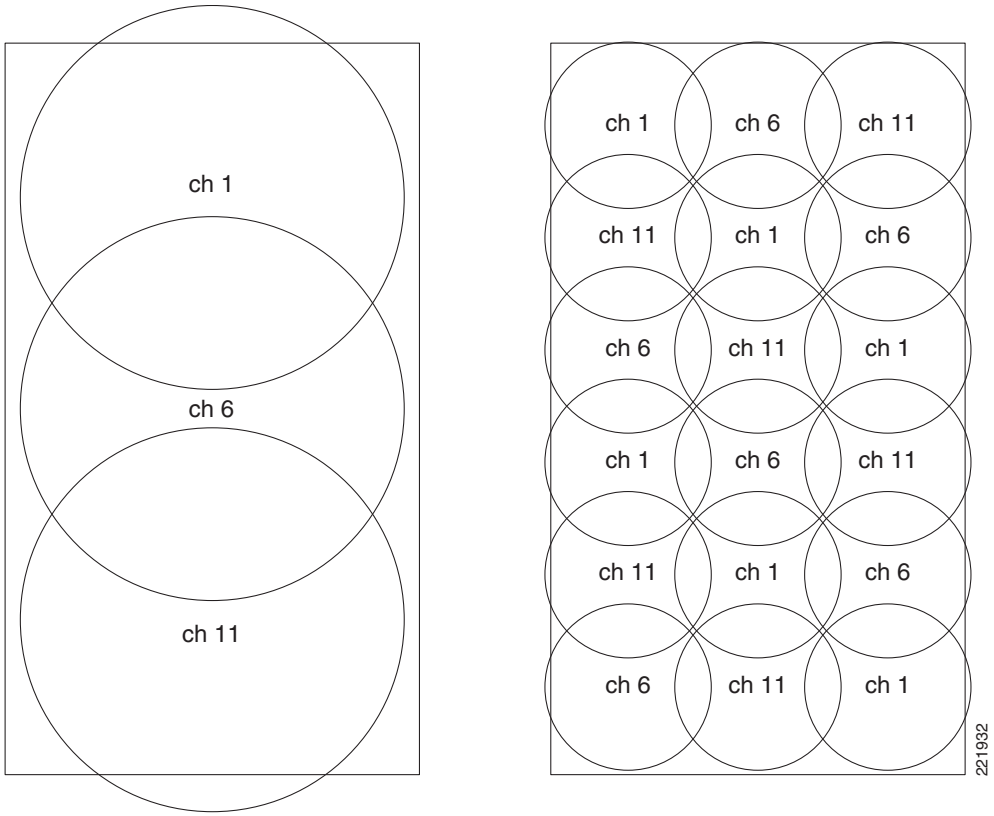
With this in mind, you must have an estimate of the maximum number of active associations (active clients). This can be adjusted more or less according to the particular application.

Each cell provides an aggregate amount of throughput that is shared by all the client devices that are within the cell and associated to a given AP. This basically defines a cell as a collision domain. After deciding on the minimum data rate, be sure to consider how much throughput should, on average, be provided to each user of the wireless LAN.

Take the example of a simple barcode scanning application; 25 Kbps may be more than sufficient bandwidth for such an application because using an 802.11b AP at 11 Mbps of data rate results in an aggregate throughput of 5–6 Mbps. A simple division results in a maximum number of 200 users that can theoretically be supported. This number cannot in fact be achieved because of the 802.11 management overhead associated with the large number of clients and packet collisions. For a 1 Mbps system, 20 users can use the same AP for similar bandwidth results.

You can increase the potential per-user throughput by decreasing the number of users contending for the aggregate throughput provided by a single AP. This can be done by decreasing the size of the coverage area, or adding a second AP on a non-overlapping channel in the same coverage area. To reduce the coverage area, the AP power or antenna gain can be reduced, resulting in fewer clients in that coverage area. This means you need more APs for the same overall area, increasing the cost of deployment. An example of this is shown in Figure 3-9.

Figure 3-9 Changing the Output Power to Increase Client Performance



180 Users per floor
30 mW transmitter power
3 Accss Points
60 users per AP
11 Mbps data rate

180 Users per floor
5 mW transmitter power
18 Accss Points
10 users per AP
11 Mbps data rate

Note Client power should be adjusted to match the AP power settings. Maintaining a higher setting on the client does not result in higher performance and it can cause interference in nearby cells.

WLAN Coverage Requirements

Different enterprises have different coverage requirements. Some need a WLAN to cover specific common areas, while others need WLANs to cover each floor of a building or to cover the entire building including stairwells and elevators, or to cover the entire campus including car parks and roads. Apart from impacting the number of APs required, the coverage requirements can introduce other requirements, such as specialized antennas, outdoor enclosures, and lightning protection.

Power Level and Antenna Choice

Power level and antenna choice go hand-in-hand to determine AP placement. Together, these two variables determine where and how powerful the RF is in any given place in the environment. Along with choosing the correct antenna to produce the required coverage area, Cisco recommends the use of RRM to control the power level and provide the optimal channel/power plan. For more information, see Radio Resource Management (Auto-RF), page 3-30.

An antenna gives the wireless system three fundamental properties:

- Gain—A measure of increase in power introduced by the antenna, over a theoretical antenna that transmits the RF energy equally in all directions.
- Direction—The shape of the antenna transmission pattern. Different antenna types have different radiation patterns that provide various amounts of gain in different directions.
- Polarization—Indicates the direction of the electric field. An RF signal has both an electric and magnetic field. If the electric field is orientated vertically, the wave is said to be vertically polarized.

A good analogy for an antenna is the reflector in a flashlight. The reflector concentrates and intensifies the light beam in a particular direction similar to what a parabolic dish antenna does to an RF source in a radio system.

Gain and direction mandate range, speed, and reliability; polarization affects reliability and isolation of noise.

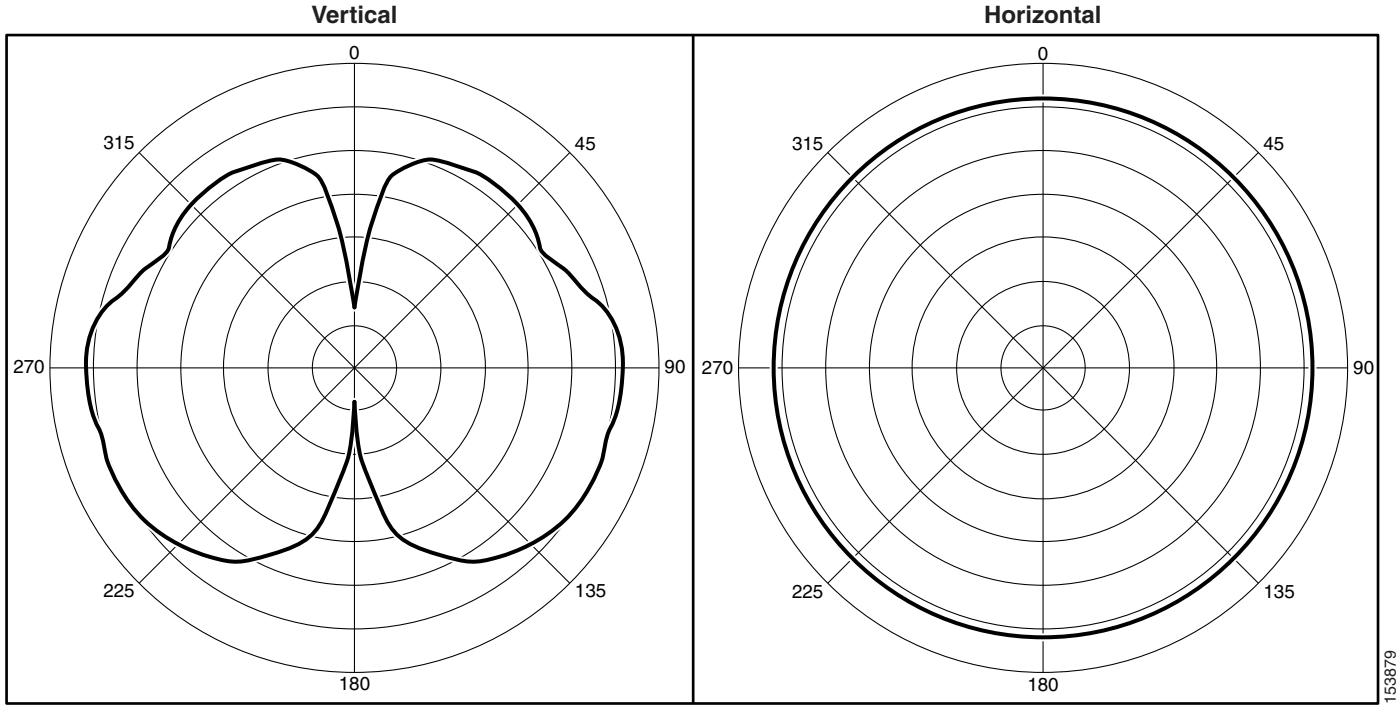
Omni-Directional Antennas

Omni-directional antennas have a different radiation pattern compared to isotropic antennas; the isotropic antenna is theoretical and all physical antennas are different to the isotropic antenna. The omni-directional antenna features a radiation pattern that is nearly symmetric about a 360 degree axis in the horizontal plane, and 75 degrees in the vertical plane (assuming the dipole antenna is standing vertically). The radiation pattern of an omni-directional antenna generally resembles a donut in shape.

Regarding antenna choice, you must consider the RF pattern produced by the antenna because the type of antenna (omni or directional) affects RF coverage by focusing the bulk of the RF energy in a specific direction, pattern, and density.

For example, the omni-directional antenna shown in Figure 3-10 shows an omni-directional antenna RF radiation pattern in the vertical and horizontal direction. This is an actual measurement, so it does not follow the donut lines perfectly, but does show from where this shape comes. As described above, other RF-affecting variables (people in the room, amount of devices stored in the facility, leaves on trees for outdoor deployment, interference from different RF sources, and so on) may affect the real RF coverage pattern.

Figure 3-10 Omni-Directional RF Pattern

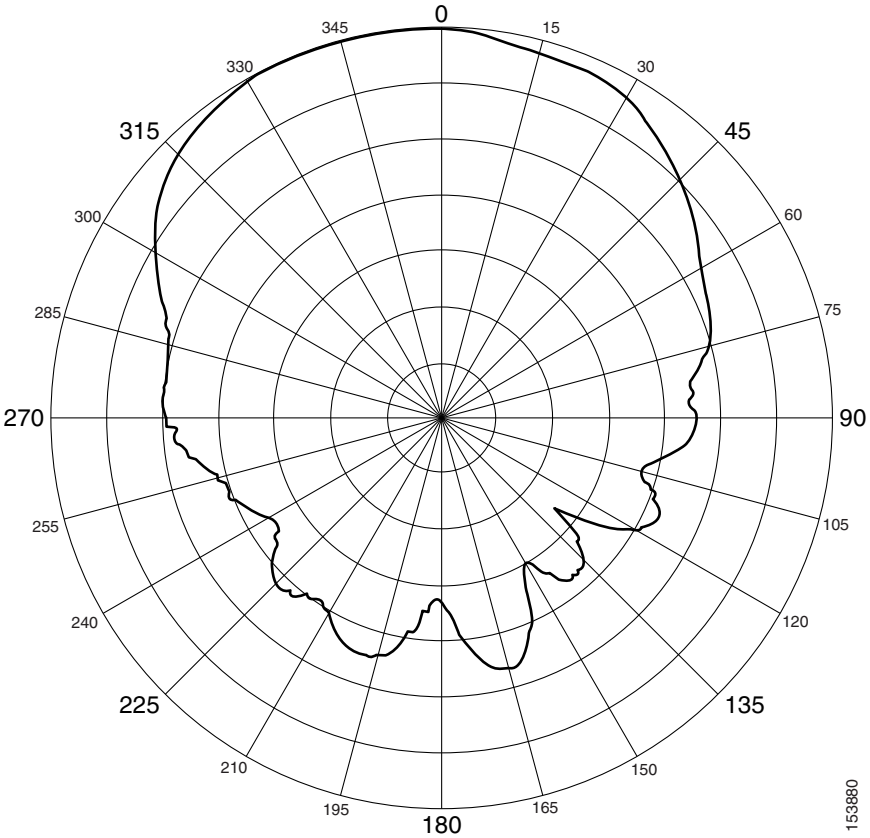


Looking at the pattern in Figure 3-10, this may be the incorrect antenna to use on a wall, especially if it is mounted along an exterior wall where the pattern can radiate outside of the building. This can open up the wireless network to hackers outside the building and compromise the wireless network.

Patch Antennas

The patch antenna is a type of directional antenna. Patch antennas not only radiate away from the wall or place where they are mounted, but also have rear and side lobes that produce a weakened but still potentially useful RF region. Figure 3-11 shows the real horizontal pattern of a diversity patch wall mount antenna. Although most of the coverage area is in front of the patch antenna, notice the back and side RF pattern from the center area. Again, antenna selection is important because it defines the radiation pattern and where wireless connectivity is possible.

Figure 3-11 Patch Wall Mount Antenna Horizontal Plane



For more information on antenna selection, see the *Cisco Antenna Selection Guide* at the following URL:

http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html

Security Policy Requirements

A good RF design can effectively minimize unintended RF radiation in areas not requiring coverage. For example, if WLAN coverage is required only in buildings and not outside, then the amount of RF coverage outside of the buildings can be minimized by using the correct power setting, AP placement and directional antennas pointing inwards towards the center of the building or areas. By tuning RF transmit levels and using the correct antenna for the coverage area, you can reduce the amount of RF that radiates outside the buildings to decrease the security exposure. This can reduce the exposure of wireless network to hackers outside the building or coverage area, and avoid a compromise of the wireless network.

RF Environment

The performance of the WLAN and its equipment depends on its RF environment, equipment, selection, coverage design, quality of audits, configurations, and quality of deployment. The following are some examples of adverse environmental variables that can disrupt wireless communications by either providing interference on the channel or in some way changing the RF characteristics of the signal:

- 2.4 GHz cordless phones
- Walls fabricated from wire mesh and stucco
- Filing cabinets and metal equipment racks
- Transformers
- Heavy duty electric motors
- Fire walls and fire doors
- Concrete
- Refrigerators
- Sulphur plasma lighting (Fusion 2.4 GHz lighting systems)
- Air conditioning duct-work
- Other radio equipment
- Microwave ovens
- HVAC ducting
- Large transient elements such as forklifts or metal fabrications
- Other WLAN equipment

A site survey might be required to ensure that the required data rates are supported in all of the required areas, often driven by the environmental variables mentioned above, although a WLC is an excellent resource for site pre-planning and initial identification of RF challenges as well as channel and power settings.

RF Deployment Best Practices

Some design considerations can be addressed by general best practice guidelines. The following applies to most situations:

- The number of users versus throughput and a given AP. A common recommended number of users per AP is 15 to 25 for data-only users only and, for the 7920 VoIP (or similar voice devices) wireless handset, 7 to 8 voice users when data is present. This number should be used as a guideline and may vary depending on the handset in use. Check your handset requirements.
- The AP data rates should be limited to those designed and for which the site survey was performed. Enabling lower data rates can cause increases in co-channel interference and greater throughput variations for clients.
- The number of APs depends on coverage and throughput requirements, which can vary. For example, Cisco System's internal information systems (IS) group currently uses six APs per 38,000 square feet of floor space for data-only operation.

Note Based on the variability in environments, Cisco recommends that a site survey be performed to determine the number of APs required and their optimal placement.

Manually Fine-Tuning WLAN Coverage

A number of factors can affect the WLAN coverage, as follows:

- Channel and data rate selection
- Overlapping WLAN coverage for location management, voice, or data-only
- Power level
- Antenna choice (omni-directional, or directional antenna)

For a given data rate and location, the WLAN designer may alter power levels and/or elect to use a different antenna, to effect changes to the coverage area and/or coverage shape. Altering power levels or channel selection can be done manually as described below, or the Cisco Wireless Controller can do this automatically via the Radio Resource Management (RRM) algorithms, also referred to as Auto-RF. Cisco recommends the use of Radio Resource Management (RRM) to control the power level and channel, keeping in mind that the channel changing algorithm is highly dampened so that only a very disruptive (and persistent) interference source would cause a change to the channel topology, which in turn would cause clients to reassociate and any voice calls to be dropped. Changes in AP power do not impact clients. (See Radio Resource Management (Auto-RF), page 3-30 for more details).

Channel and Data Rate Selection

Channel selection depends on the frequencies that are permitted for a particular region. For example, the North American and ETSI 2.4 GHz channel sets permit allocation of three nonoverlapping channels: 1, 6, and 11 while the 5 GHz channel set permits 23 channels.

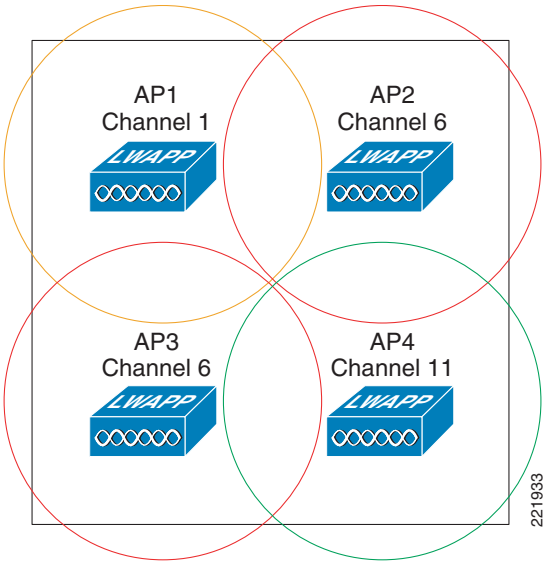
The channels should be allocated to the coverage cells as follows:

- Overlapping cells should use nonoverlapping channels.
- Where channels must be re-used in multiple cells, those cells should have minimal overlap with each other. Figure 3-12 shows this pattern. In 802.11a deployments, adjacent channels should be avoided as overlapping cells.

Recommendations for Channel Selection

Channel selection can be done manually, as described below.

Figure 3-12 Channel Allocated To APs



A site survey should be conducted using the same frequency plan as intended for the actual deployment. Some sites have high noise backgrounds which may prohibit the use of one or more channels. This provides a better estimate of how a particular channel at a particular location will react to the interference and the multipath. Channel selection also helps in planning for co-channel and the adjacent channel interference, and provides information about where you can reuse a frequency (see Figure 3-13).

In multi-story buildings, check the cell overlap between floors, especially where windows may be located, according to these rules/guidelines. Careful pre-planning and selection of AP location might be required in approximately 10 percent of the cases. Multi-story structures such as office towers, hospitals, and university classroom buildings introduce a third dimension to coverage planning. The 2.4 GHz waveform of 802.11b and 802.11g can pass through many walls. The 5 GHz waveform of 802.11a has approximately half the tendency for a given power to transmit suitable amounts of energy through walls because of its higher frequency. With 2.4 GHz Wi-Fi LANs in particular, you must not only avoid overlapping cells on the same floor, but also on adjacent floors when coverage models include cells that cover windows on both floors. With only three channels, this can be achieved through careful three-dimensional planning.

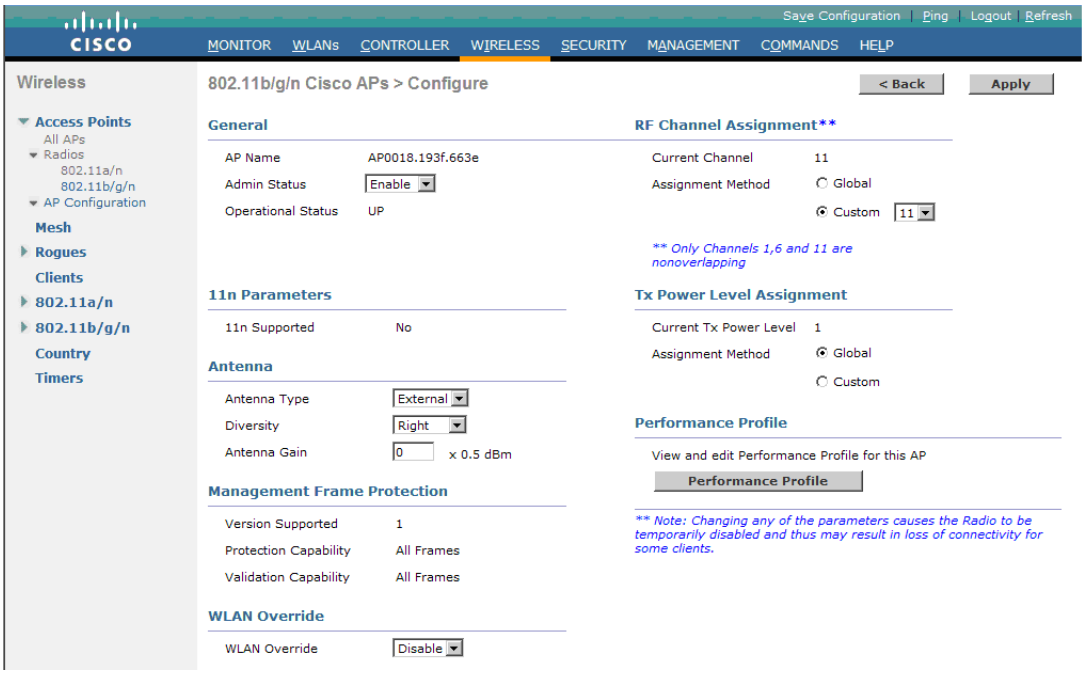
As a final step, after setting up the WLAN network, you should always retest the site using the selected channels and check for any interference. Keep in mind that the RRM algorithms are logical and subject to the physical topology of the network. It thus takes into account the three-dimensional placement of APs and provides the optimal channel/power setting for the sampling interval.

Manual Channel Selection

Figure 3-13 shows a screenshot of the web page for configuring one of the 802.11b/g radios under the wireless selection. On the top right-hand side, channel 11 has been manually selected and the transmit power is set to 1, the highest level (8 sets the AP to the lowest level).

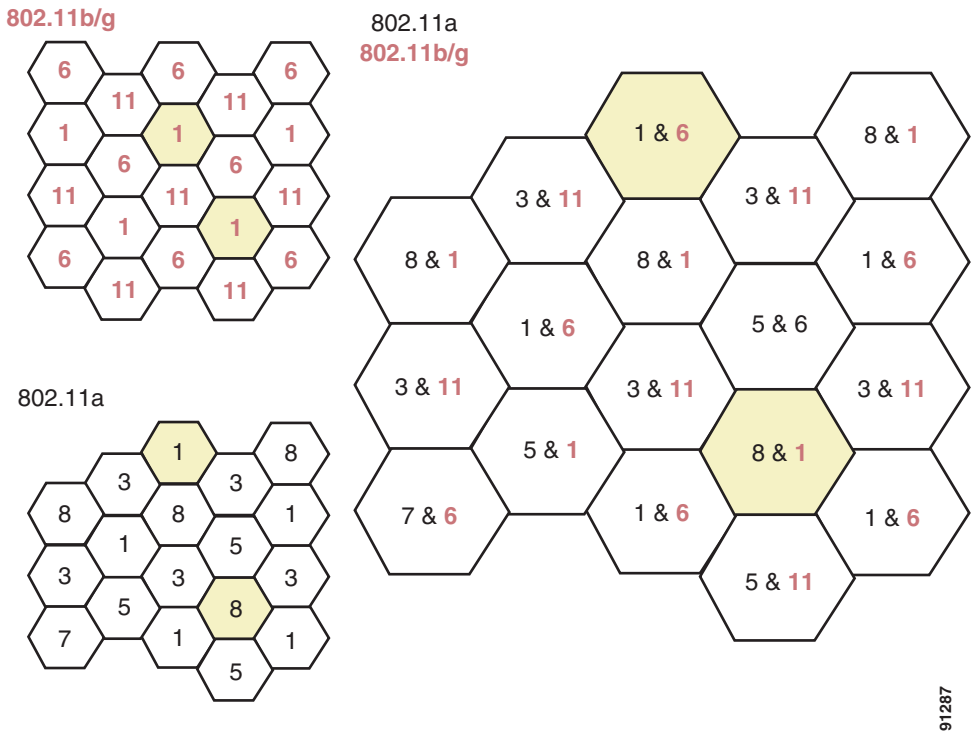
Note The assignment method should normally be left at the global setting, unless there is a desire to manually control these settings. This allows the controller to dynamically change the channel number and transmit power as determined by the RRM. See Radio Resource Management (Auto-RF), page 3-30 for more information.

Figure 3-13 Channel Assignment



It is also possible to implement a dual-band deployment scheme, as shown in Figure 3-14. The top left portion of the diagram shows the 802.11b/g-only deployment, which uses the three nonoverlapping channels (channels 1, 6, and 11) to map out a pattern that has the least co-channel interference; that is, interference from an AP close by that is on the same channel, that is operating at sufficient power levels with its coverage pattern overlapping with that of another access point. It also shows an 802.11a deployment, which uses the eight nonoverlapping channels. The right side of the diagram illustrates how the channels would be mapped in a dual-band deployment.

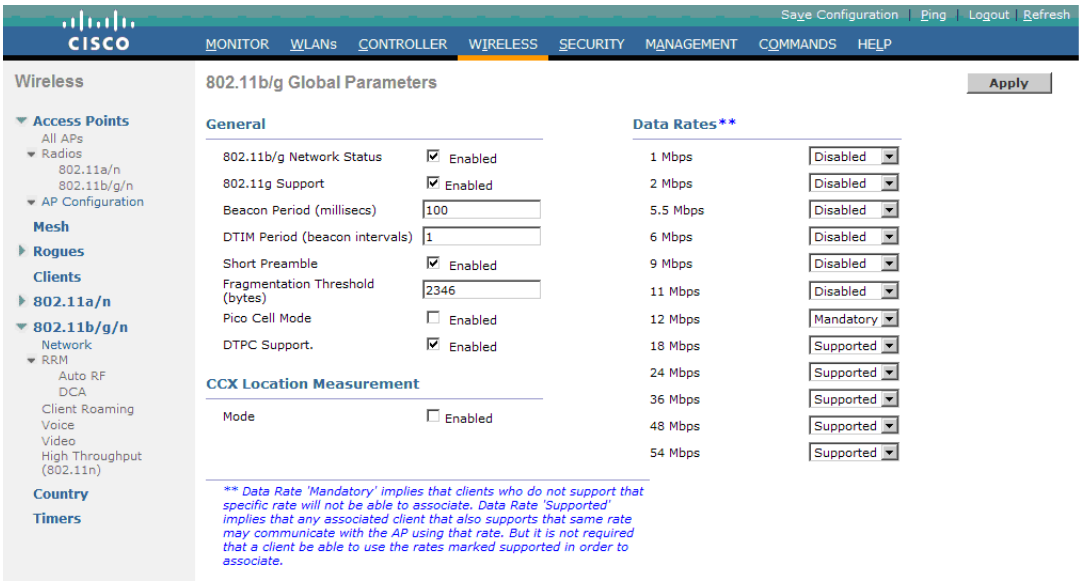
Figure 3-14 Dual Band Deployment Diagram



Data Rate Selection

Figure 3-15 is a screenshot of the web page of the global 802.11b/g parameters. The data rate settings are shown on the right side of the screen.

Figure 3-15 Data Rate Assignment



Mandatory, Supported, and Disabled Rate Modes

You can use the data rate settings to choose which data rates the wireless device can use for data transmission. There is a direct correlation between data rates, range, and reliability. The lower the data rate, the greater the reliability and range for a given power setting. Sites vary for specifics, but a reasonable rule of thumb for carpeted space is an order of magnitude of increased reliability for every time you halve the data rate. Range is generally affected by a factor of a 30 percent increase (approximately) for every halving of data rate. Managing the square footage of the area covered within a -67 dBm edge can be effectively managed using this technique. Setting the data rates to match client, application, or user needs is an effective RF design element that should be considered before deploying APs.

Data rates are expressed in megabits per second. You can set each data rate to one of three modes:

- Mandatory—Allows transmission at this rate for all packets, both unicast and multicast. The data rate on at least one of the APs must be set to Mandatory, and all clients that associate to the AP must be able to physically support this data rate on their radio to use the network. Additionally, for the wireless clients to associate to the AP, they must be able to currently receive packets at the lowest mandatory rate and their radios must physically support the highest mandatory data rate. If more than one data rate is set to mandatory, multicast and broadcast frames are sent at the highest common mandatory transmission rate of all associated clients (the lowest mandatory receive rate of all of the clients). This allows all clients to receive broadcast packets. The lowest mandatory rate is normally set at 1 Mb/s.
- Supported—Allows transmission at this rate for unicast packets only. The AP transmits only unicast packets at this rate; multicast and broadcast packets are transmitted at one of the data rates set to mandatory. The wireless clients always attempt to transmit and receive at the highest possible data rate. They negotiate with the AP for the highest data rate set to supported or mandatory to transmit and receive unicast packets. The wireless client devices are able to receive broadcast or multicast packets at any mandatory rate at or below the negotiated rate.
- Disabled—The AP does not transmit data at this rate.

Lowest and Highest Mandatory Rate Settings

Multiple clients associated to the AP can have different transmission rates, depending on interference, obstacles, or their distance from the AP. For example, if an 802.11b client is far from the AP and can only transmit and receive at a speed of 1 Mb/s because of the distance, it would be able to associate to the AP because the lowest mandatory rate (see Figure 3-15) is set to 1 Mb/s. If a second 802.11g client associates to the AP at 54 Mb/s, the AP would transmit broadcasts and multicasts at 1 Mb/s because this is the highest mandatory rate that all clients can receive. If the lowest mandatory rate was set to 5.5 Mb/s, the 802.11b client would not be able to associate to the AP because it could not receive broadcast packets at the lowest mandatory rate.

In Figure 3-15, note that the highest mandatory setting is 11 Mb/s. The highest mandatory rate tells the AP what rate the client radios must be able to physically transmit at. This does not mean that they are actually transmitting and receiving packets at that rate, it just means that the radio physically supports that rate; the wireless client needs only to be able to receive packets at the lowest mandatory rate. 802.11b devices would be able to associate to the AP shown in Figure 3-15 because their radios can physically transmit at 11 Mb/s. If a higher data rate (such as 18Mb/s) was set to mandatory, only 802.11g clients would be able to associate to the APs.

Setting any of the OFDM rates (rates above 11mb/s) to mandatory disables 802.11b connectivity. This can, for example, allow the administrator to exclude 802.11b clients from the AP by requiring an 802.11g data rate or setting a minimum transmission rate of all clients by disabling 802.11 rates. The reason this might be done is that the same 1500 byte packet at a lower data rate takes a longer time to transmit, and thus, lowers the effective data rate for all wireless clients associated to the AP.

Radio Resource Management (Auto-RF)

In the Cisco WLAN "split MAC" architecture (see Chapter 2, "Cisco Unified Wireless Technology and Architecture,") the processing of 802.11 data and management protocols and access point capabilities is distributed between a lightweight access point and a centralized WLAN controller. More specifically, time-sensitive activities, such as probe response and MAC layer encryption, are handled at the access point. All other functions are sent to the controller, where system-wide visibility is required.

Real-time RF management of a WLAN network requires system-wide visibility and is implemented at the controller level. The controller learns about the necessary information for an effective RF channel/power plan via information forwarded by the APs in the RF network group.

Note An RF network group (or RF group) is not the same as a mobility group. A mobility group defines a mobility domain of 1–25 controllers in which a client would not be required to change IP address during a roaming event. This is accomplished by building Ethernet over IP tunnels for forwarding client data from an "anchor" controller to the "foreign" controller handling the new AP servicing the client.

Radio Resource Management (RRM), also known as Auto-RF, can adjust the channel (dynamic channel assignment) and power (dynamic transmit power control) to maintain the RF coverage area. It adjusts the power level of the AP to maintain a baseline signal strength with neighboring APs at -65 dBm (configurable) (See Overview of Auto-RF Operation, page 3-30). It adjusts the channel of the AP when it notices nearby interference sources on the channel on which the AP is currently located. It continues to optimize the RF coverage for the best reception and throughput for the wireless network.

Note The transmit power control and dynamic frequency management performed by RRM are not the TPC and DFS required for operation in the UNII-2 bands that are defined in 802.11h.

RRM understands that the RF environment is not static. As different RF affecting variables change (people in the room, amount of devices stored in the facility, leaves on trees for outside deployment, interference from different RF sources, and so on), the RF coverage adjusts to these variables and changes with them. Because these variables change continuously, monitoring for the RF coverage and adjusting it periodically is necessary.

WLC software Release 4.185 introduced significant number of enhancements to Radio Resource Management (Auto-RF). For details on the changes and operation, see the following URL:

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a008072c759.shtml.

Overview of Auto-RF Operation

Each controller is configured with an RF network group name (called RF Network Name under the WLC Controller -> General menu). In each RF group (if Group Mode is enabled), the controllers elect a leader and form an RF domain. The function of the leader is to collect the network-wide neighbor information from a group of controllers and do the channel/power computation for an optimal system-wide map. If Group Mode is not enabled, the controllers run computations based only on the neighbor data gathered from the APs connected via LWAPP, trying to optimize the signal to -70 dBm between APs.

The APs transmit Radio Resource Management (RRM) neighbor packets at full power at regular intervals. These messages contain a field that is a hash of the RF group name, BSSID, and time stamp. The APs accept only RRM neighbor packets sent with this RF network name.

When neighboring APs receive neighbor messages, they validate them before forwarding them to the controller. If they can validate the message hash and confirm that it belongs to the same RF group, the packet is sent to the controller; otherwise, the AP drops the neighbor packet. The APs then forward the validated messages to the controller, filling in the LWAPP packet status field with the SNR and RSSI of the received neighbor packet.

Table 3-7 provides a summary of the various functions of the devices in the system.

Note TPC performs only downward power level adjustments. Coverage hole detection and correction increases power levels on APs.

Auto-RF should not be confused with Rogue Detection (channel scanning), which is done separately from the auto-RF algorithm. APs perform rogue detection by periodically monitoring all country-specific channels (channel scanning). The APs goes "off-channel" for a period not greater than 60 ms to listen to the other channels. Packet headers collected during this time are sent to the controller, where they are analyzed to detect rogue access points, whether service set identifiers (SSIDs) are broadcast or not, rogue clients, ad-hoc clients, and interfering access points.

By default, each access point spends approximately 0.2 percent of its time off-channel. This is statistically distributed across all access points so that no two adjacent access points are scanning at the same time, which can adversely affect WLAN performance. Packets received by the AP from clients are forwarded to the controller with the LWAPP status field filled in, which provides the controller with radio information including RSSI and signal-to-noise ratio (SNR) for all packets received by the AP during reception of the packet.

Table 3-7 Device Function

Device	Functions
RF Group Leader	Collects data from WLCs in the RF group and analyzes it for TX Power Control (TPC) and Dynamic Channel Assignment (DCA) system-wide. TPC adjusts power levels only downward.
Local WLC	Collects data and runs the Coverage Hole Detection and Correction algorithm. Adjusts power levels upward if necessary for clients
Light-weight access point	• Sends neighbor messages on all channels at full power at configured interval • Verifies neighbor hash on received neighbor messages • Scans configured channels for noise, interference, and IDS/rogue detection and alerts if profile fails

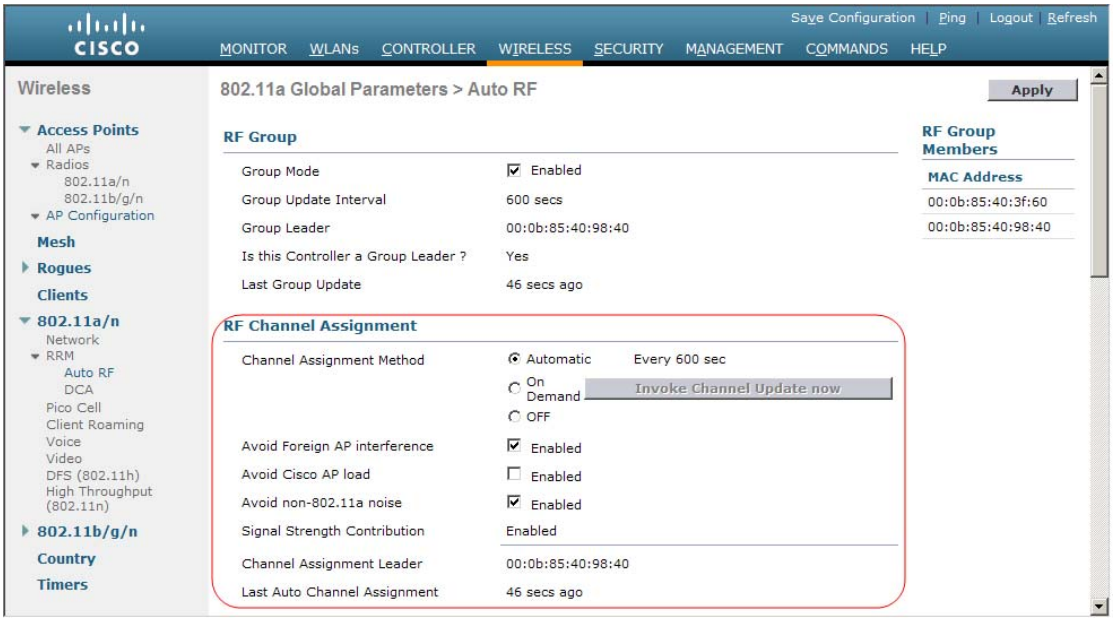
Auto-RF Variables and Settings

Auto-RF can be turned on and off via the global setting on the Channel Selection (**Wireless > 802.11b/g/n > Configure**) web page (see Figure 3-13). You can manually set the channel and transmit level for the AP from this web page. Additionally, it can be turned off and on from the global Auto-RF web page. Remember that Auto-RF is per band and RF group computations are done for both the 802.11b/g band and another set of computations for 802.11a. The two radios do not have to share to have the same configuration. But these configurations are applied to every AP associated to the controller. Auto-RF configuration variables are shown on the global parameters Auto-RF configuration page (see Figure 3-16).

The first set of variables on the Auto-RF configuration web page corresponds to the RF group. These determine whether the controller joins the dynamic grouping with the other controllers. The dynamic grouping helps the controller find out about APs that are neighbors but might be associated to another controller in the mobility group. If this is disabled, the controller only optimizes the parameters of the access points that it knows about (that is, the ones that are associated to it). The group leader indicates the MAC address of the elected leader. You can find the MAC address of the controller on the inventory web page (you can reach the web page by clicking on **Controller** at the top menu and then **Inventory**).

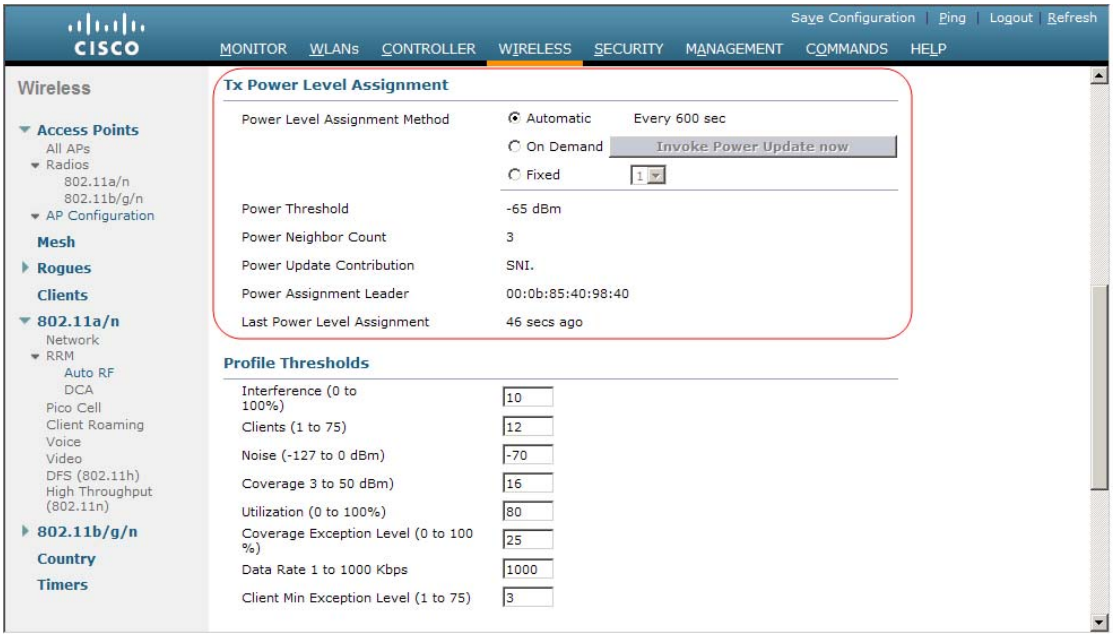
The Auto-RF configuration web page is divided into three pages, or sections, with a scroll bar that is used to move among the three pages. The first page (see Figure 3-16) is for dynamic channel assignment. This allows the controller to automatically change the channel that the AP is on (for more information, see Dynamic Channel Assignment, page 3-35).

Figure 3-16 Auto-RF (Page 1)



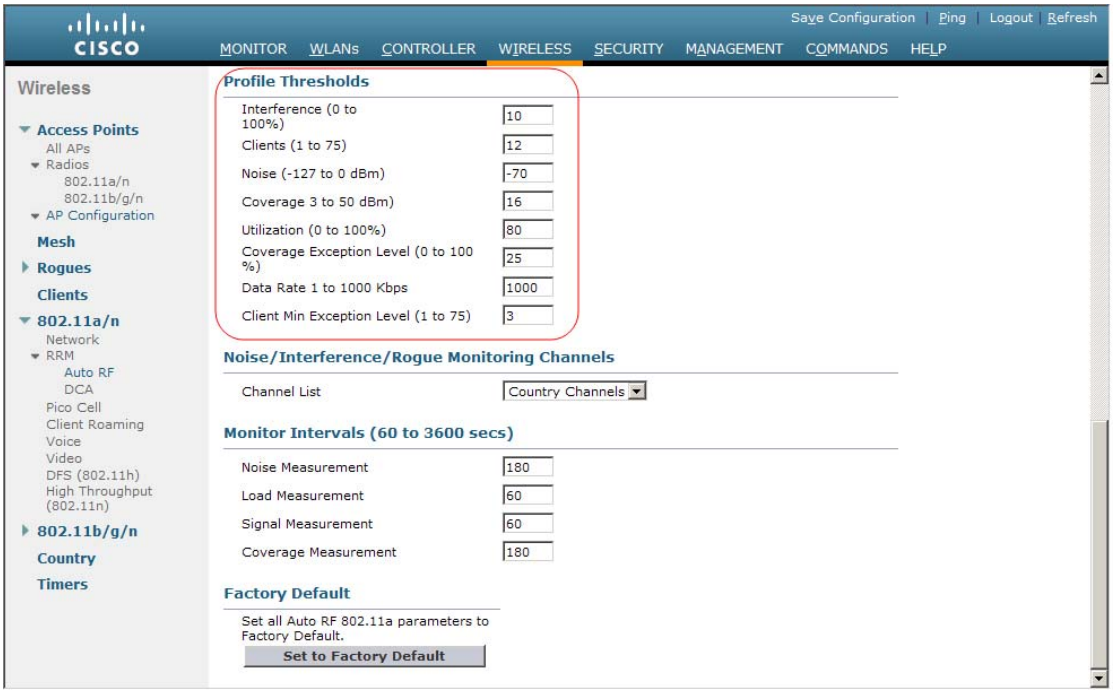
Following the RF channel assignment is the section for assigning the transmit (tx) power level (see Figure 3-17). On this web page, the power level can be fixed for all APs, or it can be automatically adjusted. The web page also indicates the number of neighbors the AP has and the power thresholds for which it is adjusting.

Figure 3-17 Auto-RF (Section 2)



The third web page is for profile thresholds.

Figure 3-18 Auto-RF (Section 3)



The WLC analyzes the information passed to it by the APs and determines a pass or fail status for each of these thresholds. These pass/fail profiles are best seen in the output of the **show ap auto-rf** *radio ap_name* command (see the following sample). The same information can be seen in graphical form on the **Monitor > 802.11b/g Radios > Detail** web page.

Sample show ap auto-rf Command Output

```
show>ap auto-rf 802.11b <access point name>
Number of Slots . . . . . . . . . . . . . . . . . . . . . . 2
AP Name . . . . . . . . . . . . . . . . . . . . . . . . . . <AP name>
MAC Address . . . . . . . . . . . . . . . . . . . . . . . . 00:0b:85:1b:df:c0
Radio Type . . . . . . . . . . . . . . . . . . . . . . . . . RADIO_TYPE_80211b/g
Noise Information
    Noise Profile . . . . . . . . . . . . . . . . . . . . . PASSED
    Channel 1 . . . . . . . . . . . . . . . . . . . . . . . -93 dBm
    Channel 2 . . . . . . . . . . . . . . . . . . . . . . . -90 dBm
 .
 .
 .
    Channel 11 . . . . . . . . . . . . . . . . . . . . . . -95 dBm
Interference Information
    Interference Profile . . . . . . . . . . . . . . . . . FAILED
    Channel 1 . . . . . . . . . . . . . . . . . . . . . . . -69 dBm @ 31 % busy
    Channel 2 . . . . . . . . . . . . . . . . . . . . . . . -58 dBm @ 26 % busy
 .
 .
 .
    Channel 11. . . . . . . . . . . . . . . . . . . . . . . -68 dBm @ 26 % busy
Load Information
    Load Profile . . . . . . . . . . . . . . . . . . . . . PASSED
    Receive Utilization . . . . . . . . . . . . . . . . . . 0 %
    Transmit Utilization . . . . . . . . . . . . . . . . . 0 %
    Channel Utilization . . . . . . . . . . . . . . . . . . 26 %
    Attached Clients . . . . . . . . . . . . . . . . . .  2 clients
Coverage Information
    Coverage Profile . . . . . . . . . . . . . . . . . . .. PASSED
    Failed Clients . . . . . . . . . . . . . . . . . . . . 0 clients
Client Signal Strengths
    RSSI -100 dBm. . . . . . . . . . . . . . . . . . . . . 0 clients
    RSSI -92 dBm . . . . . . . . . . . . . . . . . . . . . 0 clients
 .
 .
 .
    RSSI -52 dBm . . . . . . . . . . . . . . . . . . . . . 1 clients
Client Signal To Noise Ratios
    SNR 0 dBm . . . . . . . . . . . . . . . . . . . . . .  0 clients
    SNR 5 dBm . . . . . . . . . . . . . . . . . . . . . .  0 clients
    SNR 10 dBm . . . . . . . . . . . . . . . . . . . . . 0 clients
 .
 .
 .
    SNR 45 dBm . . . . . . . . . . . . . . . . . . . . . 1 clients
Nearby APs
Radar Information
Channel Assignment Information
    Current Channel Average Energy . . . . . . . . . . . . -68 dBm
    Previous Channel Average Energy . . . . . . . . . . . . -51 dBm
    Channel Change Count . . . . . . . . . . . . . . . . . 21
    Last Channel Change Time . . . . . . . . . . . . . . . Thu Mar 9 12:18:03 2006
    Recommend Best Channel . . . . . . . . . . . . . . . . 11
RF Parameter Recommendations
    Power Level . . . . . . . . . . . . . . . . . . . . . 1
    RTS/CTS Threshold . . . . . . . . . . . . . . . . . . 2347
    Fragmentation Threshold . . . . . . . . . . . . . . . 2346
    Antenna Pattern . . . . . . . . . . . . . . . . . . . 0
```

The following sections describe some of the Auto-RF variables.

Dynamic Channel Assignment

The 802.11 MAC layer uses Carrier-Sense Multiple Access/Collision Avoidance (CSMA/CA). With CSMA/CA, two APs on the same channel (in the same vicinity) get approximately half the capacity of two APs on different channels because of the shared wireless channel. This is caused by the 802.11 MAC sensing that the channel is busy, and deferring sending frames until the channel has become free. If the 802.11 MAC defers traffic that is not part of its own AP cell, this is considered interference. Interference from another AP on the same channel is commonly called co-channel interference, and is to be expected in most 2.4 GHz 802.11 deployments, because there are insufficient non-overlapping channels to prevent some channel overlap from occurring. One of the goals of design, planning, and dynamic radio management is to minimize the amount of co-channel overlap, which minimizes co-channel interference and therefore maximizes AP traffic capacity. The Cisco Unified Wireless Network addresses this problem and other co-channel interference issues by dynamically allocating AP channel assignments to avoid conflict. Because the WLC, or a designated WLC (RF Group Leader), has system-wide visibility, it can control how channels are "reused" to minimize co-channel interference.

The WLC examines a variety of real-time RF characteristics to efficiently handle channel assignments, including the following:

- Noise—This limits signal quality at the client and AP, and can vary in range and periodicity. There are numerous potential types and effects of interference. An increase in noise reduces the effective cell size. The WLC, at regular intervals, reassesses the RF environment of an AP, and optimizes channel selection to avoid noise sources while still maintaining overall system capacity. Channels that become unusable because of excessive noise can be avoided. If other wireless networks are present, the WLC shifts its channel usage to complement the other networks. For example, if one network is on Channel 6, the adjacent WLAN is assigned Channel 1 or 11. This increases the capacity of the network by limiting the sharing of frequencies. If a channel is used so much that no capacity is available, the WLC might choose to avoid this channel.
- Client load—Client load is taken into account when changing the channel structure to minimize the impact on the clients currently on the WLAN system. The WLC periodically monitors the channel assignment in search of the best assignments. Change occurs only if it significantly improves the performance of the network or corrects the performance of a poorly performing AP.

The WLC combines the RF characteristic information to make system-wide decisions. The end result is an optimal channel configuration in a three-dimensional space, where APs on the floor above and below factor into an overall WLAN configuration.

Interference Detection and Avoidance

Interference (as it pertains to a Cisco Unified Wireless deployment) is defined as unwanted RF signals in the same frequency band that can lead to a degradation or loss of service. These signals can either be from 802.11 or non-802.11 sources such as certain microwave ovens or many cordless phones. It can, in certain instances, also include various sources of electromagnetic interference (EMI) such as arc welders or federal/military radar facilities. APs are constantly scanning all channels looking for major sources of interference.

If the amount of 802.11 interference hits a predefined threshold, the WLC attempts to rearrange channel assignments to optimize system performance in the presence of the interference. This might result in adjacent APs being on the same channel, but logically this represents a better scenario than staying on a channel that is otherwise totally unusable because of an interfering AP.

For example, the WLC can respond to a rogue AP on channel 11 by shifting nearby APs to channel 1 or channel 6.

Dynamic Transmit Power Control

Appropriate AP power levels are essential to maintaining a coverage area, not only to ensure correct (not maximum) amount of power covering an area, but also to ensure that excessive power is not used, which would add unnecessary interference to the radiating area. AP power settings are also used to control network redundancy by helping to ensure real-time failover in the event of the loss of an AP. The WLC is used to dynamically control the AP transmit power level based on real-time WLAN conditions. In normal instances, power can be minimized to gain extra capacity and reduce interference among the APs. RRM attempts to balance APs so that they see their neighbors at -65 dBm. If an AP outage is detected, power can be automatically increased on surrounding APs to fill the coverage gap created by the loss of the AP.

RRM algorithms are designed to create the optimal user experience. For example, if the power of an AP is turned down to Level 4 (where Level 1 = highest and Level 8 = lowest) and the received signal strength indicator (RSSI) value of a user drops below an acceptable threshold, the AP power is increased to provide a better experience to that client. When Dynamic Transmit Power Control (DTPC) is enabled, the access points add channel and transmit power information to beacons. Client devices using DTPC receive the information and adjust their settings automatically.

Coverage Hole Detection and Correction

The coverage hole detection and correction algorithm is aimed at determining coverage holes based on the quality of client signal levels and then increasing the transmit power of the APs to which those clients are associated.

The algorithm determines whether a coverage hole exists when client SNR levels pass below a given SNR threshold. The SNR threshold is considered on an individual AP basis and based primarily on the transmit power of each AP.

When the average SNR of a single client dips below the SNR threshold for at least 60 seconds, this is seen as an indication that the WLAN client does not have a viable location to which to roam. The AP transmit power of that client is increased, correcting the coverage hole.

Client and Network Load Balancing

The IEEE 802.11 standard does not define the process or reasons for client roaming, and therefore it cannot be easily predicted what clients will do in any given situation. For example, all users in a conference room can associate with a single AP because of its close proximity, ignoring other APs that are farther away but with greater free capacity.

The WLC has a centralized view of client distribution across all APs. This can be used to influence where new clients attach to the network if there are multiple “good” APs available. If configured, the WLC can proactively use AP probe responses to guide clients to the most appropriate APs to improve WLAN performance. This results in a smooth distribution of capacity across an entire wireless network. Keep in mind that this load balancing is done at client association, not while a client is connected.

CHAPTER 4

Cisco Unified Wireless Network Architecture—Base Security Features

The Cisco Unified Wireless Network solution builds upon the base security features of 802.11 by augmenting RF, 802.11, and network-based security features where necessary to improve overall security. Although the 802.11 standards address the security of the wireless medium, the Cisco Unified Wireless Network solution addresses end-to-end security of the entire system by using architecture and product security features to protect WLAN endpoints, the WLAN infrastructure, client communication, and the supporting wired network.

Base 802.11 Security Features

This section focuses on the enterprise security features that are currently available for 802.11 wireless networks.

Although there were initially security flaws native to the 802.11 protocol, the introduction of 802.11i has addressed all the known data privacy issues, which are to ensure that the requirements for confidential communications are achieved through the use of strong authentication and encryption methods.

Additional WLAN security issues are discussed later in this guide. Some of these issues are being addressed by standards bodies, while others are being addressed in the Cisco Unified Wireless Network Solution.

WLAN Security Implementation Criteria

For the WLAN network, security is based on both authentication and encryption. Common security mechanisms for WLAN networks are as follows:

- Open Authentication, no encryption
- Wired Equivalent Privacy (WEP)
- Cisco WEP Extensions (Cisco Key Integrity Protocol +Cisco Message Integrity Check)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA 2)

WPA and WPA 2 are defined by the Wi-Fi Alliance, which is the global Wi-Fi organization that created the "Wi-Fi" brand. The Wi-Fi Alliance certifies inter-operability of IEEE 802.11 products and promotes them as the global, wireless LAN standard across all market segments. The Wi-Fi Alliance has instituted a test suite that defines how member products are tested to certify that they are interoperable with other Wi-Fi Certified products.

The original 802.11 security mechanism, WEP, was a static encryption method used for securing wireless networks. Although it applies some level of security, WEP is viewed as insufficient for securing business communications. In short, the WEP standard within 802.11 did not address the issue of how to manage encryption keys. The encryption mechanism itself was found to be flawed, in that a WEP key could be derived simply by monitoring client traffic. Cisco WLAN products addressed these issues by introducing 802.1x authentication and dynamic key generation and by introducing enhancements to WEP encryption: Cisco Key Integrity Protocol (CKIP) and Cisco Message Integrity Check (CMIC). 802.11i is a standard introduced by the IEEE to address the security shortcomings of the original 802.11 standard. The time between the original 802.11 standard and the ratification of 802.11i saw the introduction of interim solutions.

WPA is an 802.11i-based security solution from the Wi-Fi Alliance that addresses the vulnerabilities of WEP. WPA uses Temporal Key Integrity Protocol (TKIP) for encryption and dynamic encryption key generation by using either a pre-shared key, or RADIUS/802.1x-based authentication. The mechanisms introduced into WPA were designed to address the weakness of the WEP solution without requiring hardware upgrades. WPA2 is the next generation of Wi-Fi security and is also based on the 802.11i standard. It is the approved Wi-Fi Alliance interoperable implementation of the ratified IEEE 802.11i standard. WPA 2 offers two classes of certification: Enterprise and Personal. Enterprise requires support for RADIUS/802.1x-based authentication and pre-shared key (Personal) requires only a common key shared by the client and the AP. The new Advanced Encryption Standard (AES) encryption mechanism introduced in WPA2 generally requires a hardware upgrade from earlier versions of WLAN clients and APs, however all Cisco LWAPP APs support WPA2.

Table 4-1 summarizes the various specifications.

Table 4-1 WLAN Security Mechanisms

Feature	Static WEP	802.1x WEP	WPA	WPA 2 (Enterprise)
Identity	User, machine or WLAN card	User or machine	User or machine	User or machine
Authentication	Shared key	EAP	EAP or pre-shared keys	EAP or pre-shared keys
Integrity	32-bit Integrity Check Value (ICV)	32-bit ICV	64-bit Message Integrity Code (MIC)	CRT/CBC-MAC (Counter mode Cipher Block Chaining Auth Code - CCM) Part of AES
Encryption	Static keys	Session keys	Per Packet Key rotation via TKIP	CCMP (AES)
Key distribution	One time, Manual	Segment of Pair-wise Master Key (PMK)	Derived from PMK	Derived from PMK
Initialization vector	Plain text, 24-bits	Plain text, 24-bits	Extended Initialization Vector (IV)-65-bits with selection/sequencing	48-bit Packet Number (PN)

Table 4-1 WLAN Security Mechanisms (continued)

Algorithm	RC4	RC4	RC4	AES
Key strength	64/128-bit	64/128-bit	128-bit	128-bit
Supporting infrastructure	None	RADIUS	RADIUS	RADIUS

The Cisco Wireless Security suite provides the user with the options to provide varying security approaches based on the required or pre-existing authentication, privacy and client infrastructure. Cisco Wireless Security Suite supports WPA and WPA2, including:

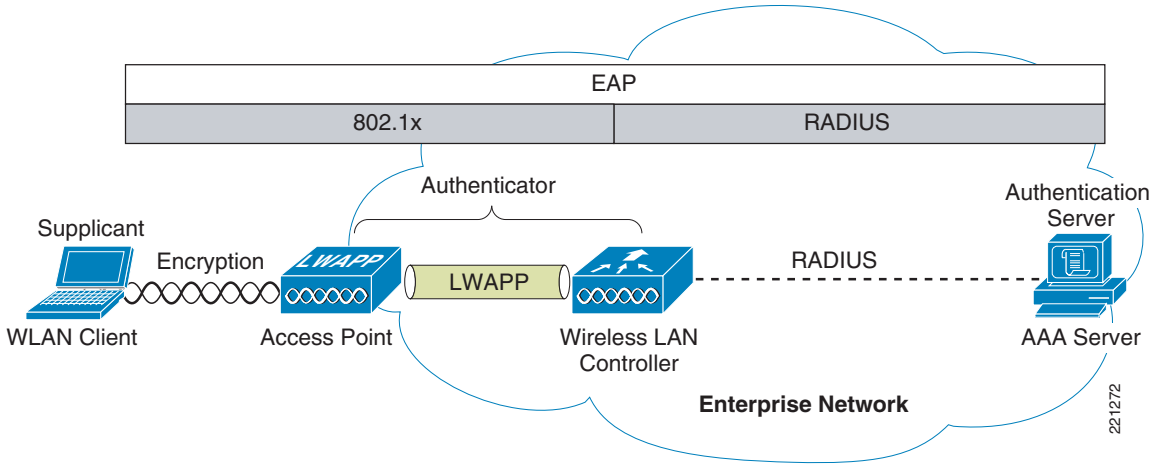
- Authentication based on 802.1X using the following EAP methods:
  - Cisco LEAP, EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
  - PEAP- Generic Token Card (PEAP-GTC)
  - PEAP-Microsoft Challenge Authentication Protocol Version 2 (PEAP-MSCHAPv2)
  - EAP-Transport Layer Security (EAP-TLS)
  - EAP-Subscriber Identity Module (EAP-SIM)
- Encryption:
  - AES-CCMP encryption (WPA2)
  - TKIP encryption enhancements: key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation via WPA TKIP Cisco Key Integrity Protocol (CKIP) and Cisco Message Integrity Check (CMIC)
  - Support for static and dynamic IEEE 802.11 WEP keys of 40 bits, 104, and 128 bits

Note 128-bit WEP (128-bit WEP key =152-bit total key size as IV is added to key) is not supported by all APs and clients. Even if it was, increasing WEP key length does not address the inherent security weaknesses of WEP.

Terminology

A number of common terms are introduced throughout this guide, and are shown in Figure 4-1.

Figure 4-1 Secure Wireless Topology



The basic physical components of the solution are as follows:

- WLAN client
- Access point (AP)
- Wireless LAN Controller (WLC)
- AAA server

Figure 4-1 also shows the basic roles and relationships associated with the 802.1X authentication process:

- An 802.1X supplicant (wireless software) resides on the WLAN client.
- The AP and WLC, using the LWAPP split-MAC architecture, act together as the 802.1X authenticator.
- The AAA server is the authentication server.

Figure 4-1 also illustrates the role of 802.1X and the RADIUS protocol in carrying EAP packets between the client and the authentication server. Both 802.1X and EAP are discussed in more detail later in this chapter.

802.1X

802.1X is an IEEE framework for port-based access control that has been adopted by the 802.11i security workgroup as a means of providing authenticated access to WLAN networks.

- The 802.11 association process creates a “virtual” port for each WLAN client at the AP.
- The AP blocks all data frames apart from 802.1X-based traffic.
- The 802.1X frames carry the EAP authentication packets, which are passed through to the AAA server by the AP.
- If the EAP authentication is successful, the AAA server sends an EAP success message to the AP, where the AP then allows data traffic from the WLAN client to pass through the virtual port.
- Before opening the virtual port, data link encryption between the WLAN client and the AP is established to ensure that no other WLAN client can access the port that has been established for a given authenticated client.

Extensible Authentication Protocol

Extensible Authentication Protocol (EAP) is an IETF RFC that stipulates that an authentication protocol must be decoupled from the transport protocol used to carry it. This allows the EAP protocol to be carried by transport protocols such as 802.1X, UDP, or RADIUS without having to make changes to the authentication protocol itself.

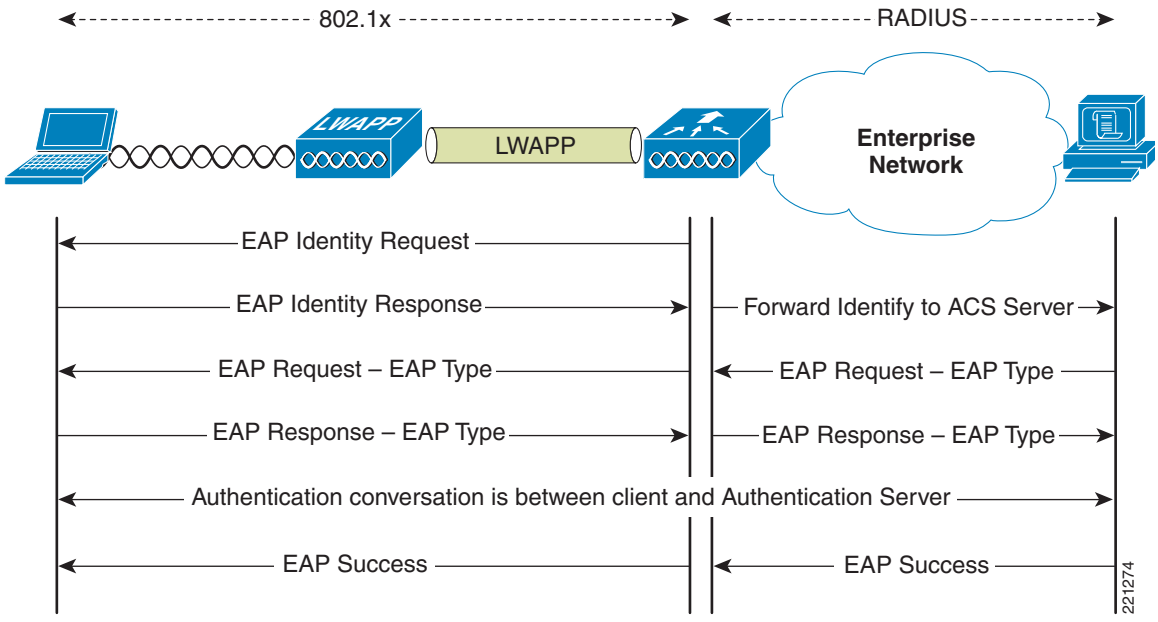
The basic EAP protocol is relatively simple, consisting of the following four packet types:

- EAP request—The request packet is sent by the authenticator to the supplicant. Each request has a type field that indicates what is being requested; for example, supplicant identity and EAP type to be used. A sequence number allows the authenticator and the peer to match an EAP response to each EAP request.
- EAP response—The response packet is sent by the supplicant to the authenticator, and uses a sequence number to match the initiating EAP request. The type of the EAP response generally matches the EAP request, except if the response is a negative-acknowledgment (NAK).
- EAP success—The success packet is sent when successful authentication has occurred, and is sent from the authenticator to the supplicant.
- EAP failure—The failure packet is sent when unsuccessful authentication has occurred, and is sent from the authenticator to the supplicant.

When using EAP in an 802.11i compliant system, the AP operates in EAP pass-through mode. In this mode, it checks the code, identifier, and length fields, and then forwards EAP packets received from the client supplicant to the AAA. EAP packets received by the authenticator from the AAA server are forwarded to the supplicant.

Figure 4-2 shows an example of EAP protocol flow.

Figure 4-2 EAP Protocol Flow



Authentication

Depending on the customer requirements, various authentication protocols such as PEAP, EAP-TLS, and EAP-FAST can be used in secure wireless deployments. Regardless of the protocol, they all currently use 802.1X, EAP, and RADIUS as their underlying transport. These protocols allow network access to be controlled based on the successful authentication of the WLAN client, and just as importantly, allow the WLAN network to be authenticated by the user.

This solution also provides authorization through policies communicated through the RADIUS protocol, as well as RADIUS accounting.

EAP types used for performing authentication are described in more detail below. The primary factor affecting the choice of EAP protocol is the authentication system (AAA) currently in use. Ideally, a secure WLAN deployment should not require the introduction of a new authentication system, but rather should leverage the authentication systems that are already in place.

Supplicants

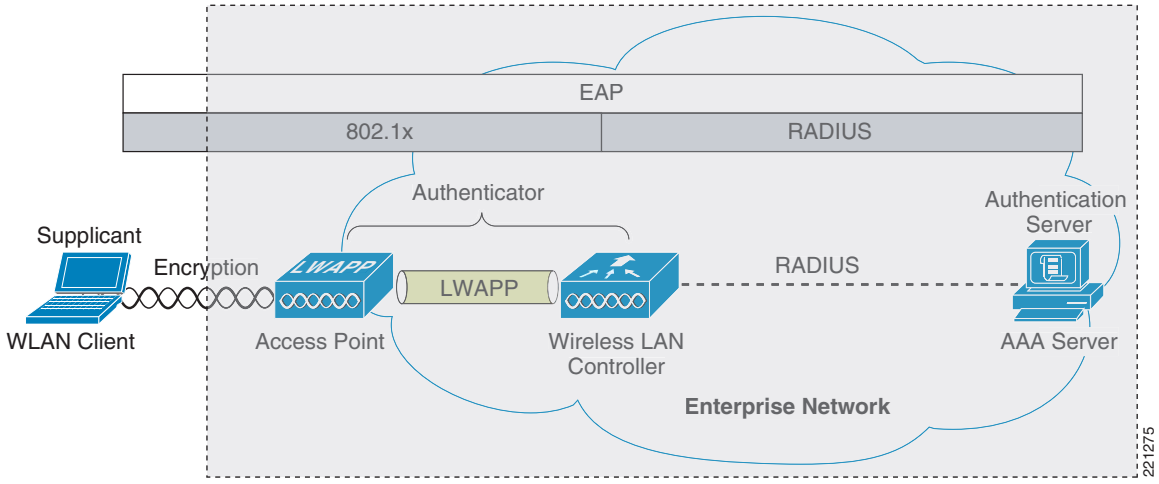
The client software used for WLAN authentication is called a supplicant, based on 802.1X terminology. The Cisco Secure Services Client (CSSC) 4.1 is a supplicant that supports both wired and wireless networks, and all the common EAP types. Supplicants may also be provided by the WLAN NIC manufacturer, or can come integrated within an operating system; for example, Windows XP supports PEAP MSCHAPv2 and EAP-TLS.

For more information on CSSC, see the following URL:

http://www.cisco.com/en/US/products/ps7034/index.html

Figure 4-3 shows the logical location of the supplicant relative to the overall authentication architecture. The role of the supplicant is to facilitate end-user authentication using EAP and 802.1X to an upstream authenticator; in this case, the WLC. The authenticator forwards EAP messages received by the supplicant and forwards them to an upstream AAA server using RADIUS.

Figure 4-3 WLAN Client Supplicant



The various EAP supplicants that are available in the marketplace reflect the diversity of authentication solutions available and customer preferences.

Table 4-2 shows a summary of common EAP supplicants:

- PEAP MSCHAPv2—Protected EAP MSCHAPv2. Uses a Transport Layer Security (TLS) tunnel, (the IETF standard of SSL) to protect an encapsulated MSCHAPv2 exchange between the WLAN client and the authentication server.
- PEAP GTC—Protected EAP Generic Token Card (GTC). Uses a TLS tunnel to protect a generic token card exchange; for example, a one-time password or LDAP authentication.
- EAP-FAST—EAP-Flexible Authentication via Secured Tunnel. Uses a tunnel similar to that used in PEAP, but does not require the use of Public Key Infrastructure (PKI).
- EAP-TLS—EAP Transport Layer Security uses PKI to authenticate both the WLAN network and the WLAN client, requiring both a client certificate and an authentication server certificate.

Table 4-2 Comparison of Common Supplicants

	Cisco EAP-FAST	PEAP MS-CHAPv2	PEAP EAP-GTC	EAP-TLS
Single sign-on (MSFT AD only)	Yes	Yes	Yes[1]	Yes
Login scripts (MSFT AD only)	Yes	Yes	Some	Yes[2]
Password change (MSFT AD)	Yes	Yes	Yes	N/A
Microsoft AD database support	Yes	Yes	Yes	Yes
ACS local database support	Yes	Yes	Yes	Yes
LDAP database support	Yes[3]	No	Yes	Yes
OTP authentication support	Yes[4]	No	Yes	No
RADIUS server certificate required?	No	Yes	Yes	Yes
Client certificate required?	No	No	No	Yes
Anonymity	Yes	Yes[5]	Yes[6]	No

1. Supplicant dependent
2. Machine account and machine authentication is required to support the scripts.
3. Automatic provisioning is not supported on with LDAP databases.
4. Supplicant dependent
5. Supplicant dependent
6. Supplicant dependent

Authenticator

The authenticator in the case of the Cisco Secure Wireless Solution is the Wireless LAN Controller (WLC), which acts as a relay for EAP messages being exchanged between the 802.1X-based supplicant and the RADIUS authentication server.

After the completion of a successful authentication, the WLC receives the following:

- A RADIUS packet containing an EAP success message
- An encryption key generated at the authentication server during the EAP authentication
- RADIUS vendor-specific attributes (VSAs) for communicating policy

Figure 4-4 shows the logical location of the "authenticator" within the overall authentication architecture. The authenticator controls network access using the 802.1X protocol, and relays EAP messages between the supplicant and the authentication server.

Figure 4-4 Authenticator Location

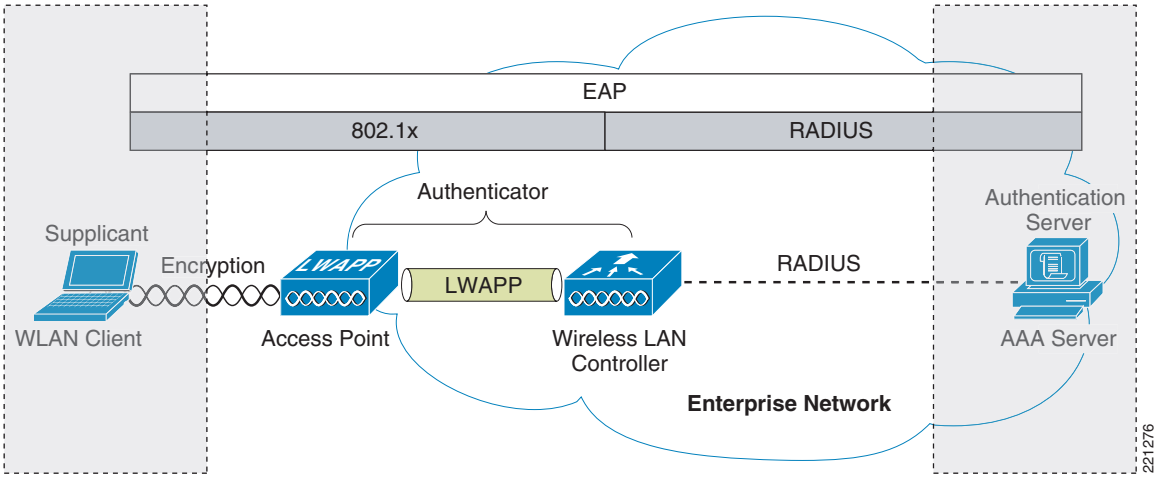


Table 4-3 shows an example decode of an EAP-TLS authentication where the four left-most columns are wireless 802.1X decodes, and the three right-most columns are decodes of the respective RADIUS transactions for the same EAP-TLS authentication.

The EAP exchange sequence is as follows:

- Packet #1 is sent by the AP to the client, requesting the client identity. This begins the EAP exchange.
- Packet #2 is the client identity that is forwarded to the RADIUS server. Based on this identity, the RADIUS server can decide whether to continue with the EAP authentication.
- In packet #3, the RADIUS server sends a request to use PEAP as the EAP method for authentication. The actual request depends on the EAP types configured on the RADIUS server. If the client rejects the PEAP request, the RADIUS server may offer other EAP types.
- Packets #4–8 are the TLS tunnel setup for PEAP.
- Packets #9–16 are the authentication exchange within PEAP.
- Packet #17 is the EAP message saying that the authentication was successful.

  In addition to informing the supplicant and the authenticator that the authentication was successful, packet #17 also carries encryption keys and authorization information in the form of RADIUS VSAs to the authenticator.

Table 4-3 EAP Transaction

#	Source	Dest	Protocol	Info	Source	Dest	RADIUS Info
1	AP	Client	EAP	Request, Identity			
2	Client	AP	EAP	Response, Identity	WLC	AAA	Access-Rq 1, id=114
3	AP	Client	EAP	Request, PEAP	AAA	WLC	Access-Ch 11, id=115
4	Client	AP	TLS[1]	Client Hello	WLC	AAA	Access-Rq 1, id=116
5	AP	Client	TLS	Server Hello, Certificate	AAA	WLC	Access-Ch 11, id=116
6	Client	AP	TLS	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	WLC	AAA	Access-Rq 1, id=117
7	AP	Client	TLS	Change Cipher Spec, Encrypted Handshake Message	AAA	WLC	Access-Ch 11, id=117
8	Client	AP	EAP	Response, PEAP	WLC	AAA	Access-Rq 1, id=118
9	AP	Client	TLS	Application Data	AAA	WLC	Access-Ch 11, id=118
10	Client	AP	TLS	Application Data	WLC	AAA	Access-Rq 1, id=119
11	AP	Client	TLS	Application Data	AAA	WLC	Access-Ch 11, id=119
12	Client	AP	TLS	Application Data	WLC	AAA	Access-Rq 1, id=120
13	AP	Client	TLS	Application Data	AAA	WLC	Access-Ch 11, id=120
14	Client	AP	TLS	Application Data	WLC	AAA	Access-Rq 1, id=121
15	AP	Client	TLS	Application Data	AAA	WLC	Access-Ch 11, id=121
16	Client	AP	TLS	Application Data	WLC	AAA	Access-Rq 1, id=122
17	AP	Client	EAP	Success	AAA	WLC	Access-Accept 2, id=122

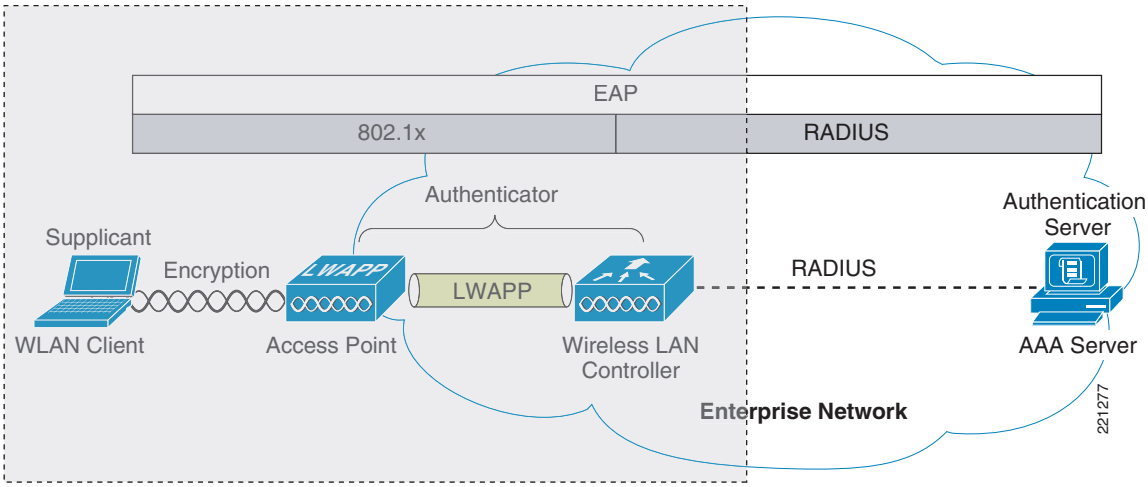
1. The TLS transaction is carried within EAP packets

Authentication Server

The authentication server used in the Cisco Secure Unified Wireless Solution is the Cisco Access Control Server (ACS). Cisco ACS is available as software that is installable on a Windows 2000 or 2003 servers, or as an appliance. Alternatively, the authentication server role can be implemented within specific WLAN infrastructure devices such as local authentication services on an IOS AP, local EAP authentication support within the WLC, AAA services integrated in the Cisco WLSExpress, or any AAA server that supports the required EAP types.

Figure 4-5 shows the logical location of the authentication server within the overall wireless authentication architecture, where it performs the EAP authentication via a RADIUS tunnel.

Figure 4-5 Authentication Server Location



After the completion of a successful EAP authentication, the authentication server sends an EAP success message to the authenticator. This message tells the authenticator that the EAP authentication process was successful, and passes the pair-wise master key (PMK) to the authenticator that is in turn used as the basis for creating the encrypted stream between the WLAN client and the AP. The following shows an example decode of an EAP success message within RADIUS:

```
Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x7a (122)
    Length: 196
    Authenticator: 1AAAD5ECBC487012B753B2C1627E493A
    Attribute Value Pairs
        AVP: l=6  t=Framed-IP-Address(8): Negotiated
        AVP: l=6  t=EAP-Message(79) Last Segment[1]
            EAP fragment
            Extensible Authentication Protocol
                Code: Success (3)
                Id: 12
                Length: 4
        AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
        AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
        AVP: l=6  t=User-Name(1): xxxxxxx
        AVP: l=24  t=Class(25): 434143533A302F313938662F63306138336330322F31
        AVP: l=18  t=Message-Authenticator(80): 7C34BA45A95F3E55425FDAC301DA1AD7
```

Encryption

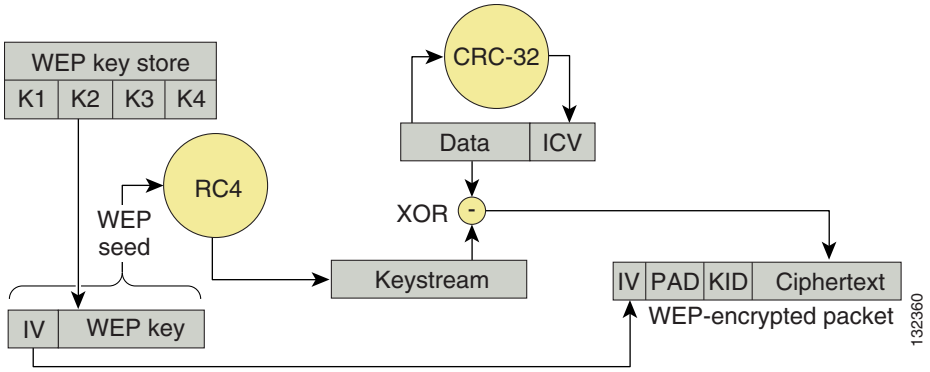
Encryption is a necessary component of WLAN security to provide privacy over a local RF broadcast network. When the 802.11 standard was first introduced, Wired Equivalent Privacy (WEP) was the standard encryption mechanism. WEP has since been found to be flawed in many ways and is not considered an effective encryption solution for securing a WLAN. A discussion of WEP is included in this document. WEP is currently supported by most WLAN products to support legacy client deployments. Any new deployment should be using either TKIP (WPA) or AES (WPA2) encryption.

Encryption keys are derived from a PMK. In the case of a dynamic WEP implementation, the WEP key is a segment of the PMK, whereas in WPA and WPA2, the encryption keys are derived during the four-way handshake discussed later in this section.

WEP

Figure 4-6 shows the WEP encryption process. A WEP key is concatenated with an initialization vector (IV), and this combined key is used as the seed for an RC4 keystream that is XORed with the WLAN data. A different IV stream is used for each frame, and therefore a different combined key is used to create a new RC4 keystream for each frame. Vulnerabilities have been exposed where repeated IVs, along with the adaptation of a stream cipher (RC4) to create the block cipher, have resulted in an insecure encryption mechanism that can be cracked with what are now commonly available tools. As stated earlier, WEP is not recommended for use.

Figure 4-6 WEP Encapsulation Process



The LWAPP WLAN solution supports three WEP key lengths: the standard 40-bit and 104-bit key lengths, and an additional 128-bit key. The use of the 128-bit key is not recommended because 128-bit keys are not widely supported in WLAN clients, and the additional key length does not address the weakness inherent in WEP encryption

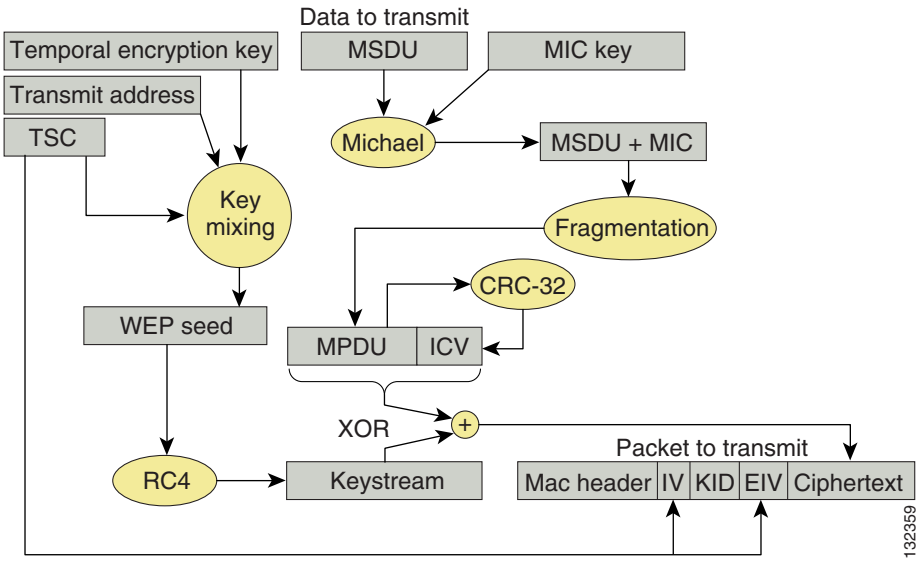
TKIP Encryption

Two enterprise-level encryption mechanisms specified by 802.11i are certified as WPA and WPA2 by the Wi-Fi Alliance: Temporal Key Integrity Protocol (TKIP), and Advanced Encryption Standard (AES).

TKIP is the encryption method certified as WPA. It provides support for legacy WLAN equipment by addressing the original flaws associated with the 802.11 WEP encryption method. It does this by making use of the original RC4 core encryption algorithm. The hardware refresh cycle of WLAN client devices is such that TKIP (WPA) is likely to be a common encryption option for a number of years to come. Although TKIP addresses all the known weaknesses of WEP, the AES encryption of WPA2 is the preferred method because it brings the WLAN encryption standards into alignment with broader IT industry standards and best practices.

Figure 4-7 shows a basic TKIP flow chart.

Figure 4-7 WPA TKIP

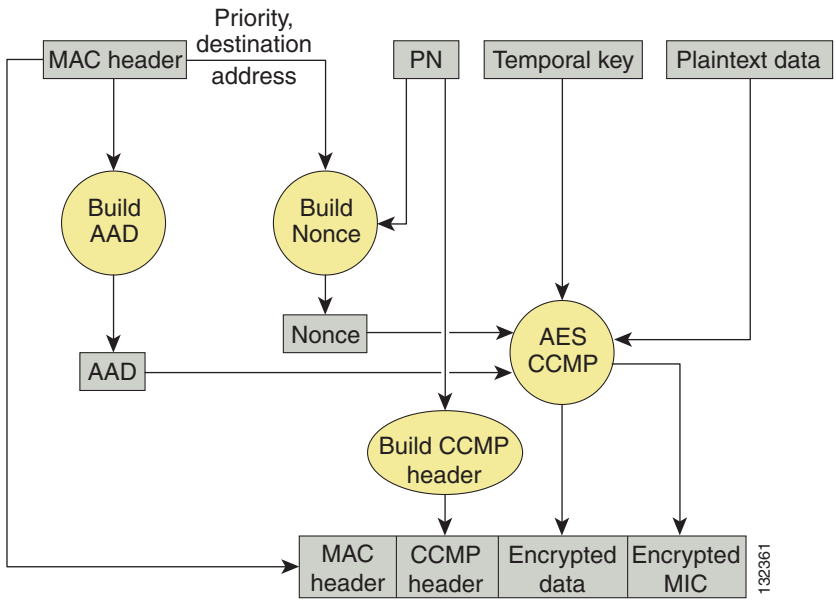


The two primary functions of TKIP are the generation of a per-packet key using RC4 encryption of the MAC service data unit (MSDU) and a message integrity check (MIC) in the encrypted packet. The per-packet key is a hash of the transmission address, the frame initialization vector (IV), and the encryption key. The IV changes with each frame transmission, so the key used for RC4 encryption is unique for each frame. The MIC is generated using the Michael algorithm to combine a MIC key with user data. The use of the Michael algorithm is a trade-off because although its low computational overhead is good for performance, it can be susceptible to an active attack. To address this, WPA includes countermeasures to safeguard against these attacks that involve temporarily disconnecting the WLAN client and not allowing a new key negotiation for 60 seconds. Unfortunately, this behavior can itself become a type of DoS attack. Many WLAN implementations provide an option to disable this countermeasure feature.

AES Encryption

Figure 4-8 shows the basic AES counter mode/CBC MAC Protocol (CCMP) flow chart. CCMP is one of the AES encryption modes, where the counter mode provides confidentiality and CBC MAC provides message integrity.

Figure 4-8 WPA2 AES CCMP



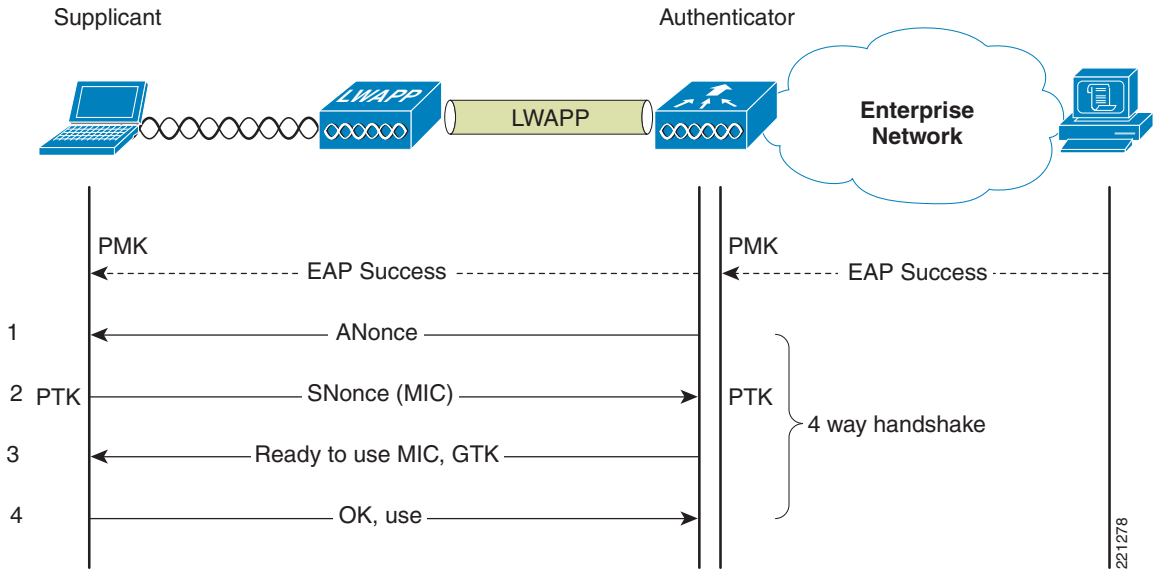
In the CCMP procedure, additional authentication data (AAD) is taken from the MAC header and included in the CCM encryption process. This protects the frame against alteration of the non-encrypted portions of the frame.

To protect against replay attacks, a sequenced packet number (PN) is included in the CCMP header. The PN and portions of the MAC header are used to generate a nonce that is turn used by the CCM encryption process.

Four-Way Handshake

The four-way handshake describes the method used to derive the encryption keys to be used to encrypt wireless data frames Figure 4-9 shows a diagram of the frame exchanges used to generate the encryption keys. These keys are referred to as temporal keys.

Figure 4-9 Four-Way Handshake



The keys used for encryption are derived from the PMK that has been mutually derived during the EAP authentication section. This PMK is sent to the authenticator in the EAP success message, but is not forwarded to the supplicant because the supplicant has derived its own copy of the PMK.

1. The authenticator sends an EAPOL-Key frame containing an authenticator nonce (ANonce), which is a random number generated by the authenticator.
   a. The supplicant derives a PTK from the ANonce and supplicant nonce (SNonce), which is a random number generated by the client/supplicant.
2. The supplicant sends an EAPOL-Key frame containing an SNonce, the RSN information element from the (re)association request frame, and an MIC.
   a. The authenticator derives a PTK from the ANonce and SNonce and validates the MIC in the EAPOL-Key frame.
3. The authenticator sends an EAPOL-Key frame containing the ANonce, the RSN information element from its beacon or probe response messages; the MIC, determining whether to install the temporal keys; and the encapsulated group temporal key (GTK), the multicast encryption key.
4. The supplicant sends an EAPOL-Key frame to confirm that the temporal keys are installed.

Cisco Compatible Extensions

The Cisco Compatible Extensions program helps promote the widespread availability of client devices that are interoperable with a Cisco WLAN infrastructure, and takes advantage of Cisco-specific innovations for enhanced security, mobility, quality of service (QoS), and network management.

Cisco Compatible Extensions build on the 802.11 and IETF standards, in addition to Wi-Fi Alliance certifications to create a superset of WLAN features, as shown in Figure 4-10. Even if a customer is not planning to deploy a Cisco Unified Wireless Network, the use of a Cisco Compatible Extensions WLAN adapter is a wise choice because it offers a simple way of tracking the standards supported and certifications associated with WLAN client devices.

Figure 4-10 Cisco Compatible Extensions Structure

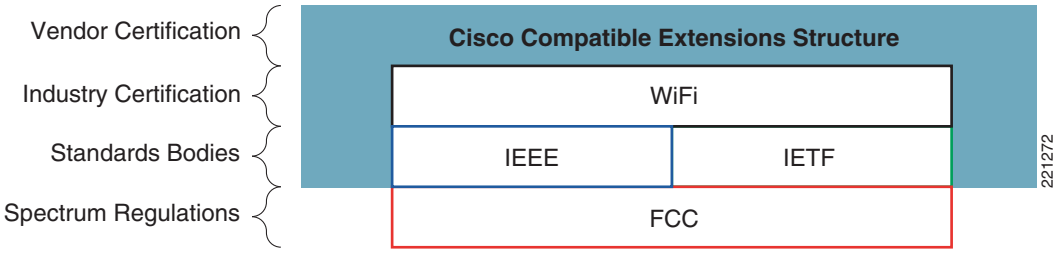


Figure 4-11 shows a summary of the security features associated with each Cisco Compatible Extensions certification level. The Cisco Compatible Extensions certification not only specifies which Wi-Fi certifications are applicable, but also which EAP supplicants have been tested as part of the Cisco Compatible Extensions certification.

Note Several features that are required for laptops are not required on application-specific devices (ASDs) that are used exclusively or primarily for data applications. Data ASDs include data capture devices, PDAs, and printers. Voice ASDs include single mode, dual mode, and smartphones.

The complete Cisco Compatible Extensions version table can be found at the following URL: http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html.

Figure 4-11 Cisco Compatible Extensions Security Features Example

Security	v1	v2	v3	v4	ASD
WEP	x	x	x	x	
IEEE 802.1X	x	x	x	x	x
LEAP	x	x	x	x	x
PEAP with EAP-GTC (PEAP-GTC)		x	x	x	optional
EAP-FAST			x	x	x
PEAP with EAP-MSCHAPv2 (PEAP-MSCHAP)				x	
EAP-TLS ASD requires either LEAP, EAP-Fast, or EAP-TLS				x	x
Cisco TKIP (encryption)	x				
WiFi Protected Access (WPA): 802.1X + WPA TKIP		x	x	x	
With LEAP (ASD requires either LEAP, EAP-Fast, or EAP-TLS)		x	x	x	x
With PEAP-GTC		x	x	x	
With EAP-FAST (ASD requires either LEAP, EAP-Fast, or EAP-TLS)			x	x	x
With PEAP-MSCHAP				x	
With EAP-TLS (ASD requires either LEAP, EAP-Fast, or EAP-TLS)				x	x
IEEE 802.11i–WPA2: 802.1X + AES			x	x	
With LEAP			x	x	
With PEAP-GTC			x	x	
With EAP-FAST			x	x	
With PEAP-MSCHAP and EAP-TLS				x	
Network Admission Control (NAC)				x	

221405

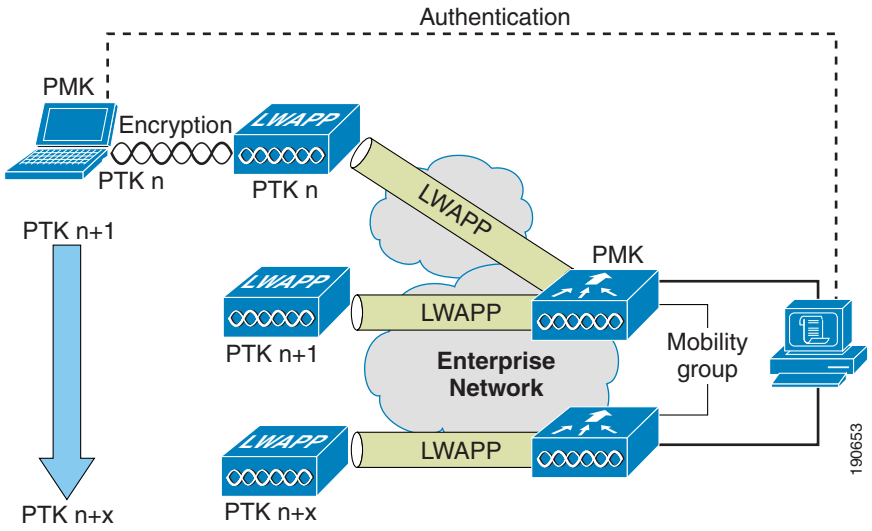
Cisco Compatible Extensions version 5 provides additional security features such as client-side management frame protection (MFP), which is described in Management Frame Protection, page 4-30.

Proactive Key Caching and CCKM

Proactive Key Caching (PKC) is an 802.11i extension that allows for the proactive caching (before the client roaming event) of the PMK that is derived during a client 802.1x/EAP authentication at the AP (see Figure 4-12). If a PMK (for a given WLAN client) is pre-cached at an AP to which the client is about to roam, full 802.1x/EAP authentication is not required. Instead, the WLAN client can simply use the WPA four-way handshake process to securely derive a new session encryption key for communication with that AP.

The distribution of these cached PMKs to APs is greatly simplified in the Unified Wireless deployment. The PMK is simply cached in the controller(s) and made available to all APs that connect to it. The PMK is also shared with all other controllers that make up a mobility group with the anchor controller.

Figure 4-12 Proactive Key Caching Architecture



Cisco Centralized Key Management (CCKM) is a Cisco standard supported by Cisco Compatible Extensions clients to provide fast secure roaming (FSR). The principle mechanism for accelerating the roaming process is the same as PKC, which is to use a cached PMK. However, the implementation in CCKM is slightly different, which makes the two mechanisms incompatible with each other.

The state of the key cache for each WLAN client can be seen with the **show pmk-cache all** command. This identifies which clients are caching the keys, and which key caching mechanism is being used.

The 802.11r workgroup is responsible for the standardization of an FSR mechanism for 802.11. The WLC controller supports both CCKM and PKC on the same WLAN -802.1x+CCKM, as shown in the following example:

```
WLAN Identifier.................................. 1
Network Name (SSID).............................. wpa2
…
Security
   802.11 Authentication:........................ Open System
   Static WEP Keys.............................. Disabled
   802.1X....................................... Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE).............................. Disabled
      WPA2 (RSN IE)............................. Enabled
         TKIP Cipher............................ Disabled
         AES Cipher............................. Enabled
   Auth Key Management
         802.1x................................. Enabled
         PSK.................................... Disabled
         CCKM................................... Enabled
…
(Cisco Controller) >show pmk-cache all
PMK-CCKM Cache
                              Entry
Type        Station           Lifetime   VLAN Override        IP Override
------    --------------    --------   ------------------   ---------------
CCKM    00:12:f0:7c:a3:47   43150                             0.0.0.0
RSN    00:13:ce:89:da:8f    42000                             0.0.0.0
```

Cisco Unified Wireless Network Architecture

Figure 4-13 shows a high level topology of the Cisco Unified Wireless Network Architecture, which includes Lightweight Access Point Protocol (LWAPP) access points (LAPs), mesh LWAPP APs (MAPs), the Wireless Control System (WCS), and the Wireless LAN Controller (WLC). Alternate WLC platforms include the Wireless LAN Controller Module (WLCM) and the Wireless Services Module (WiSM). The Cisco Access Control Server (ACS) and its Authentication, Authorization, and Accounting (AAA) features complete the solution by providing RADIUS services in support of wireless user authentication and authorization.

Figure 4-13 Cisco Unified Wireless Network Architecture

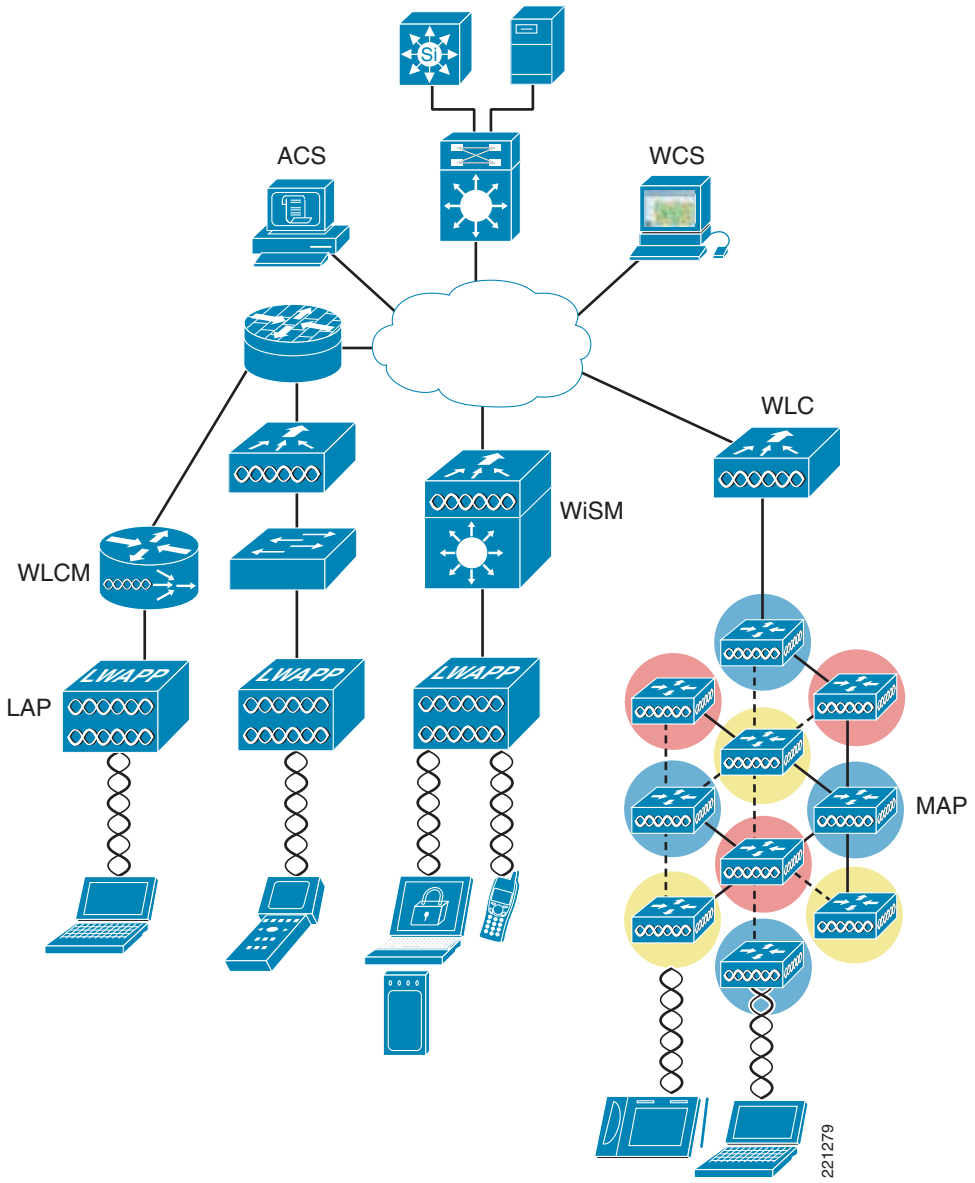
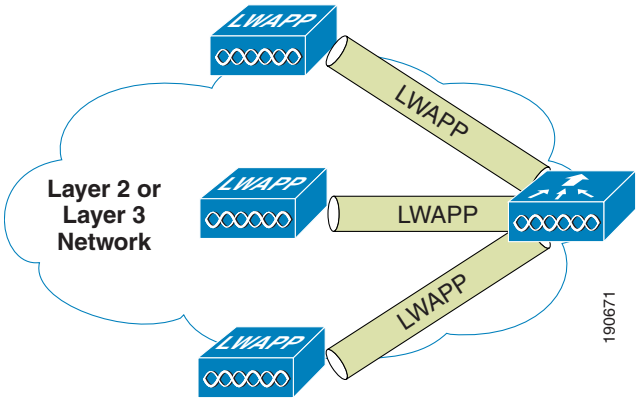


Figure 4-14 illustrates one of the primary features of the architecture: how LAPs use the LWAPP protocol to communicate with and tunnel traffic to a WLC.

Figure 4-14 LAP and WLC Connection



LWAPP has three primary functions:

- Control and management of the LAP
- Tunneling of WLAN client traffic to the WLC
- Collection of 802.11 data for the management of the Cisco Unified Wireless System

LWAPP Features

The easier a system is to deploy and manage, the easier it will be to manage the security associated with that system. Early implementers of WLAN systems that used “fat” APs (standalone) found that the implementation and configuration of such APs is equivalent to deploying and managing hundreds of individual firewalls, each requiring constant attention to ensure correct firmware, configuration, and safeguarding. Even worse, APs are often deployed in physically unsecured areas where theft of an AP could result in someone accessing its configuration to gain information to aid in some other form of malicious activity.

LWAPP addresses deployment, configuration, and physical security issues by doing the following:

- Removing direct user interaction and management of the AP. Instead, the AP is managed by the WLC through its LWAPP connection. This moves the configuration and firmware functions to the WLC, which can be further centralized through the use of the WCS.
- Having the AP download its configuration from the WLC, and be automatically updated when configuration changes occur on the WLC.
- Having the AP synchronize its firmware with its WLC, ensuring that the AP is always running the correct software version.
- Storing sensitive configuration data at the WLC, and storing only IP address information on the AP. In this way, if the AP is physically compromised, there is no configuration information resident in NVRAM that can be used to perform further malicious activity.
- Mutually authenticating LAPs to WLCs, and AES encrypting the LWAPP control channel.

In addition to the security benefits described above, tunneling WLAN traffic in an LWAPP-based architecture improves the ease of deployment without compromising the overall security of the solution. LAPs that support multiple WLAN VLANs can be deployed on access layer switches without requiring

dot1q trunking or adding additional client subnets at the access switches. All WLAN client traffic is tunneled to centralized locations (where the WLC resides), making it simpler to implement enterprise-wide WLAN access and security policies.

Cisco Unified Wireless Security Features

The native 802.11 security features combined with the physical security and ease of deployment of an LWAPP architecture serves to improve the overall security of WLAN deployments. In addition to the inherent security benefits offered by the LWAPP protocol described above, the Cisco Unified Wireless solution also includes the following additional security features:

- Enhanced WLAN security options
- ACL and firewall features
- Dynamic Host Configuration Protocol (DHCP) and Address Resolution Protocol (ARP) protection
- Peer-to-peer blocking
- Wireless intrusion detection system (IDS)
  - Client exclusion
  - Rogue AP detection
- Management frame protection
- Dynamic radio frequency management
- Architecture integration
- IDS integration

Enhanced WLAN Security Options

The Cisco Unified Wireless Network solution supports multiple concurrent WLAN security options. For example, multiple WLANs can be created on a WLC, each with its own WLAN security settings that can range from an open guest WLAN network and WEP networks for legacy platforms to combinations of WPA and/or WPA2 security configurations.

Each WLAN SSID can be mapped to either the same or different dot1q interface on the WLC, or Ethernet over IP (EoIP) tunneled to a different controller through a mobility anchor (Auto Anchor Mobility) connection.

If a WLAN client authenticates via 802.1x, a dot1q VLAN assignment can be controlled via RADIUS attributes passed to the WLC up successful authenticaiton.

Figure 4-15 and Figure 4-16 show a subset of the Unified Wireless WLAN configuration screen. The following three main configuration items appear on this sample screen:

- The WLAN SSID
- The WLC interface to which the WLAN is mapped
- The security method (additional WPA and WPA2 options are on this page, but are not shown)

Figure 4-15 WLAN General Tab

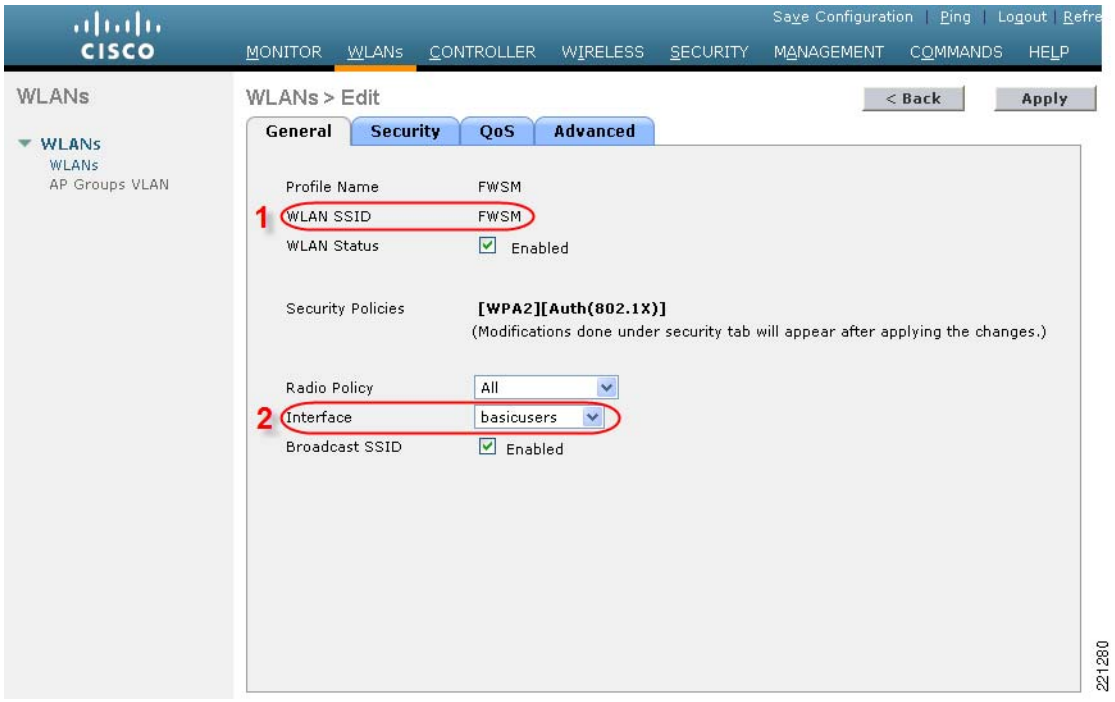
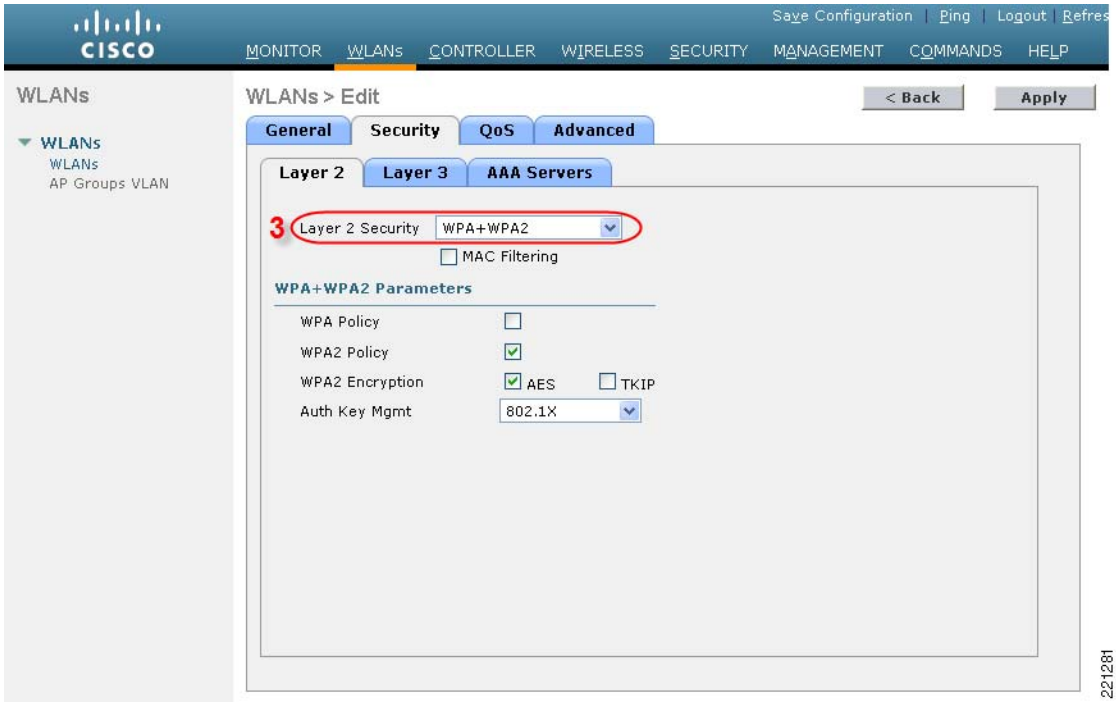


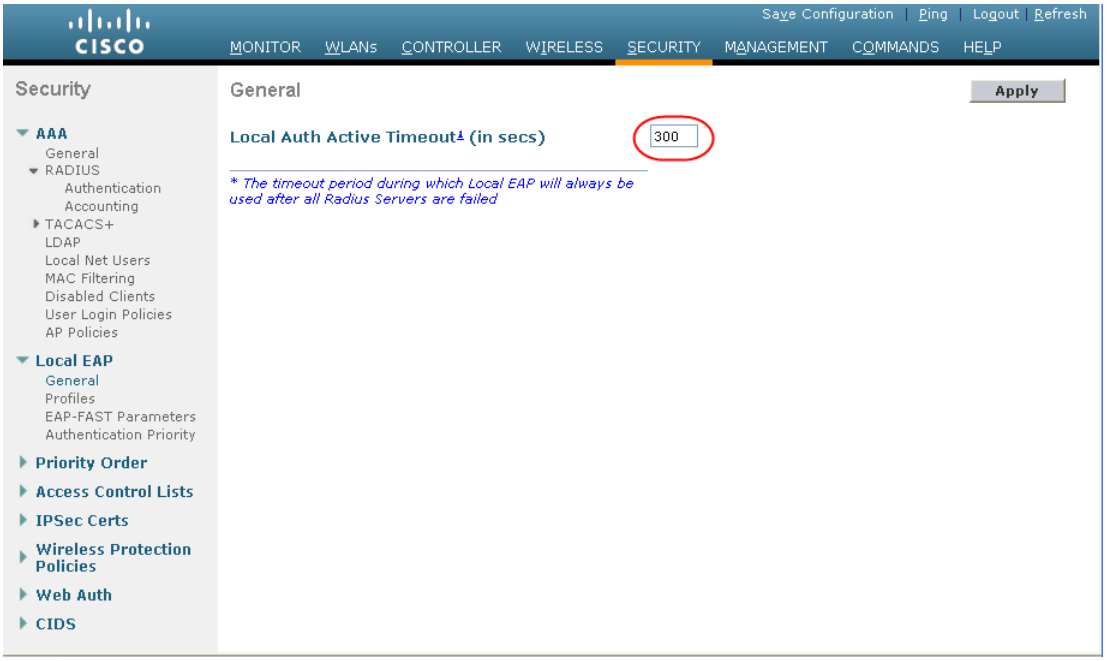
Figure 4-16 WLAN Layer 2 Security Tab



Local EAP Authentication

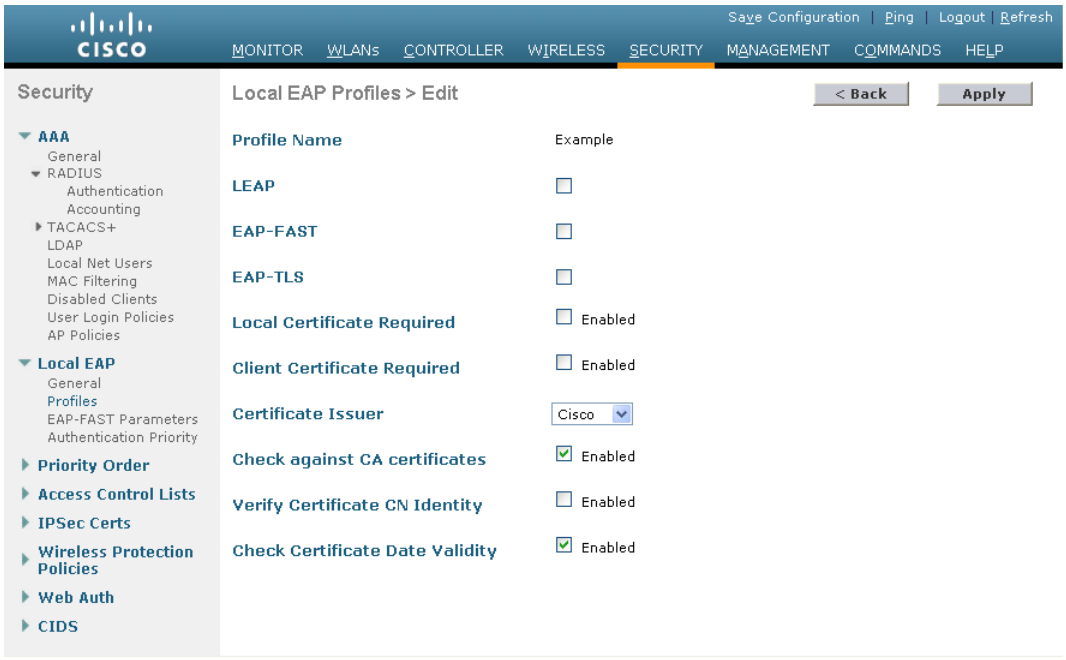
The 4.1 WLC software release provides local EAP authentication capabilities, which can be used when an external RADIUS server is not available or becomes unavailable. The delay before switching to local authentication is configurable, as shown in Figure 4-17. When RADIUS server availability is restored, the WLC automatically switches back from local authentication to RADIUS server authentication.

Figure 4-17 Local Auth Timeout



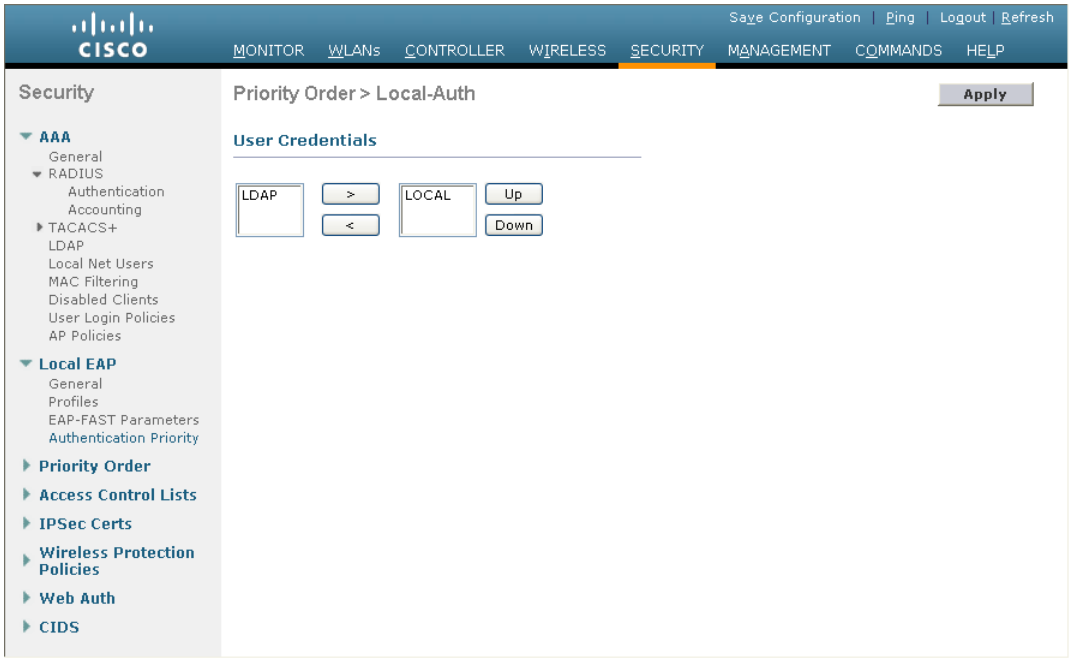
The EAP types supported locally on the WLC are LEAP, EAP-FAST, and EAP-TLS. Examples of local EAP profiles are shown in Figure 4-18.

Figure 4-18 Local EAP Profiles



A WLC can use its local database for authentication data, and it can also access an LDAP directory to provide data for EAP-FAST or EAP-TLS authentication. The user credential database priority (LDAP versus Local) is configurable, as shown in Figure 4-19.

Figure 4-19 Local EAP Priority



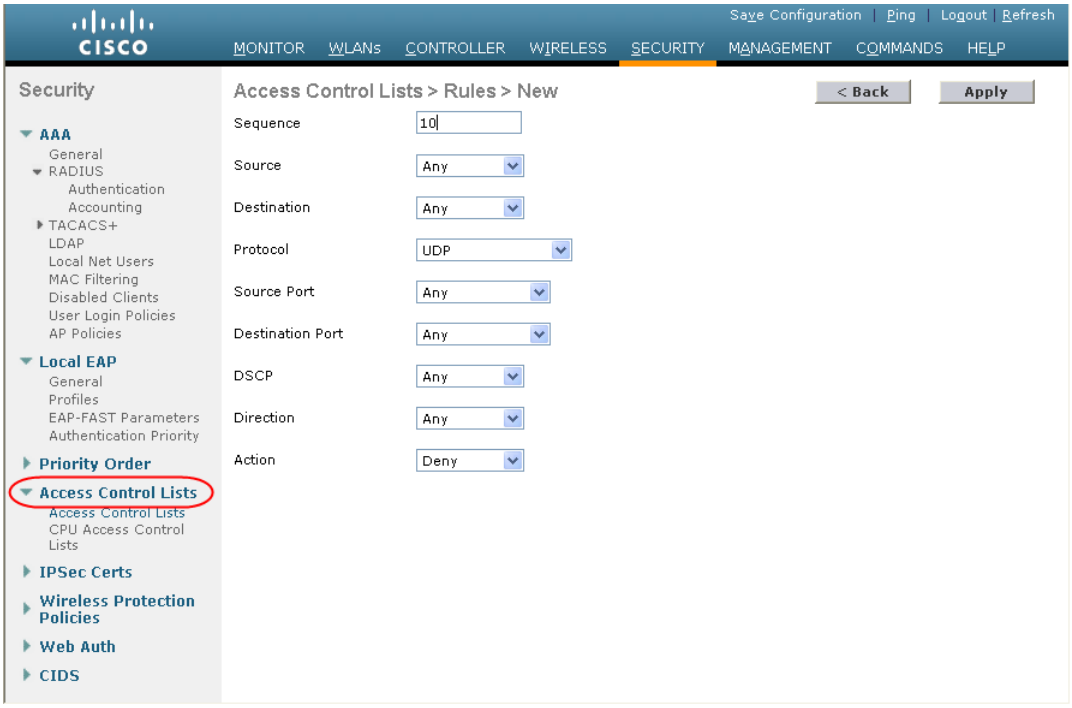
ACL and Firewall Features

The WLC allows access control lists (ACLs) to be defined for any interface configured on the WLC, as well as ACLs to be defined for the CPU of the WLC itself. These ACLs can be used to enforce policy on specific WLANs to limit access to particular addresses and/or protocols, as well as to provide additional protection to the WLC itself.

Interface ACLs act on WLAN client traffic in and out of the interfaces to which the ACLs are applied. CPU ACLs are independent of interfaces on the WLC, and are applied to all traffic to and from the WLC system.

Figure 4-20 shows the ACL Configuration page. The ACL can specify source and destination address ranges, protocols, source and destination ports, differentiated services code point (DSCP), and direction in which the ACL is to be applied. An ACL can be created out of a sequence of various rules.

Figure 4-20 ACL Configuration Page



DHCP and ARP Protection

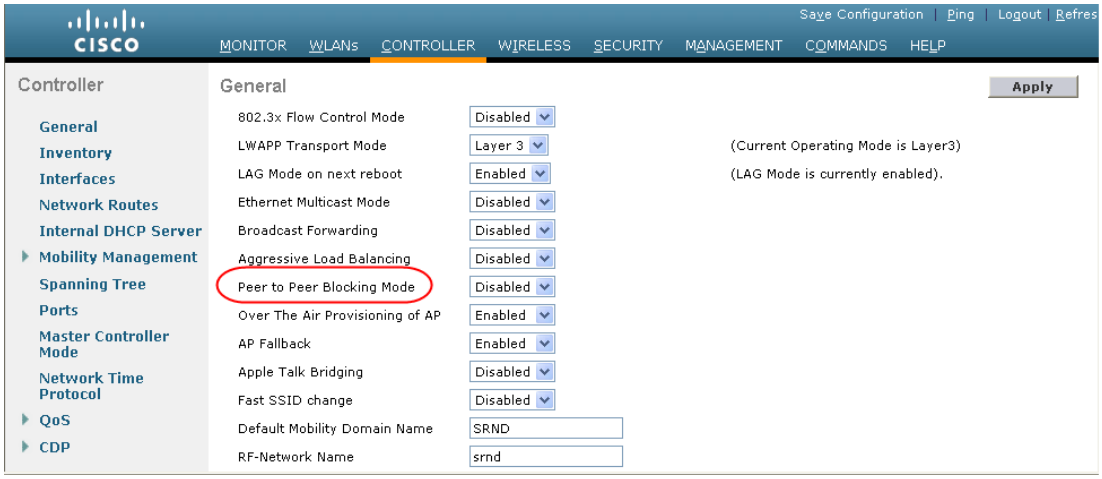
The WLC acts as a relay agent for WLAN client DHCP requests. In doing so, the WLC performs a number of checks to protect the DHCP infrastructure. The primary check is to verify that the MAC address included in the DHCP request matches the MAC address of the WLAN client sending the request. This protects against DHCP exhaustion attacks, by restricting a WLAN client to one DHCP request (IP address) for its own interface. The WLC by default does not forward broadcast messages from WLAN clients back out onto the WLAN, which prevents a WLAN client from acting as a DHCP server and spoofing incorrect DHCP information.

The WLC acts as an ARP proxy for WLAN clients by maintaining the MAC address-IP address associations. This allows the WLC to block duplicate IP address and ARP spoofing attacks. The WLC does not allow direct ARP communication between WLAN clients. This also prevents ARP spoofing attacks directed at WLAN client devices.

Peer-to-Peer Blocking

The WLC can be configured to block communication between clients on the same WLAN. This prevents potential attacks between clients on the same subnet by forcing communication through the router. Figure 4-21 shows the configuration of peer-to-peer blocking on the WLC. Note that this is a global setting on the WLC and applies to all WLANs configured on the WLC.

Figure 4-21 Peer-to-Peer Blocking



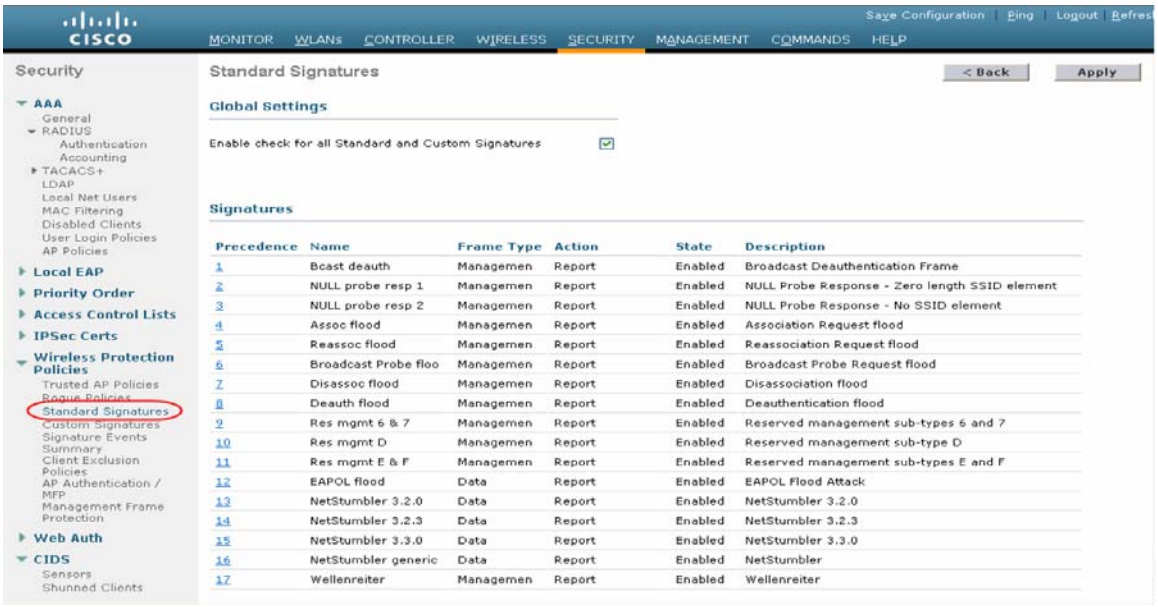
Wireless IDS

The WLC performs WLAN IDS analysis using information obtained from all of the connected LAPs, and reports detected attacks to WLC as well to the WCS. The Wireless IDS analysis is complementary to any analysis that may otherwise be performed by a wired network IDS system. The embedded Wireless IDS capability of the WLC analyzes 802.11and WLC-specific information that is not otherwise visible or available to a wired network IDS system.

The wireless IDS signature files used by the WLC are included in WLC software releases; however, they can be updated independently using a separate signature file. Custom signatures are displayed in the Custom Signatures window.

Figure 4-22 shows the Standard Signatures window on the WLC.

Figure 4-22 Standard WLAN IDS Signatures

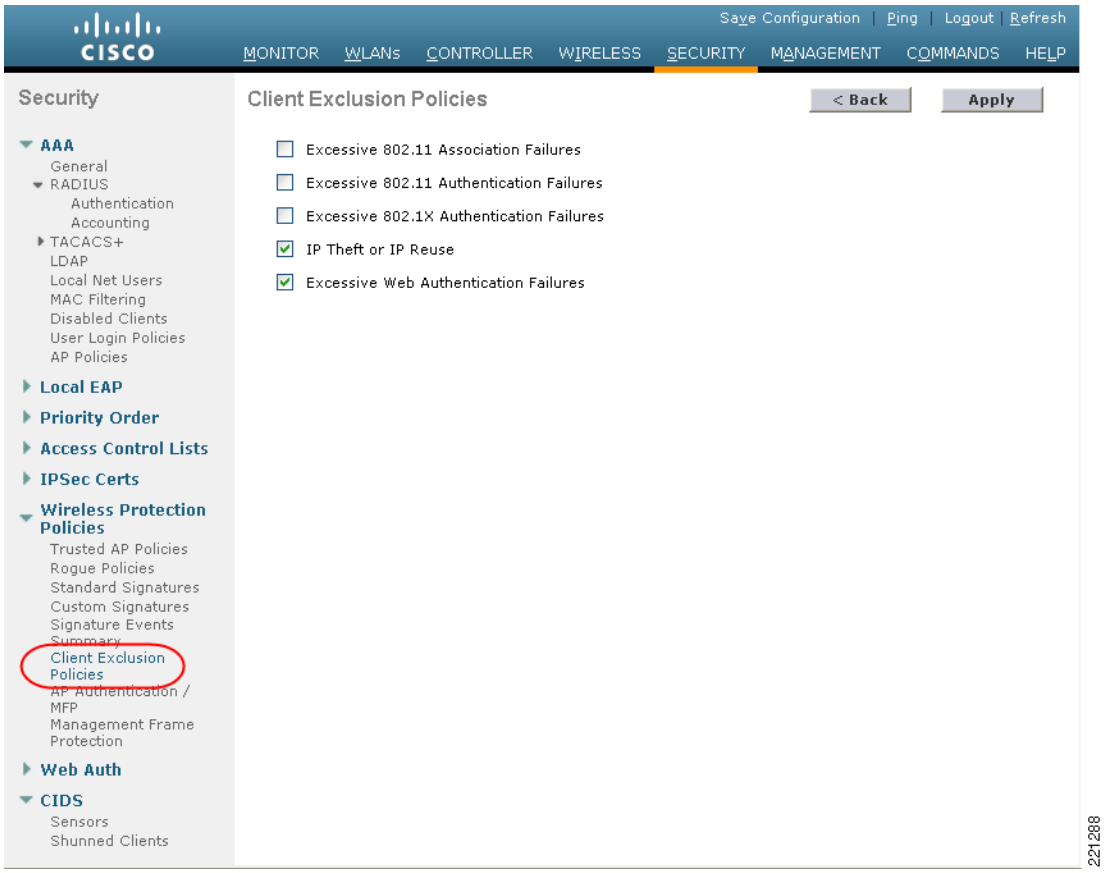


Client Exclusion

In addition to Wireless IDS, the WLC is able to take additional steps to protect the WLAN infrastructure and WLAN clients. The WLC is able to implement policies that exclude WLAN clients whose behavior is considered threatening or inappropriate. Figure 4-23 shows the Exclusion Policies window, containing the following currently supported client exclusion policies:

- Excessive 802.11 association failures—Possible faulty client or DoS attack
- Excessive 802.11 authentication failures—Possible faulty client or DoS attack
- Excessive 802.1X authentication failures—Possible faulty client or DoS attack
- External policy server failures—Network-based IPS server identified client for exclusion
- IP theft or IP reuse—Possible faulty client or DoS attack
- Excessive web authentication failures—Possible DoS or password-cracking attack

Figure 4-23 Client Exclusion Policies

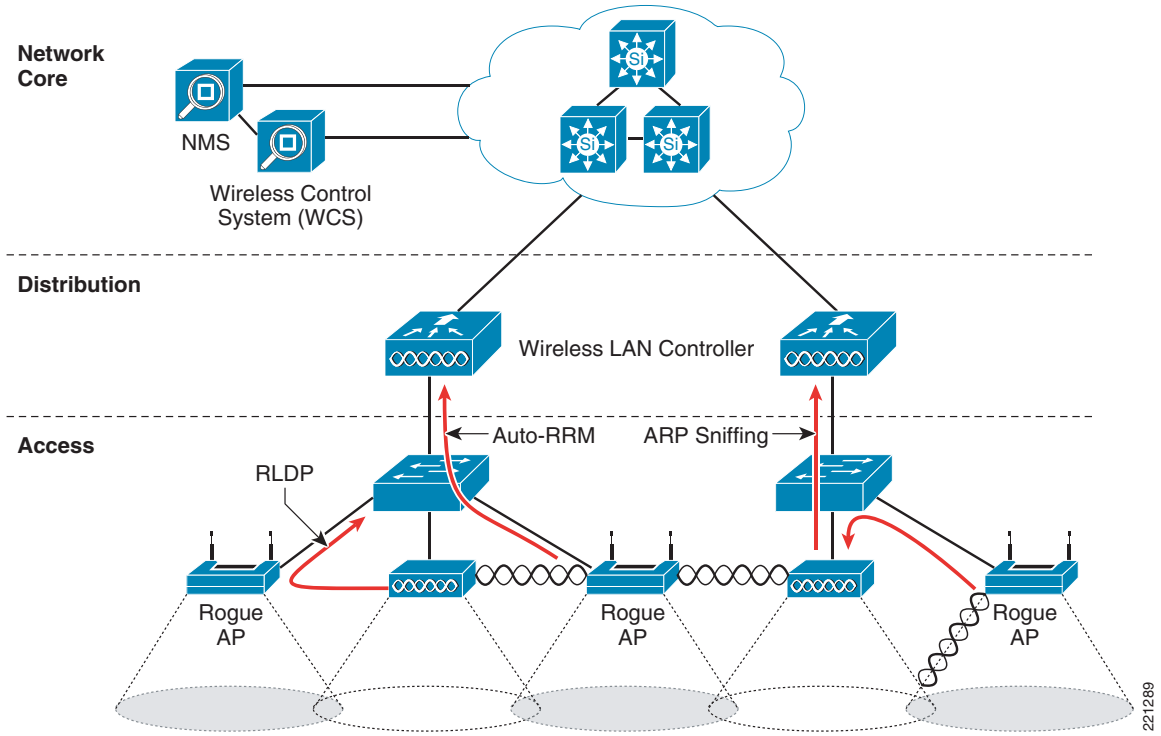


Rogue AP

The Cisco Unified Wireless Networking solution provides a complete rogue AP solution, shown in Figure 4-24, which provides the following:

- Air/RF detection—Detection of rogue devices by observing/sniffing beacons and 802.11 probe responses
- Rogue AP location—Use of the detected RF characteristics and known properties of the managed RF network to locate the rogue device
- Wire detection—A mechanism for tracking/correlating the rogue device to the wired network
- Rogue AP isolation —A mechanism to prevent client connection to a rogue AP

Figure 4-24 Unified Wireless Rogue AP Detection



Air/RF Detection

There are two AP RF detection deployment models:

- Standard AP deployment
- Monitor mode AP deployment

Both deployment models support RF detection and are not limited to rogue APs, but can also capture information upon detection of ad-hoc clients and rogue clients (the users of rogue APs). An AP that is configured for monitor is dedicated to scanning the RF channels and does not support client association or data transmission.

When searching for rogue APs, a LAP goes off channel for 50 ms to listen for rogue clients, and to monitor for noise and channel interference. The channels to be scanned are configured in the global WLAN network parameters for 802.11a and 802.11b/g. Any detected rogue clients and/or access points are sent to the controller, which gathers the following information:

- Rogue AP MAC address
- Rogue AP name
- Rogue connected client(s) MAC address
- Whether the frames are protected with WPA or WEP
- The preamble
- Signal-to-noise ratio (SNR)
- Received signal strength indication (RSSI)

The WLC then waits before it "labels" a prospective client or AP as a rogue, until it has been reported by another AP, or until it completes another detection cycle. The same AP again moves to the same channel to monitor for rogue access points/clients, noise, and interference. If the same clients and/or access points are detected, they are identified as a rogue on the WLC. The WLC then begins to determine whether this rogue is attached to the local network or is simply a neighboring AP. In either case, an AP that is not part of the managed Unified Wireless network is considered a rogue.

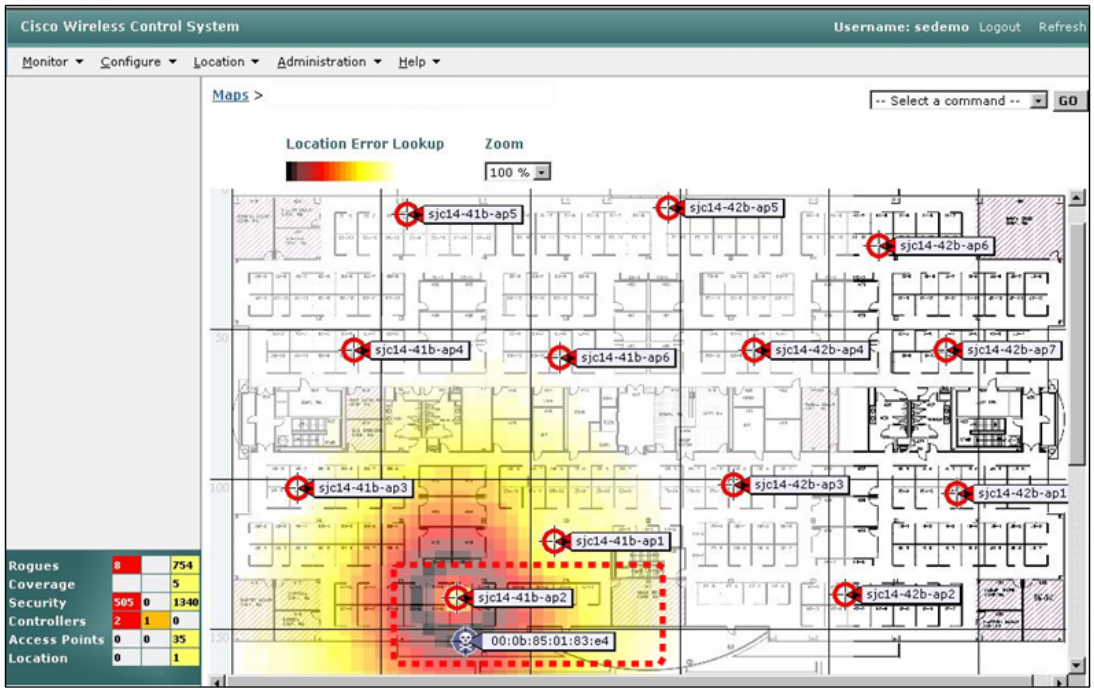
In monitor mode, the AP does not carry user traffic but spends all its time scanning channels. This mode of deployment is most common when a customer does not want to support WLAN services in a particular area, but wants to monitor that area for rogue APs and rogue clients.

Location

The location features of the WCS can be used to provide a floor plan indicating the approximate location of a rogue AP. An example of this is shown in Figure 4-25. The floor plan shows the location of all legitimate APs, and highlights the location of a rogue AP using the skull-and-crossbones icon.

For more information on the Cisco Unified Wireless Location features, see the following URL: http://www.cisco.com/en/US/products/ps6386/index.html.

Figure 4-25 Rogue AP Mapping



Wire Detection

Situations may exist where the WCS rogue location features described above are not effective, such as in branch offices that contain only a few APs or where accurate floor plan information may not be available. In those cases, the Cisco Unified Wireless solution offers two other "wire"-based detection options:

- Rogue detector AP

- Rogue Location Discovery Protocol (RLDP)

If an AP is configured as a rogue detector, its radio is turned off and its role is to listen on the wired network for MAC addresses of clients associated to rogue APs; that is, rogue clients. The rogue detector listens for ARP packets that include these rogue client MAC addresses. When it detects one of these ARPs, it reports this to the WLC, providing verification that the rogue AP is attached to the same network as the Cisco Unified Wireless Network. To be effective at capturing ARP information, the rogue AP detector should be connected to all available broadcast domains using a Switched Port Analyzer (SPAN) port because this maximizes the likelihood of detection. Multiple rogue AP detector APs may be deployed to capture the various aggregated broadcast domains that exist on a typical network.

If a rogue client resides behind a wireless router (a common home WLAN device), their ARP requests are not seen on the wired network, so an alternative to the rogue detector AP method is needed. Additionally, rogue detector APs may not be practical for some deployments because of the large number of broadcast domains to be monitored (such as in the main campus network).

The RLDP option can aid in these situations. In this case, a standard LAP, upon detecting a rogue AP, can attempt to associate with the rogue AP as a client and send a test packet to the controller, which requires the AP to stop behaving as a standard AP and temporarily go into client mode. This action confirms that the rogue AP in question is actually on the network, and provides IP address information that indicates its logical location in the network. Given the difficulties in deriving location information in branch offices coupled with the likelihood of a rogue being located in multi-tenant buildings, rogue AP detector and RLDP are useful tools that augment location-based rogue AP detection.

Rogue AP Containment

Rogue AP- connected clients, or rogue ad-hoc connected clients, may be contained by sending 802.11 de-authentication packets from nearby LAPs. This should be done only after steps have been taken to ensure that the AP is truly a rogue AP, because it is illegal to do this to a legitimate AP in a neighboring WLAN. This is the reason why Cisco removed the automatic rogue AP containment feature from the solution.

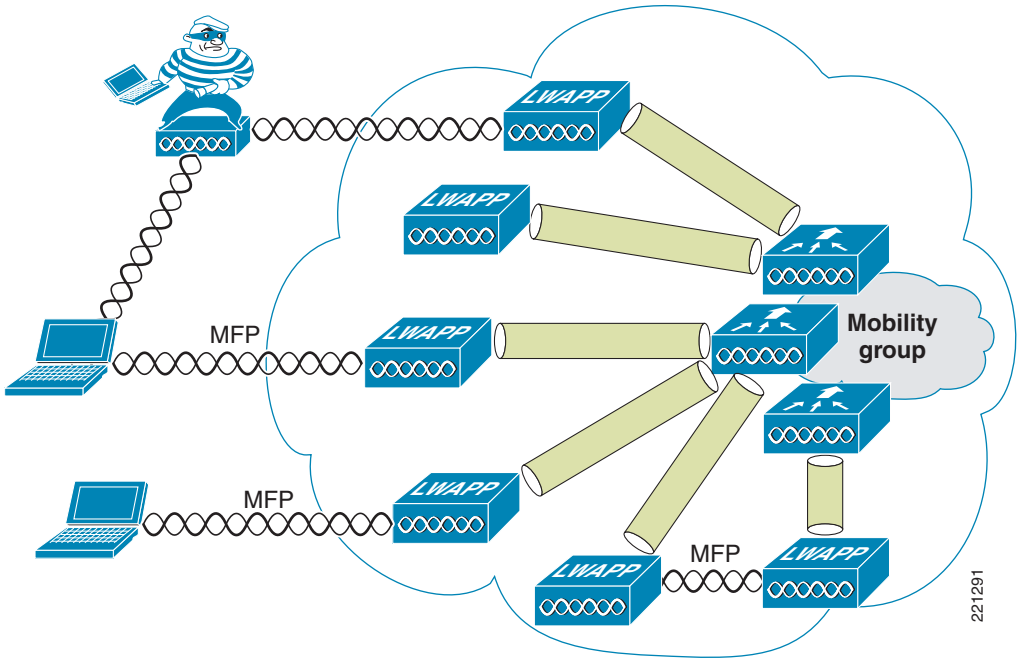
To determine whether rogue AP clients are also clients on the enterprise WLAN, the client MAC address can be compared with MAC addresses collected by the AAA during 802.1X authentication. This allows for the identification of potential WLAN clients that may have been compromised or users who are not following security policies.

Management Frame Protection

One of the challenges in 802.11 has been that management frames are sent in the clear with no encryption or message integrity checking and are therefore vulnerable to spoofing attacks. WLAN management frame spoofing can be used to attack a WLAN network. To address this, Cisco created a digital signature mechanism to insert a message integrity check (MIC) into 802.11 management frames. This allows legitimate members of a WLAN deployment to be identified, as well being able identify rogue infrastructure devices, and spoofed frames through their lack of valid MICs.

The MIC used in management frame protection (MFP) is not a simple CRC hashing of the message, but also includes a digital signature component. The MIC component of MFP ensures that a frame has not been tampered with, and the digital signature component ensures that the MIC could have only been produced by a valid member of the WLAN domain. The digital signature key used in MFP is shared among all controllers in a mobility group; different mobility groups have different keys. This allows the validation of all WLAN management frames processed by the WLCs in that mobility group. (See Figure 4-26.)

Figure 4-26 Management Frame Protection



Both infrastructure-side and client MFP are currently possible, but client MFP requires Cisco Compatible Extensions v5 WLAN clients to be able to learn the mobility group MFP key before they can detect and reject invalid frames.

MFP provides the following benefits:

- Authenticates 802.11 management frames generated by the WLAN network infrastructure
- Allows detection of malicious rogues that spoof a valid AP MAC or SSID to avoid detection as a rogue AP, or as part of a man-in-the-middle attack
- Increases the effectiveness of the rogue AP and WLAN IDS signature detection of the solution
- Provides protection of client devices using Cisco Compatible Extensions v5
- Supported by standalone AP/WDS/WLSE in version 12.3(8)/v2.13

Two steps are required to enable MFP: enabling it on the WLC (see Figure 4-27) and enabling it on the WLANs in the mobility group (see Figure 4-28).

Figure 4-27 Enabling MFP on the Controller

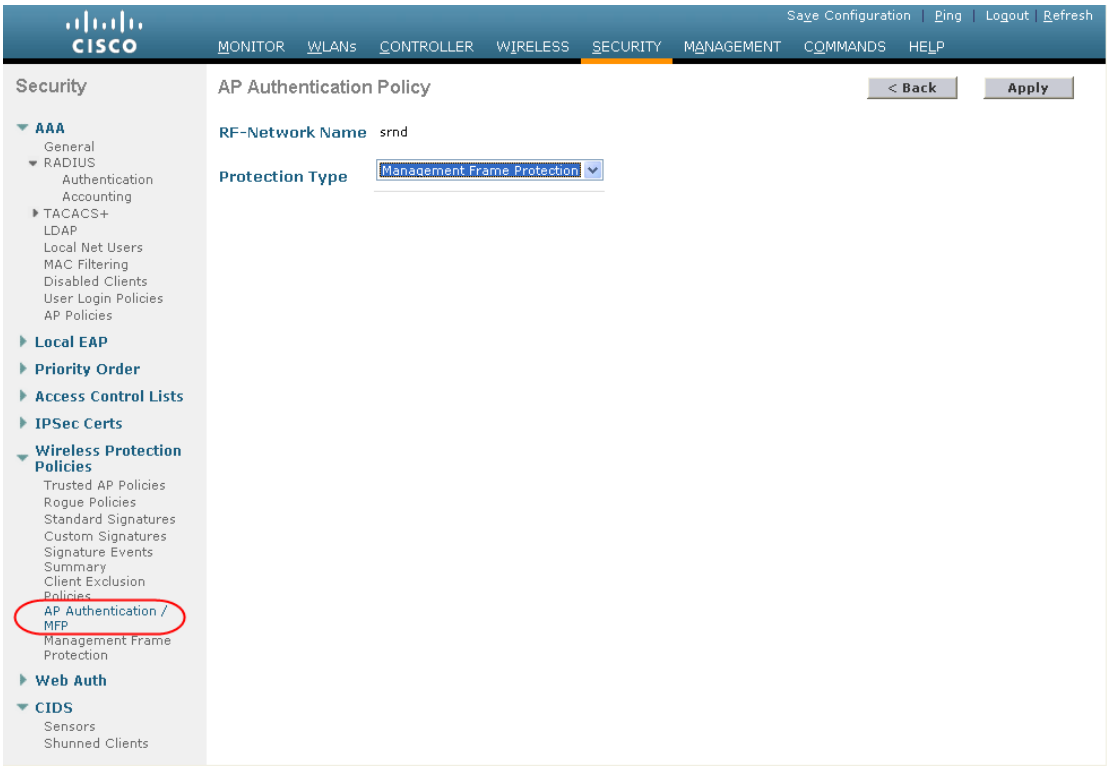
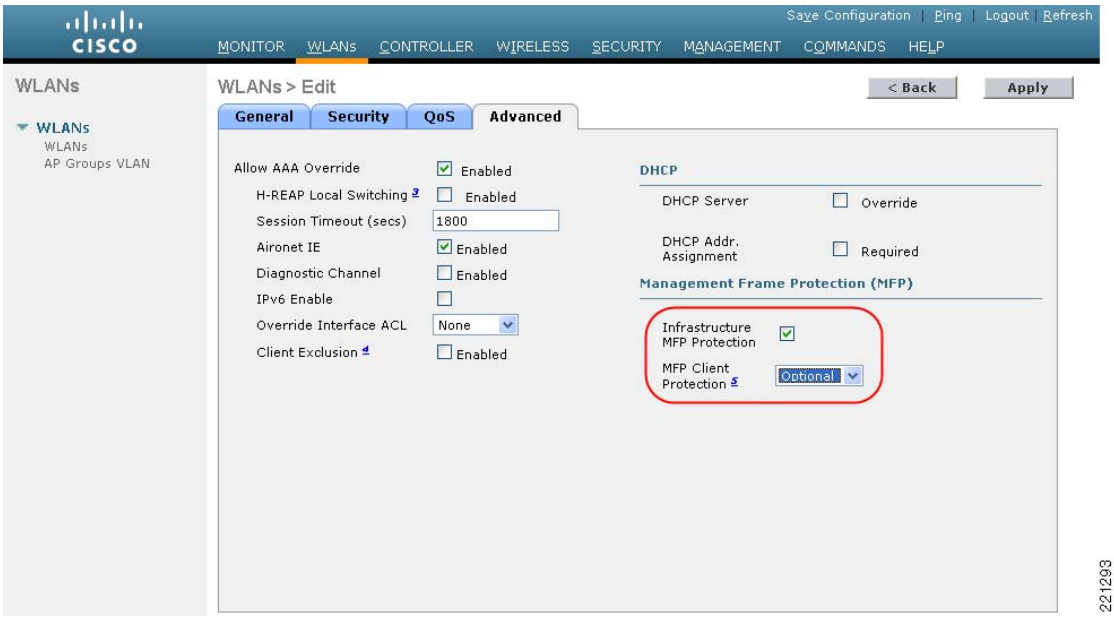


Figure 4-28 Enabling MFP per WLAN



Client Management Frame Protection

Cisco Compatible Extensions v5 WLAN clients support MFP. This is enabled on a per-WLAN basis, as is shown in Figure 4-28.

The method of providing MFP for WLAN clients is fundamentally the same as that used for APs, which is to use a MIC in the management frames. This allows trusted management frames to be identified by the client. MIC cryptographic keys are passed to the client during the WPA2 authentication process. Client MFP is available only for WPA2. If WPA and WPA2 clients share the same WLAN, client MFP must be set to “optional”.

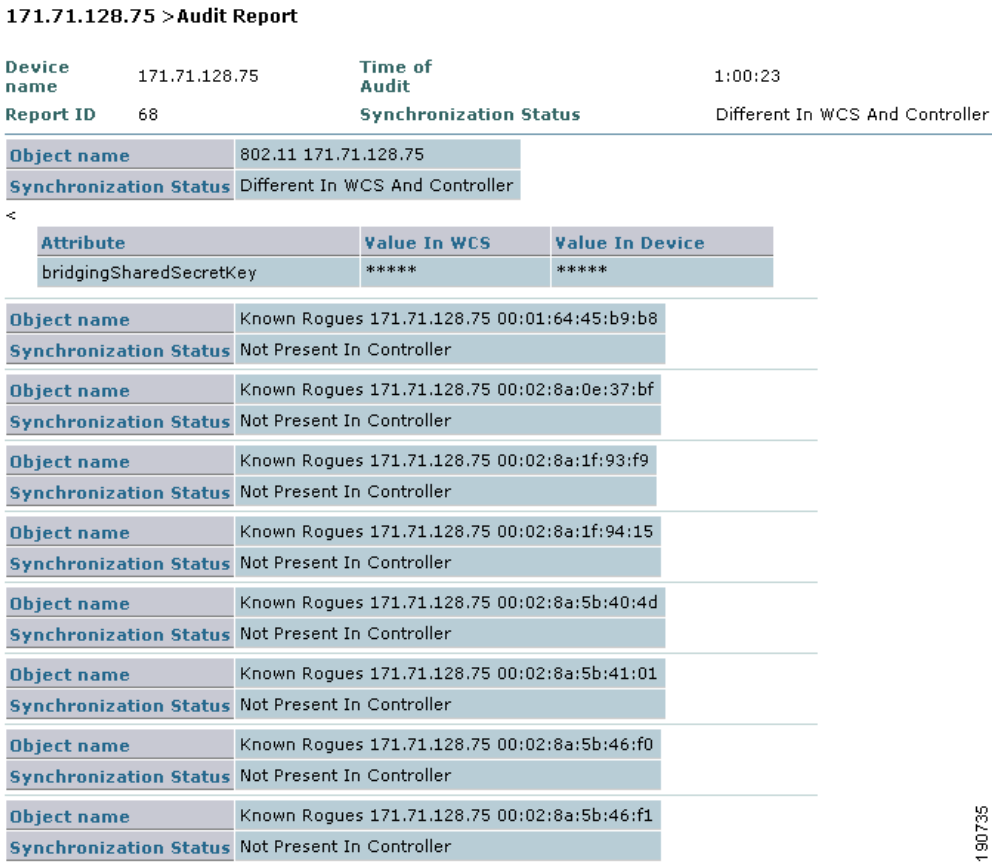
WCS Security Features

Apart from providing location support for Rogue AP detection, the WCS provides two additional Unified Wireless security features: WLC configuration verification management and an alarm and reporting interface.

Configuration Verification

The WCS can provide on-demand or regularly-scheduled configuration audit reports, which compare the complete current running configuration of a WLC and its registered access points with that of a known valid configuration stored in the WCS databases. Any exceptions between the current running configuration and the stored database configuration are noted and brought to the attention of the network administrator via screen reports. (See Figure 4-29.)

Figure 4-29 Audit Report Example



171.71.128.75 >Audit Report

Device name	171.71.128.75	Time of Audit	1:00:23
Report ID	68	Synchronization Status	Different In WCS And Controller

Object name	802.11 171.71.128.75
Synchronization Status	Different In WCS And Controller

<

Attribute	Value In WCS	Value In Device
bridgingSharedSecretKey	*****	*****

Object name	Known Rogues 171.71.128.75 00:01:64:45:b9:b8
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:0e:37:bf
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:1f:93:f9
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:1f:94:15
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:40:4d
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:41:01
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:46:f0
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:46:f1
Synchronization Status	Not Present In Controller

190735

Alarms and Reports

Apart from the alarms that can be generated directly from a WLC and sent to an enterprise network management system (NMS), the WCS can also send alarm notifications. The primary difference between alarm notification methods, apart from the type of alarm sent by the various components, is that the WLC uses Simple Network Management Protocol (SNMP) traps to send alarms (which can be interpreted only by an NMS system), whereas the WCS uses Simple Mail Transfer Protocol (SMTP) e-mail to send an alarm message to an administrator.

WCS provides both real-time and scheduled reports, and can export or e-mail reports. The WCS provides reports on the following:

- Access points
- Audits
- Clients
- Inventory
- Mesh
- Performance
- Security

Architecture Integration

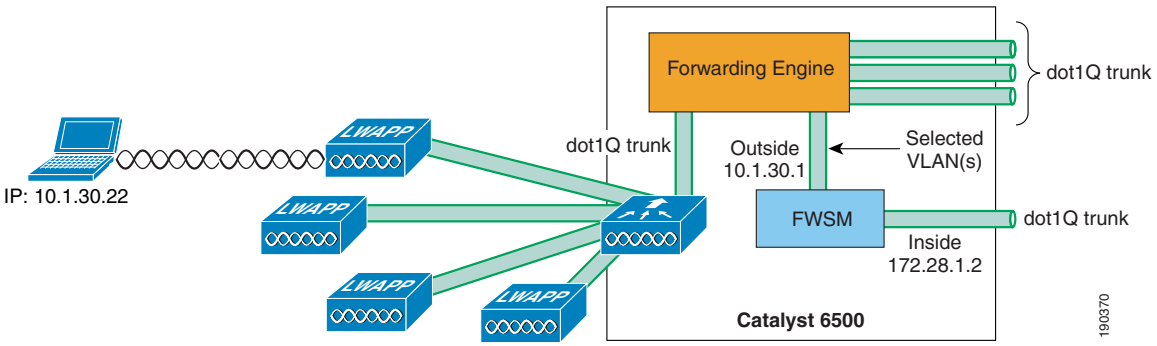
Cisco provides a wide variety of security services that are either integrated into Cisco IOS, integrated into service/network modules, offered as standalone appliances, or as software.

The Cisco Unified Wireless Network architecture eases the integration of these security services into the solution because it provides a Layer 2 connection between the WLAN clients and the upstream wired network. This means that appliances or modules that operate by being "inline" with client traffic can be easily inserted between WLAN clients and the wired network. For example, an older WLSM-based deployment requires the implementation of VRF-Lite on the Cisco 6500 to enable WLAN client traffic to flow through a Cisco Firewall Service Module (FWSM); whereas in a Cisco Unified WLAN deployment, a WiSM can simply map the (WLAN) client VLAN directly to the FWSM. The only WLAN controllers in the Cisco Unified Wireless portfolio that cannot directly map WLAN traffic to a physical/logical interface at Layer 2 are ISR-based WLC modules. An ISR WLAN module does have access to all the IOS and IPS features available on the ISR, but IP traffic from the WLAN clients must be directed in and out specific ISR service module interfaces using IOS VRF features on the router.

Figure 4-30 shows an example of architectural integration between a WiSM and the FWSM module. In this example, the WLAN client is on the same subnet as the outside firewall interface. No routing policy or VRF configuration is required to ensure that WLAN client traffic in both directions goes through the firewall.

A Cisco Network Admission Control (NAC) Appliance (formerly Cisco Clean Access) can be implemented in combination with a WLAN deployment to ensure that end devices connecting to the network meet enterprise policies for compliance with latest security software requirements and operating system patches. Like the FWSM module discussed above, the Cisco NAC Appliance can also be integrated into a Cisco Unified Wireless Network architecture at Layer 2, thereby permitting strict control over which wireless user VLANs are subject to NAC policy enforcement.

Figure 4-30 Firewall Module Integration Example



In addition to ease of integration at the network layer, the Cisco Unified Wireless Network solution provides integration with Cisco IDS deployments, allowing clients blocked by the Cisco IDS to be excluded from the Cisco Unified Wireless Network.

For more information on the design, and configuration of these solution, as well Cisco Security Agent (CSA) WLAN features, see the *Secure Wireless Design Guide 1.0* at the following URL: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns386/c649/ccmigration_09186a0080871da5.pdf.

Cisco Integrated Security Features

Cisco Integrated Security Features (CISF) are available on Cisco Catalyst switches, and help mitigate against a variety of attacks that a malicious user might launch after gaining wireless access to the network. This section describes these attacks, how a WLC protects against these attacks, and how CISF, when enabled on the access switch, can help protect the network.

Note This section describes only the attacks that CISF can help prevent when enabled on access switches, and is not meant to be a comprehensive analysis of all the possible attacks that are possible on wireless networks.

Types of Attacks

Attacks can occur against either wired or wireless networks. However, a wireless network connection allows an attacker to craft an attack without physical connectivity to the network. The WLC and CISF include features that are specifically designed to prevent such attacks, including the following:

- MAC flooding attacks
- DHCP rogue server attacks
- DHCP exhaustion attacks
  - ARP spoofing attacks
  - IP spoofing attacks

MAC Flooding Attack

MAC flooding attacks are attempts to fill the content-addressable memory (CAM) table of a switch, and thus force the switch to start flooding LAN traffic. These attacks are performed with tools such as macof (part of the dsniff package), which generates a flood of frames with random MAC and IP source and destination addresses.

The Layer 2 learning mechanism of an Ethernet switch is based on the source MAC addresses of packets. For each new source MAC address received on a port, the switch creates a CAM table entry for that port and for the VLAN to which the port belongs. The macof utility typically fills the CAM table in less than ten seconds, given the finite memory available to store these entries on the switch. CAM tables are limited in size. If enough entries are entered into the CAM table before other entries expire, the CAM table fills up to the point that no new entries can be accepted.

When the switch CAM table of a switch is filled, it then floods all its ports with incoming traffic because it cannot find the port number for a particular MAC address in the CAM table. The switch, in essence, acts like a hub to the detriment of performance and security. The overflow floods traffic within the local VLAN, so the intruder sees traffic within the VLAN to which he or she is connected.

At Layer 3, the random IP destinations targeted by macof also use the multicast address space. Thus, the distribution layer switches that have multicast turned on experience high CPU usage levels as the protocol independent multicast (PIM) process attempts to handle the false routes.

DHCP Rogue Server Attack

The DHCP rogue server event may be the result of a purposeful attack, or a user may have accidentally brought up a DHCP server on a network segment and begun to inadvertently issue IP addresses. An intruder may bring up a DHCP server and offer IP addresses representing a DNS server or default gateway that redirects unsuspecting user traffic to a computer under the control of the intruder.

DHCP Starvation Attack

DHCP starvation attacks are designed to deplete all of the addresses within the DHCP scope on a particular segment. Subsequently, a legitimate user is denied an IP address requested via DHCP and thus is not able to access the network. Gobbler is a public domain hacking tool that performs automated DHCP starvation attacks. DHCP starvation may be purely a DoS mechanism or may be used in conjunction with a malicious rogue server attack to redirect traffic to a malicious computer ready to intercept traffic.

ARP Spoofing-based Man-In-the-Middle Attack

A man-in-the-middle (MIM) attack is a network security breach in which a malicious user intercepts (and possibly alters) data traveling along a network. One MIM attack uses ARP spoofing, in which a gratuitous Address Resolution Protocol (ARP) request is used to misdirect traffic to a malicious computer such that the computer becomes the “man in the middle” of IP sessions on a particular LAN segment. The hacking tools ettercap, dsniff, and arpspoof may be used to perform ARP spoofing. Ettercap in particular provides a sophisticated user interface that displays all the stations on a particular LAN segment and includes built-in intelligent packet capturing to capture passwords on a variety of IP session types.

IP Spoofing Attack

IP spoofing attacks spoof the IP address of another user to perform DoS attacks. For example, an attacker can ping a third-party system while sourcing the IP address of the second party under attack. The ping response is directed to the second party from the third-party system.

CISF for Wireless Deployment Scenarios

This section describes the various unified wireless deployment scenarios used. The following section describes how the WLC or CISF features defend against wireless attacks.

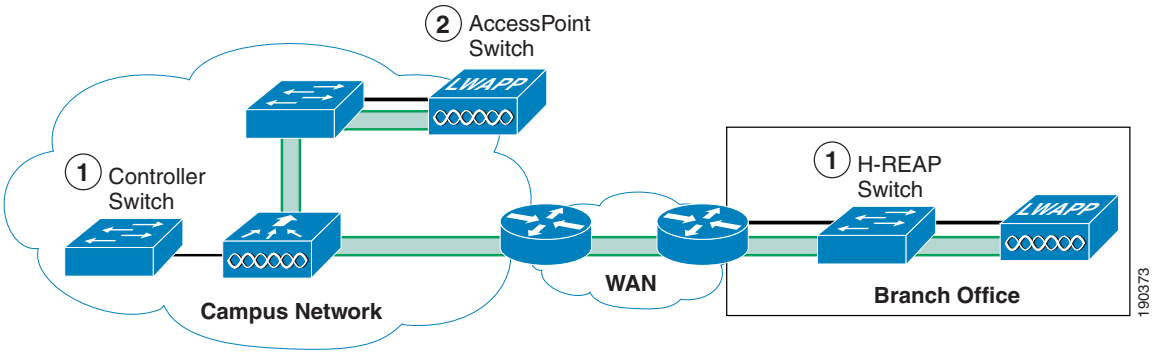
CISF is currently available only on the access switch, not directly on the access point (AP); thus, the benefits of these features are available only if the traffic from the wireless attacker goes through the switch.

The definition of an access switch is slightly different in the Unified Wireless solution, because three locations can be considered an access switch:

- The point that a controller interface terminates on the network
- The point that a standard LAP terminates on the network
- The point that an hybrid remote edge access point (H-REAP) terminates on the network

These locations are illustrated in Figure 4-31.

Figure 4-31 Access Switches



The connections of interest to CISF are the controller switch and the H-REAP switch. The AP switch is not discussed because WLAN traffic does not terminate on this switch, and the AP simply appears as a single device connected to that switch port, so from a security point of view it can be considered an access client.

Note The primary difference between the LAP and a standard client is that the differentiated services code point (DSCP) value of a LAP should be trusted.

The scope of the following scenarios is limited to attacks between wireless users because it is assumed that wireless and wired users are supported on separate subnets (as recommended by Cisco best practices) and because any discussion of inter-subnet attacks is beyond the scope of this discussion.

The three following scenarios are considered:

- Scenario 1—Target is associated to the same AP to which the attacker is connected
- Scenario 2—Target is associated to a different AP than the attacker
- Scenario 3—Target is associated to a different AP than the attacker, and this AP is connected to a different controller

For Scenario 1, in which both attacker and target are associated to the same AP, the traffic remains local to the H-REAP or WLC, and CISF is not useful, but the Cisco Unified Wireless Networks native security address these issues. The second and third scenarios are the ones in which CISF can be effective.

For an enterprise WLAN deployment requiring different levels of authorization, multiple VLANs per SSID are commonly used. This requires configuring an 802.1q trunk between the Fast Ethernet port on the H-REAP AP or WLC, and the corresponding port on the access switch. With multiple VLANs defined, the administrator can keep the data traffic separated from the AP and WLC management traffic. The company security policy is also likely to require having different types of authentication and encryptions for different type of users (open authentication and no encryption for guest access, dot1x authentication and strong encryption for employees, and so on). This is achieved by defining multiple SSIDs and VLANs on the H-REAP AP or WLC.

Given the above, the configurations used in the test configurations assume a trunk connection between the WLC or H-REAP AP and the access switch.

Using CISF for Wireless Features

This section describes each of the features provided within CISF that were tested for protection against wireless attacks.

Using Port Security to Mitigate a MAC Flooding Attack

Port security sets a maximum number of MAC addresses allowed on a port. You can add addresses to the address table manually, dynamically, or by a combination of the two. Packets are dropped in hardware when the maximum number of MAC addresses in the address table is reached, and a station that does not have a MAC address in the address table attempts to send traffic.

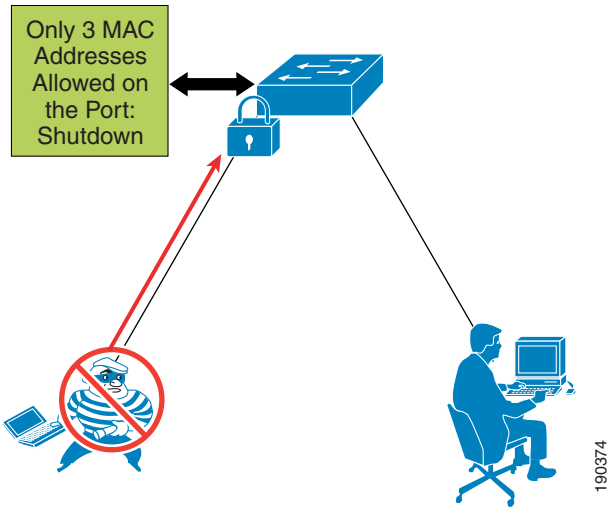
Enabling port security on the access port of the switch stops a MAC flooding attack from occurring because it limits the MAC addresses allowed through that port. If the response to a violation is set to **shutdown**, the port goes to error-disable state. If the response is set to **restrict**, traffic with unknown source MAC addresses are dropped.

Port Security in a Wireless Network

It is not generally recommended to enable port security on a switch port connected to an H-REAP AP or WLC. The use of port security implies knowing the exact number of MAC addresses that the switch learns and allows from that port; in the case of an H-REAP AP or WLC, the various source MAC addresses that the switch learns usually correspond to wireless users. Setting port security on the switch port allows only a certain number of users on the wired network.

For example, a company might have a security policy that allows only certain MACs, and a certain number of them, to send traffic through the access point. In this case, a combination of MAC filtering on the H-REAP AP or WLC and port security on the switch ensures that only the selected users access the wired network. Most of the time, however, a company implements a WLAN to facilitate the mobility of the employees, which implies that an H-REAP AP or WLC, at any given time, does not have a predetermined number of users associated with it. Therefore in cases where it is impossible to determine the number of users connected to the AP, enabling port security on the switch port offers no advantages. At worst, it can create an involuntary DoS attack; if the policy for port security is set to shut down the port in the event of a violation. When this happens, all the users connected to that AP lose network connectivity. Figure 4-32 shows an example of using port security to limit a wireless MAC flooding attack by locking down the port and sending an SNMP trap.

Figure 4-32 Using Port Security



Effectiveness of Port Security

Even when port security is not a viable option to stop this attack (as explained), a MAC flooding attack does not succeed if it is launched by a wireless user. The reason for this is the 802.11 protocol itself. Association with an AP is MAC-based; this means that the AP bridges (translational bridge) traffic coming from or going to known users (known MACs). If a MAC flooding attack is launched from a wireless user, all the 802.11 frames with random source MAC addresses that are not associated to the AP are dropped. The only frame allowed is the one with the MAC address of the malicious user, which the switch has probably already learned. Thus, the fundamental behavior of the access point itself prevents the switch from being susceptible to MAC flooding attacks.

Using Port Security to Mitigate a DHCP Starvation Attack

For wired access, port security can currently prevent a DHCP starvation attack launched from a PC connected to a switch that is using a tool such as Gobbler. The inability of the attack to succeed is due more to a limitation of the tool than the mitigation offered by port security. The only reason such an attack fails is that Gobbler uses a different source MAC address to generate a different DHCP request and can be mitigated by port protection.

However, if an attacker is able to use their MAC address in the Ethernet packet and simply changes the MAC address in the DHCP payload (the field is called chaddr), port security would not stop the attack. In this case, all that can currently be done is to try to slow down the attack using a DHCP rate limiter on the switch port.

Wireless DHCP Starvation Attack

In a Unified Wireless deployment, the vulnerability to a DHCP starvation attack depends on whether the WLC terminates the user traffic or an H-REAP terminates the user traffic.

The WLC protects the network from DHCP starvation attacks because it examines DHCP requests to ensure that the client MAC address matches the chaddr. If the addresses do not match, the DHCP request is dropped.

In the case of H-REAP, the user VLAN is terminated locally, the DHCP request does not go through the controller, and an analysis of the chaddr cannot performed. In this case, the same security considerations apply for this method of access as they do for wired access. A smart (wireless) attacker uses the MAC address with which he or she is associated to the AP to generate the random DHCP requests, and then simply changes the requesting MAC address within the DHCP packet payload. To the AP, the packet looks valid because the originating MAC is the same as the MAC used to associate to the AP.

Using DHCP Snooping to Mitigate a Rogue DHCP Server Attack

DHCP snooping is a DHCP security feature that provides security by building and maintaining a DHCP snooping binding table and filtering untrusted DHCP messages. It does this by differentiating between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch. End-user ports can be restricted to sending only DHCP requests and no other type of DHCP traffic. Trusted ports allow any DHCP message to be forwarded. The DHCP snooping table is built per VLAN and ties the IP address/MAC address of the client to the untrusted port. Enabling DHCP snooping prevents users from connecting a non-authorized DHCP server to an untrusted (user-facing) port and start replying to DHCP requests.

DHCP Snooping for Wireless Access

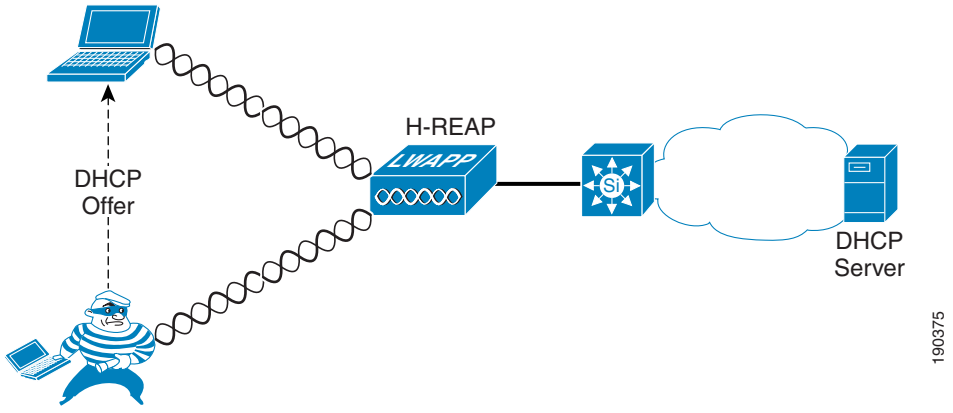
The WLC manages all DHCP requests from clients and acts as a DHCP relay agent. DHCP requests from WLAN clients are not broadcast back out to the WLAN, and they are unicasted from the WLC to a configured DHCP server. This protects other WLAN clients connected to the WLC from rogue DHCP server attacks.

Clients connecting to VLANs via an H-REAP 802.1q trunk interface are not protected against rogue DHCP server attacks.

Keep in mind that the CISF features (in this case DHCP snooping) are implemented on the switch, not on the AP, so the ability of a switch to intercept malicious messages from a rogue server goes only happens if traffic is seen by the switch.

Figure 4-33 shows an example of using DHCP snooping to mitigate against a rogue DHCP server attack, and how an attack can happen before the switch is able to provide DHCP protection.

Figure 4-33 Security Used Against Rogue DHCP Server Attack



Effectiveness of DHCP Snooping

DHCP snooping is enabled on a per-VLAN basis, so it works on a trunk port. A separate DHCP snooping entry is inserted for each DHCP request received on a given trunk port for clients in different VLANs. The fact that DHCP snooping works on trunk ports is very important because it makes this CISF feature applicable to a WLAN deployment where multiple SSIDs/VLANs are configured on the local interface of the H-REAP. If an attacker is associated to the same WLAN/VLAN as the target, but via a different H-REAP, the switch is able to protect against the DHCP spoof attack. However, if the attacker and the target are associated to the same H-REAP, the attack does not traverse the access switch and it is not detected.

DHCP snooping also provides some protection against DHCP server attacks by rate limiting the DHCP requests to the DHCP server.

Using Dynamic ARP Inspection to Mitigate a Man-in-the-Middle Attack

Dynamic ARP Inspection (DAI) is enabled on the access switch on a per-VLAN basis. It compares ARP requests and responses, including gratuitous ARPs (GARPs), with the MAC/IP entries populated by DHCP snooping in the DHCP binding table. If the switch receives an ARP message with no matching entry in the DHCP binding table, the packet is discarded and a log message is sent to the console. DAI prevents ARP poisoning attacks that may lead to MIM attacks such as those launched using ettercap by stopping the GARP messages that the malicious user sends to the target to alter their ARP table and receive their traffic. The ARP messages are filtered directly at the port to which the attacker is connected.

DAI for Wireless Access

The WLC protects against MIM attacks by performing a similar function as DAI on the WLC itself. DIA should not be enabled on the access switch for those VLANs connecting directly to the WLCs because the WLC uses the GARP to support Layer 3 client roaming.

It is possible to enable DAI for each VLAN configured on a trunk between an H-REAP and access switch. Therefore, DAI is useful in wireless deployments where multiple SSIDs/VLANs exist on an H-REAP. However, in an H-REAP deployment, two scenarios can impact the effectiveness of the DAI feature. The following scenarios assume that the attacker is associated to an H-REAP and is Layer 2-adjacent to his/her targets:

- Scenario 1—One of the targets is wireless and associated to the same AP as the attacker while the other target is the default gateway. This is considered to be the most typical attack.
- Scenario 2—Both targets are wireless.

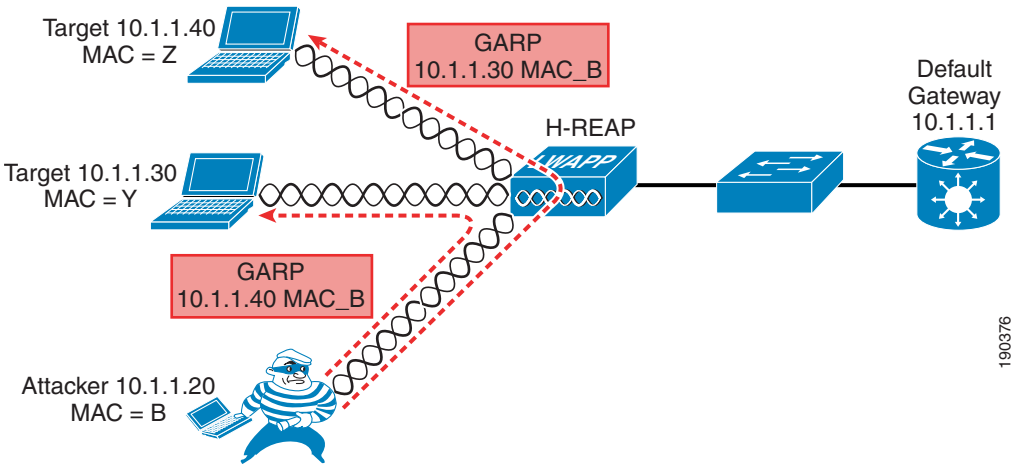
These two scenarios illustrate in which cases the traffic goes through the switch and thus can be stopped.

In Scenario 1, the MIM attack attempts to use a GARP to change the ARP table entries for the default gateway and or a wireless target, to redirect traffic to the attacker. DAI can block a GARP for the default gateway, but DAI has no impact on a spoofed GARP for the wireless client. This limits the effectiveness of the MIM attack, but does not prevent it completely

In Scenario 2, the MIM attack sends GARPs to wireless clients, and the switch implementing DAI does not see these GARPs and cannot block the attack.

Figure 4-34 shows an example of the attack mechanism where GARPs are sent to the two IP connection nodes on the subnet to divert the traffic between them.

Figure 4-34 Dynamic ARP Inspection



Effectiveness of DAI

In the example of Figure 4-34, the attack is completely successful only when the traffic remains local to the H-REAP and never goes through the switch. Usually, the interesting traffic for an attacker, such as passwords and account information, travels from the wireless client to the wired network (server or Internet), so this is not too harmful.

The scenario where the default gateway and a wireless client are the attack targets can be called a half-duplex MIM attack. Ettercap is able to modify the ARP table of the wireless user that is now sending all the traffic to the intruder, but the GARP to the default gateway is intercepted by the switch and a message is logged, as shown in the following example:

```
4507-ESE#sh ip arp inspection log
Total Log Buffer Size : 32
Syslog rate : 5 entries per 1 seconds.
Interface Vlan Sender MAC Sender IP Num of Pkts Reason
---------- ---- -------------- --------------- ----------- ------
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Wed Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Interface Vlan Sender MAC Sender IP Num of Pkts Reason
---------- ---- -------------- --------------- ----------- ------
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:49 PDT Tue Feb 3 2003) DHCP Deny
```

Because the MAC address is provided in the log, the administrator can take further action to block the attack by disassociating the attacker.

When DAI is configured on a VLAN, an ARP rate limiter is configured globally to prevent flooding of ARP requests coming from a certain port. The default value of the rate limiter is 15 packets per second (pps). If this limit is reached, the switch disables the port to prevent the attack. In this case, to launch a MIM attack, an attacker must first discover who else is Layer 2 adjacent. To do this, ettercap generates a series of GARPs, claiming to be each one of the IP address on the subnet. In this way, the real owner of that address replies and ettercap can build its table.

In lab tests, this limit has been reached immediately when using ettercap and the port shuts down. This is acceptable in a wired scenario, but in a wireless scenario, by shutting down the port connected to the AP, all the wireless users lose their connection to the outside world and a possible MIM attack turns into a DoS attack.

To avoid this potential DoS (involuntarily created by enabling DAI), Cisco recommends turning off the ARP rate limiter on the port of the switch connected to the AP. You can do this with the following interface level command:

```
ip arp inspection limit none
```

An alternative is to change the threshold value to a value larger than 15 pps. However, this is not a general remedy because it depends on the implementation of the specific tool being used to launch the attack.

Using IP Source Guard to Mitigate IP and MAC Spoofing

When enabled on an interface of the access switch, IP Source Guard dynamically creates a per-port access control list (PACL) based on the contents of the DHCP snooping binding table. This PACL enforces traffic to be sourced from the IP address issued at DHCP binding time and prevents any traffic from being forwarded by other spoofed addresses. This also prevents an attacker from impersonating a valid address by either manually changing the address or running a program designed to do address spoofing, such as hping2. This feature has an option (port security) to filter the incoming address, also using the MAC address in the DHCP snooping binding table.

The attacker typically uses the spoofed address to hide his or her real identity and launch an attack, such as a DoS attack, against a target.

IP Source Guard for Wireless Access

In the case of wireless access, IP Source Guard can be enabled on the trunk port connecting the access switch to the H-REAP. This allows the switch to filter any traffic coming from wireless users that does not match an entry in the DHCP binding table.

IP Source Guard does not need to be enabled on the VLANs configured behind a WLC, because the WLC performs a similar function to ensure that the IP address used by a client is the IP address that has been assigned to that client.

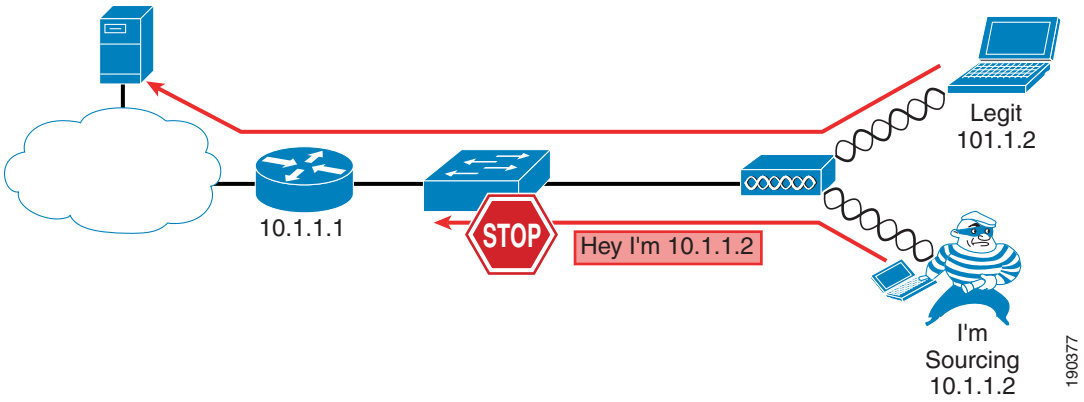
IP Source Guard is beneficial in H-REAP deployments because the H-REAP (unlike a standard LAP) is not able to check the WLAN client MAC-to-IP address binding relationship.

In tests, the following two scenarios were considered:

- Scenario 1—The target is represented by another wireless user associated to the same AP.
- Scenario 2—The target is another wireless user associated to a different AP.

Figure 4-35 shows an example of using IP Source Guard to mitigate IP and MAC spoofing attacks.

Figure 4-35 IP Source Guard Preventing MIM



Effectiveness of IP Source Guard

The effectiveness of this feature depends on two factors: the way the attacker is able to spoof the address, and which scenario is being tested.

An association to the AP is based on the client MAC address, so if the AP receives a frame with an unknown source MAC address, it drops the frame. When launching an IP spoofing attack, the attacker has the option to use his or her own MAC address or to use one from another user connected to the same AP. All the other combinations, such as using a random MAC address or using the MAC address of a user connected to another AP, lead to a failed attack because the AP drops the frame.

In case the attacker uses his or her own MAC address but spoofs the IP address, IP Source Guard enabled on the switch stops the attack in all the second scenario but not the first. In the first scenario, the traffic stays local to the AP and the CISF feature is not invoked. In the other scenarios, CISF successfully stops the attack because the IP-spoofed packet sent by the malicious user has no entry in the DHCP snooping table.

However, if the attacker is able to spoof both the MAC and the IP address of another wireless user connected to the same AP, basically assuming the identity of another user, the attack is successful in Scenarios 1 and 2.

Spoofing both the Mac and IP address is realistically possible in a hotspot environment where no encryption is used, or when the weaknesses of WEP are exploited. This is one of the reasons why Cisco highly recommends the use of strong encryption whenever possible.

Summary of Findings

The results of the tests are presented in Table 4-4.

Table 4-4 Summary of Findings

Targeted Attack	Applicability	Considerations	Solution
MAC flooding	No	Macof uses random MAC addresses as source and destination	AP discards frames from a source MAC not in the association table
DHCP starvation	Yes on H-REAP Controller discards bad DHCP requests	The requesting MAC is carried in the DHCP payload	None–rate limiting
Rogue DHCP server	Yes on H-REAP Controller blocks DHCP offers from the WLAN	It is assumed the rogue DHCP server is wireless	None
MIM between wireless clients	Yes on H-REAP Controller blocks GARPs	Traffic does not go through the switch in this case	None
MIM between wireless clients on different APs	Yes on H-REAP Controller blocks GARPs	The hacker can intercept traffic only toward the wire.	DAI with violation
MIM between wireless and wired clients	Yes on H-REAP Not a supported controller configuration	The hacker can intercept traffic only toward the wire.	DAI with violation
IP spoofing	Yes on H-REAP Controller checks IP address and MAC address binding	Encryption over the air is required to prevent identity spoofing	IP Source Guard

Note that Cisco tested only those attacks that are targeted by the CISF features on wired access, and it was always assumed that the attacker was wireless, while the target could be either wired or wireless depending on the scenario considered. Finally, the solution reported in Table 4-4 represents what is currently available using the CISF features on the access switch; when those features do not help, Cisco proposes an alternative solution using features available directly on the access point.

References

- Deploying Cisco 440X Series Wireless LAN Controllers—
http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html
- Cisco Wireless LAN Controller Configuration Guide, Release 4.1—
http://www.cisco.com/en/US/docs/wireless/controller/4.1/configuration/guide/ccfig41.html
- Cisco Wireless Control System Configuration Guide, Release 4.1—
http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcscfg41.html

CHAPTER 5

Cisco Unified Wireless QoS

This chapter describes quality-of-service (QoS) in the context of WLAN implementations. This chapter describes WLAN QoS in general, but does not provide in-depth coverage on topics such as security, segmentation, and voice over WLAN (VoWLAN), although these topics have a QoS component. This chapter also provides information on the features of the Cisco Centralized WLAN Architecture.

This chapter is intended for those who are tasked with designing and implementing enterprise WLAN deployments using the Cisco Unified Wireless technology.

QoS Overview

QoS refers to the capability of a network to provide differentiated service to selected network traffic over various network technologies. QoS technologies provide the following benefits:

- Provide building blocks for business multimedia and voice applications used in campus, WAN, and service provider networks
- Allow network managers to establish service-level agreements (SLAs) with network users
- Enable network resources to be shared more efficiently and expedite the handling of mission-critical applications
- Manage time-sensitive multimedia and voice application traffic to ensure that this traffic receives higher priority, greater bandwidth, and less delay than best-effort data traffic

With QoS, bandwidth can be managed more efficiently across LANs, including WLANs and WANs. QoS provides enhanced and reliable network service by doing the following:

- Supporting dedicated bandwidth for critical users and applications
- Controlling jitter and latency (required by real-time traffic)
- Managing and minimizing network congestion
- Shaping network traffic to smooth the traffic flow
- Setting network traffic priorities

Wireless QoS Deployment Schemes

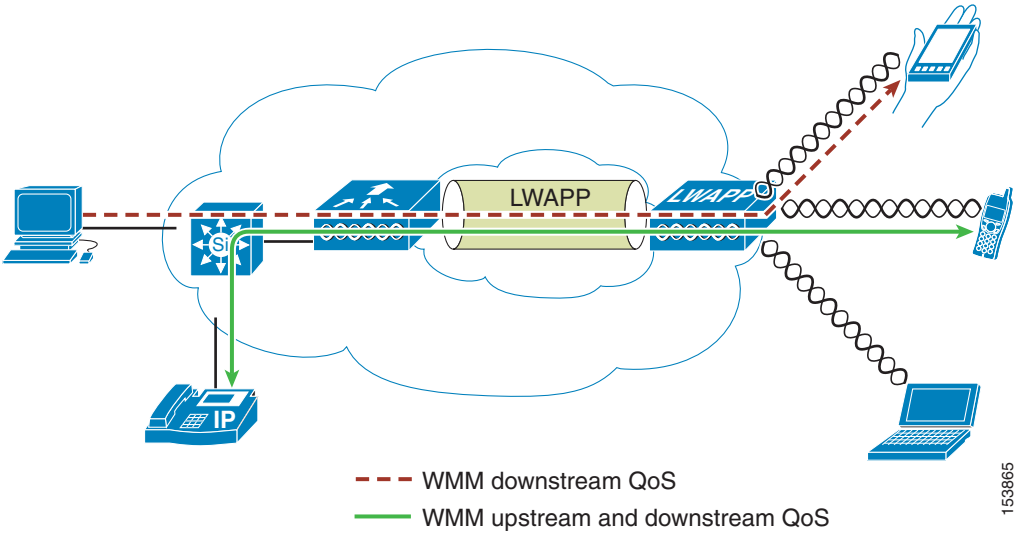
In the past, WLANs were mainly used to transport low-bandwidth, data-application traffic. Currently, with the expansion of WLANs into vertical (such as retail, finance, and education) and enterprise environments, WLANs are used to transport high-bandwidth data applications, in conjunction with time-sensitive multimedia applications. This requirement led to the necessity for wireless QoS.

Several vendors, including Cisco, support proprietary wireless QoS schemes for voice applications. To speed up the rate of QoS adoption and to support multi-vendor time-sensitive applications, a unified approach to wireless QoS is necessary. The IEEE 802.11e working group within the IEEE 802.11 standards committee has completed the standard definition, but adoption of the 802.11e standard is in its early stages, and as with many standards there are many optional components. Just as occurred with 802.11 security in 802.11i, industry groups such as the Wi-Fi Alliance and industry leaders such as Cisco are defining the key requirements in WLAN QoS through their WMM and Cisco Compatible Extensions programs, ensuring the delivery of key features and interoperation through their certification programs.

Cisco Unified Wireless products support Wi-Fi MultiMedia (WMM), a QoS system based on IEEE 802.11e that has been published by the Wi-Fi Alliance, and WMM Power Save, as well as Admission Control.

Figure 5-1 shows a sample deployment of wireless QoS based on Cisco Unified Wireless technology features.

Figure 5-1 QoS Deployment Example



QoS Parameters

QoS is defined as the measure of performance for a transmission system that reflects its transmission quality and service availability. Service availability is a crucial element of QoS. Before QoS can be successfully implemented, the network infrastructure must be highly available. The network transmission quality is determined by latency, jitter, and loss, as shown in Table 5-1.

Table 5-1 QoS Parameters

Transmission Quality	Description
Latency	Latency (or delay) is the amount of time it takes for a packet to reach the receiving endpoint after being transmitted from the sending endpoint. This time period is called the end-to-end delay and can be divided into two areas: • Fixed network delay—Includes encoding and decoding time (for voice and video), and the finite amount of time required for the electrical or optical pulses to traverse the media en route to their destination. • Variable network delay—Generally refers to network conditions, such as queuing and congestion, that can affect the overall time required for transit.
Jitter	Jitter (or delay-variance) is the difference in the end-to-end latency between packets. For example, if one packet requires 100 ms to traverse the network from the source endpoint to the destination endpoint, and the next packet requires 125 ms to make the same trip, the jitter is calculated as 25 ms.
Loss	Loss (or packet loss) is a comparative measure of packets successfully transmitted and received to the total number that were transmitted. Loss is expressed as the percentage of packets that were dropped.

Upstream and Downstream QoS

Figure 5-2 illustrates the definition of *radio upstream* and *radio downstream* QoS.

Figure 5-2 Upstream and Downstream QoS

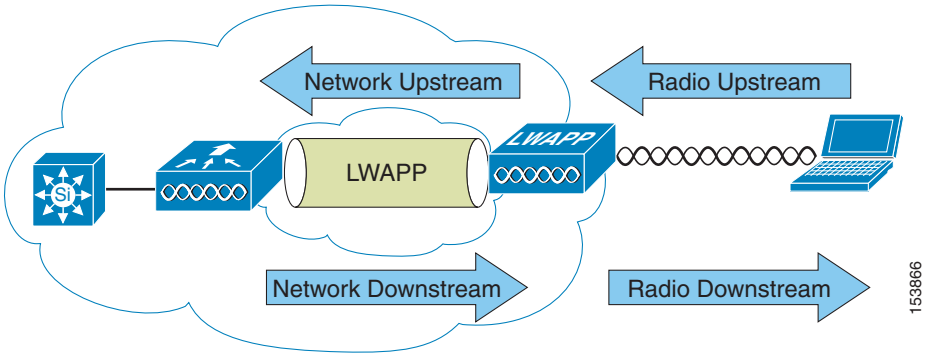


Figure 5-2 shows the following:

- *Radio downstream* QoS—Traffic leaving the AP and traveling to the WLAN clients. Radio downstream QoS is the primary focus of this chapter, because this is still the most common deployment. The radio client upstream QoS depends on the client implementation.
- *Radio upstream* QoS—Traffic leaving the WLAN clients and traveling to the AP. WMM provides upstream QoS for WLAN clients supporting WMM.

- *Network downstream*—Traffic leaving the WLC traveling to the AP. QoS can be applied at this point to prioritize and rate-limit traffic to the AP. Configuration of Ethernet downstream QoS is not covered in this chapter.
- *Network upstream*—Traffic leaving the AP, traveling to the WLC. The AP classifies traffic from the AP to the upstream network according to the traffic classification rules of the AP.

QoS and Network Performance

The application of QoS features might not be easily detected on a lightly loaded network. If latency, jitter, and loss are noticeable when the media is lightly loaded, it indicates either a system fault, poor network design, or that the latency, jitter, and loss requirements of the application are not a good match for the network. QoS features start to be applied to application performance as the load on the network increases. QoS works to keep latency, jitter, and loss for selected traffic types within acceptable boundaries. When providing only radio downstream QoS from the AP, radio upstream client traffic is treated as best-effort. A client must compete with other clients for upstream transmission as well as competing with best-effort transmission from the AP. Under certain load conditions, a client can experience upstream congestion, and the performance of QoS-sensitive applications might be unacceptable despite the QoS features on the AP. Ideally, upstream and downstream QoS can be operated either by using WMM on both the AP and WLAN client, or by using WMM and a client proprietary implementation.

Note Even without WMM support on the WLAN client, the Cisco Unified Wireless solution is able to provide network prioritization in both network upstream and network downstream situations.

Note WLAN client support for WMM does not mean that the client traffic automatically benefits from WMM. The applications looking for the benefits of WMM assign an appropriate priority classification to their traffic, and the operating system needs to pass that classification to the WLAN interface. In purpose-built devices, such as VoWLAN handsets, this is done as part of the design. However, if implementing on a general purpose platform such as a PC, application traffic classification and OS support must be implemented before the WMM features can be used to good effect.

802.11 DCF

Data frames in 802.11 are sent using the Distributed Coordination Function (DCF), which is composed of the following two main components:

- Interframe spaces (SIFS, PIFS, and DIFS).
- Random backoff (contention window) DCF is used in 802.11 networks to manage access to the RF medium.

A baseline understanding of DCF is necessary to deploy 802.11e-based enhanced distributed channel access (EDCA). For more information on DCF, see the IEEE 802.11 specification at the following URL: http://ieeexplore.ieee.org/xpl/standardstoc.jsp?isnumber=14251&isYear=1997.

Interframe Spaces

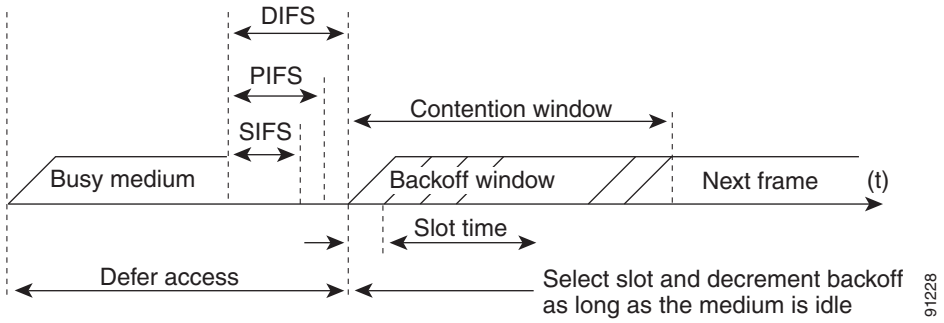
802.11 currently defines three interframe spaces (IFS), as shown in Figure 5-3:

- Short interframe space (SIFS)—10 µs
- PCF interframe space (PIFS)—SIFS + 1 x slot time = 30 µs
- DCF interframe space (DIFS)—50 µs SIFS + 2 x slot time = 50 µs

Note The base timing used in this interframe space example are for 802.11b; the timing in 802.11g and 802.11a are different, but the principles applied are the same.

The interframe spaces (SIFS, PIFS, and DIFS) allow 802.11 to control which traffic gets first access to the channel after carrier sense declares the channel to be free. Generally, 802.11 management frames and frames not expecting contention (a frame that is part of a sequence of frames) use SIFS, and data frames use DIFS.

Figure 5-3 Interframe Spaces



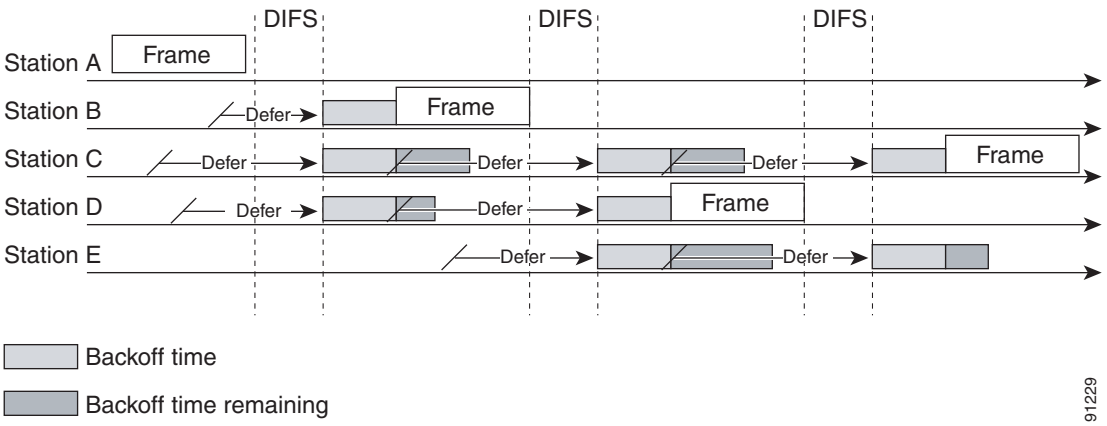
Random Backoff

When a data frame using DCF is ready to be sent, it goes through the following steps:

1. Generates a random backoff number between 0 and a minimum contention window (CWmin).
2. Waits until the channel is free for a DIFS interval.
3. If the channel is still free, begins to decrement the random backoff number, for every slot time (20 µs) that the channel remains free.
4. If the channel becomes busy, such as another station getting to 0 before your station, the decrement stops and steps 2 through 4 are repeated.
5. If the channel remains free until the random backoff number reaches 0, the frame can be sent.

Figure 5-4 shows a simplified example of how the DCF process works. In this simplified DCF process, no acknowledgements are shown and no fragmentation occurs.

Figure 5-4 Distributed Coordination Function Example



The DCF steps illustrated in Figure 5-4 are as follows:

1. Station A successfully sends a frame; three other stations also want to send frames but must defer to Station A traffic.
2. After Station A completes the transmission, all the stations must still defer to the DIFS. When the DIFS is complete, stations waiting to send a frame can begin to decrement the backoff counter, once every slot time, and can send their frame.
3. The backoff counter of Station B reaches zero before Stations C and D, and therefore Station B begins transmitting its frame.
4. When Station C and D detect that Station B is transmitting, they must stop decrementing the backoff counters and defer until the frame is transmitted and a DIFS has passed.
5. During the time that Station B is transmitting a frame, Station E receives a frame to transmit, but because Station B is sending a frame, it must defer in the same manner as Stations C and D.
6. When Station B completes transmission and the DIFS has passed, stations with frames to send begin to decrement the backoff counters. In this case, the Station D backoff counter reaches zero first and it begins transmission of its frame.
7. The process continues as traffic arrives on different stations.

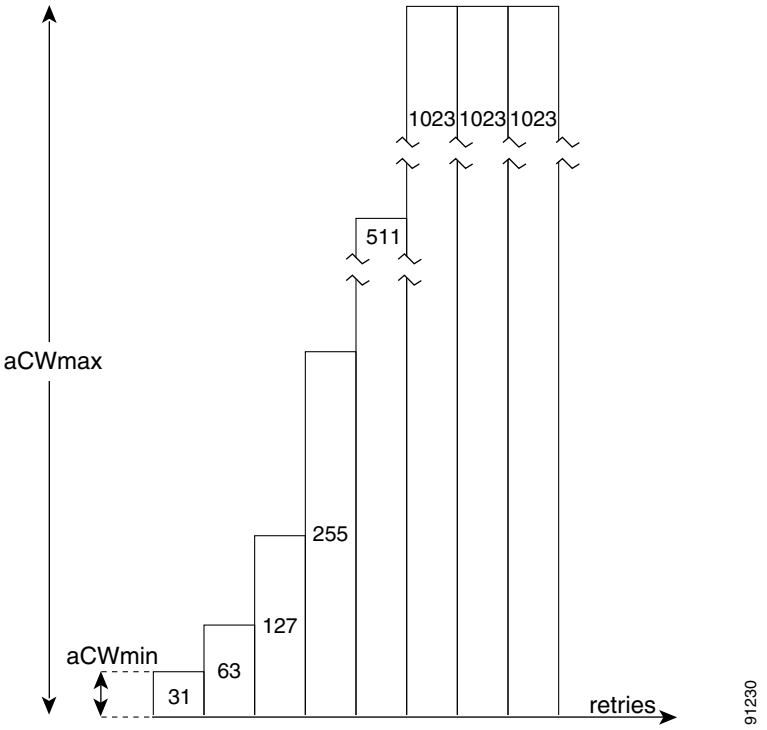
CWmin, CWmax, and Retries

DCF uses a contention window (CW) to control the size of the random backoff. The contention window is defined by two parameters:

- aCWmin
- aCWmax

The random number used in the random backoff is initially a number between 0 and aCWmin. If the initial random backoff expires without successfully sending the frame, the station or AP increments the retry counter, and doubles the value random backoff window size. This doubling in size continues until the size equals aCWmax. The retries continue until the maximum retries or time-to-live (TTL) is reached. This process of doubling the backoff window is often referred to as a *binary exponential backoff*, and is illustrated in Figure 5-5 where the aCWmin if 2^5-1, and increases to 2^6-1, on the next backoff level, up to the aCWmax value of 2^{10}-1.

Figure 5-5 Growth in Random Backoff Range with Retries



Note These values are for 802.11b, and values can be different for different physical layer implementations.

Wi-Fi Multimedia

This section describes three WMM implementations:

- WMM access
- WMM power save
- Access control

WMM Access

WMM is a Wi-Fi Alliance certification of support for a set of features from an 802.11e draft. This certification is for both clients and APs, and certifies the operation of WMM. WMM is primarily the implementation of the EDCA component of 802.11e. Additional Wi-Fi certifications are planned to address other components of the 802.11e.

WMM Classification

WMM uses the 802.1P classification scheme developed by the IEEE (which is now a part of the 802.1D specification).

This classification scheme has eight priorities, which WMM maps to four access categories: AC_BK, AC_BE, AC_VI, and AC_VO. These access categories map to the four queues required by a WMM device, as shown in Table 5-2.

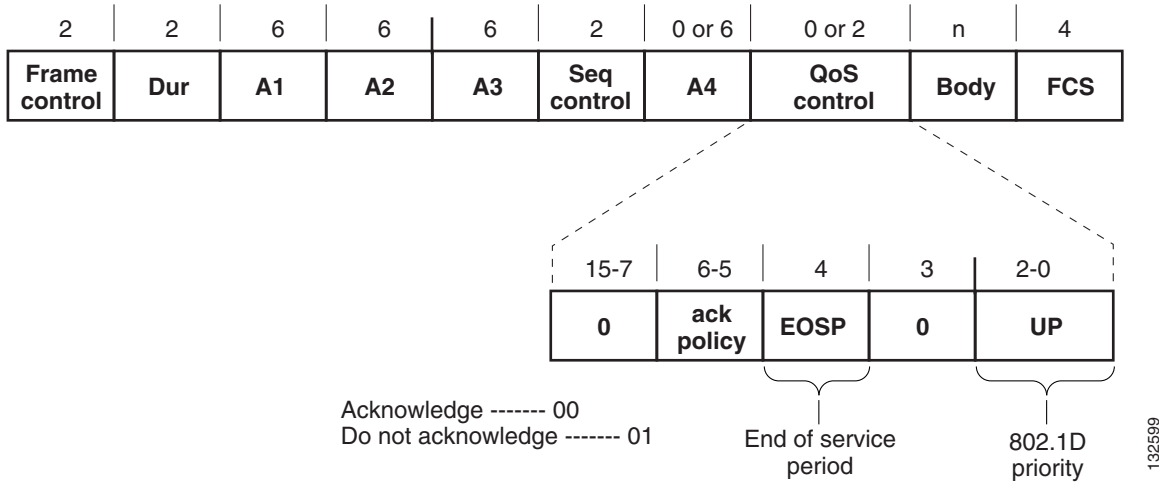
Table 5-2 Table 2 802.1P and WMM Classification

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

Figure 5-6 shows the WMM data frame format. Note that even though WMM maps the eight 802.1P classifications to four access categories, the 802.11D classification is sent in the frame.

Note The WMM and IEEE 802.11e classifications are different from the classifications recommended and used in the Cisco network, which are based on IETF recommendations. The primary difference in classification is the changing of voice and video traffic to 5 and 4, respectively. This allows the 6 classification to be used for Layer 3 network control. To be compliant with both standards, the Cisco Unified Wireless solution performs a conversion between the various classification standards when the traffic crosses the wireless-wired boundary.

Figure 5-6 WMM Frame Format



WMM Queues

Figure 5-7 shows the queuing performed on a WMM client or AP. There are four separate queues, one for each of the access categories. Each of these queues contends for the wireless channel in a similar manner to the DCF mechanism described previously, with each of the queues using different interframe space, CWmin, and CWmax values. If more than one frame from different access categories collide internally, the frame with the higher priority is sent, and the lower priority frame adjusts its backoff parameters as though it had collided with a frame external to the queuing mechanism. This system is called enhanced distributed channel access (EDCA).

Figure 5-7 WMM Queues

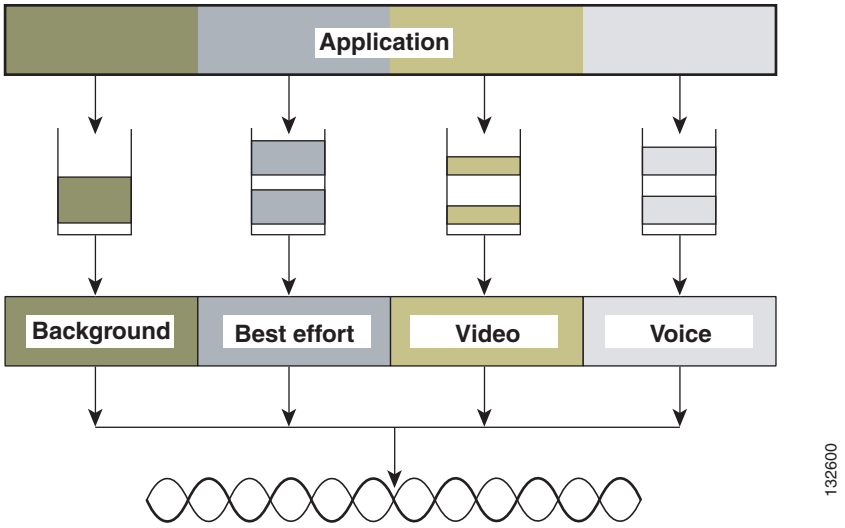
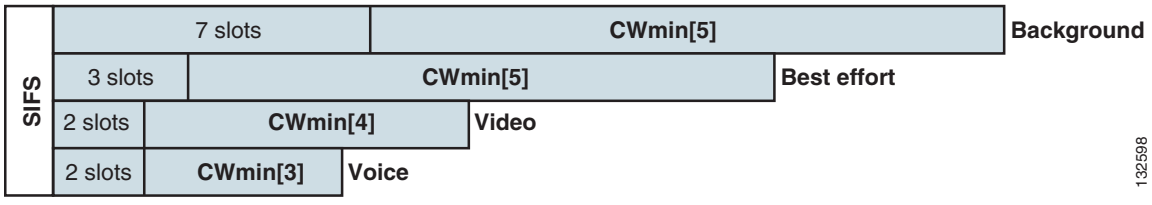


Figure 5-8 shows the principle behind EDCF, where different interframe spacing and CWmin and CwMax values (for clarity CwMax is not shown) are applied per traffic classification. Different traffic types can wait different interface spaces before counting down their random backoff, and the CW value used to generate the random backoff number also depends on the traffic classification. For example, the CWmin[3] for Voice is 2^3-1, and CWmin[5] for Best effort traffic is 2^5-1. High priority traffic has a small interframe space and a small CWmin value, giving a short random backoff, whereas best-effort traffic has a longer interframe space and large CWmin value that on average gives a large random backoff number.

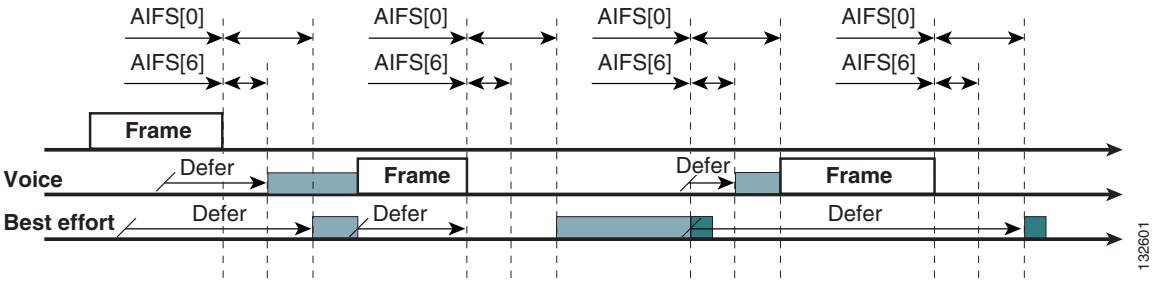
Figure 5-8 Access Category Timing



EDCA

The EDCA process is illustrated in Figure 5-9.

Figure 5-9 EDCA Example



The EDCA process follows this sequence:

1. While Station X is transmitting its frame, three other stations determine that they must send a frame. Each station defers because a frame was already being transmitted, and each station generates a random backoff.
2. Because the Voice station has a traffic classification of voice, it has an arbitrated interframe space (AIFS) of 2, and uses an initial CWmin of 3, and therefore must defer the countdown of its random backoff for 2 slot times, and has a short random backoff value.
3. Best-effort has an AIFS of 3 and a longer random backoff time, because its CWmin value is 5.
4. Voice has the shortest random backoff time, and therefore starts transmitting first. When Voice starts transmitting, all other stations defer.
5. After the Voice station finishes transmitting, all stations wait their AIFS, then begin to decrement the random backoff counters again.
6. Best-effort then completes decrementing its random backoff counter and begins transmission. All other stations defer. This can happen even though there might be a voice station waiting to transmit. This shows that best-effort traffic is not starved by voice traffic because the random backoff decrementing process eventually brings the best-effort backoff down to similar sizes as high priority traffic, and that the random process might, on occasion, generate a small random backoff number for best-effort traffic.
7. The process continues as other traffic enters the system. The access category settings shown in Table 5-3 and Table 5-4 are, by default, the same for an 802.11a radio, and are based on formulas defined in WMM.

Note Table 5-3 refers to the parameter settings on a client, which are slightly different from the settings for an AP. The AP has a larger AIFSN for voice and video ACs.

Table 5-3 WMM Client Parameters

AC	CWmin	CWmax	AIFSN	TXOP Limit (802.11b	TXOP Limit (802.11a/g)
AC_BK	aCWmin	aCWmax	7	0	0
AC_BE	aCWmin	4*(aCQmin+1)-1	3	0	0

Table 5-3 WMM Client Parameters

AC	CWmin	CWmax	AIFSN	TXOP Limit (802.11b	TXOP Limit (802.11a/g)
AC_VI	(aCWmin+1)/2-1	aCWmin	1	6.016 ms	3.008 ms
AC_VO	(aCWmin+1)/4-1	(aCWmin+1)/2-1	1	3.264 ms	1.504 ms

Table 5-4 WMM AP Parameters

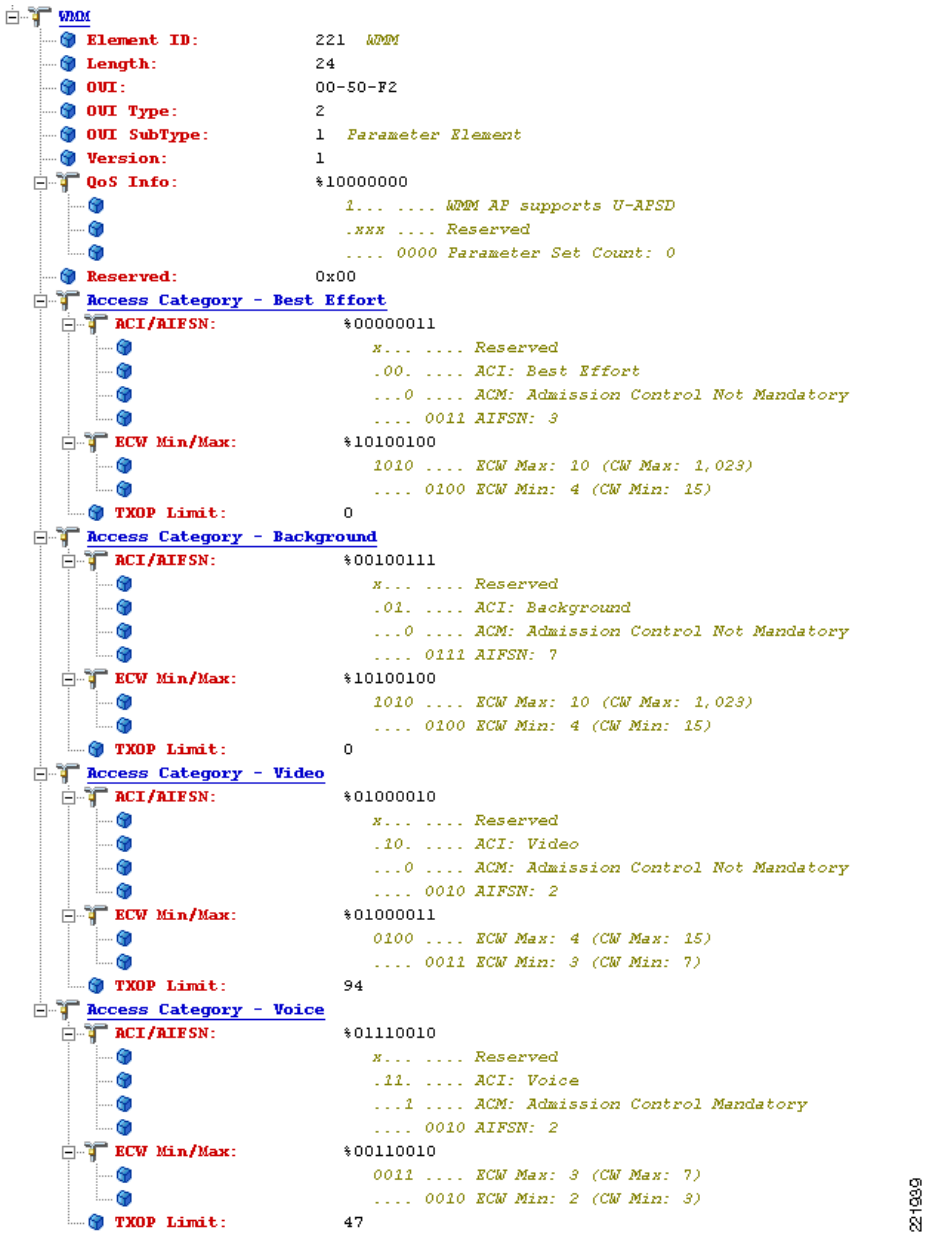
Access Category	CWmin	CWmax	AIFSN	TXOP Limit (802.11b	TXOP Limit (802.11a/g)
AC_BK	aCWmin	aCWmax	7	0	0
AC_BE	aCWmin	4*(aCQmin+1)-1	3	0	0
AC_VI	(aCWmin+1)/2-1	aCWmin	2	6.016 ms	3.008 ms
AC_VO	(aCWmin+1)/4-1	(aCWmin+1)/2-1	2	3.264 ms	1.504 ms

The overall impact of the different AIFS, CWmin, and CWmax values is difficult to illustrate in timing diagrams because their impact is more statistical in nature. It is easier to compare the AIFS and the size of the random backoff windows, as shown in Figure 5-8.

When comparing voice and background frames as examples, these traffic categories have CWmin values of 2^3-1 (7) and 2^5-1 (31), and AIFS of 2 and 7, respectively. This an average delay of 5 (2+7/1) slot times before sending a voice frame, and an average of 22 slot (7+31/2) times for background frame. Therefore, voice frames are statistically much more likely to be sent before background frames.

Figure 5-10 shows the WMM information in a probe response. Apart from the WMM access category information contained in this element, the client also learns which WMM categories require admission control. As can be seen in this example, the Voice AC has admission control set to mandatory. This requires the client to send the request to the AP, and have the request accepted, before it can use this AC. Admission control is discussed in more detail later in this chapter.

Figure 5-10 Probe Response WMM Element Information



U-APSD

Unscheduled automatic power-save delivery (U-APSD) is a feature that has two key benefits:

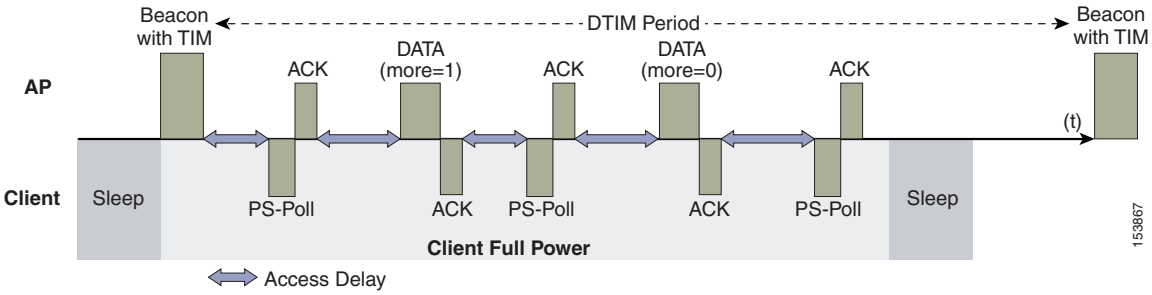
- The primary benefit of U-APSD is that it allows the voice client to synchronize the transmission and reception of voice frames with the AP, thereby allowing the client to go into power-save mode between the transmission/reception of each voice frame tuple. The WLAN client frame transmission in the access categories supporting U-APSD triggers the AP to send any data frames queued for that WLAN client in that access category. A U-APSD client remains listening to the AP until it receives a frame from the AP with an end-of-service period (EOSP) bit set. This tells the client that it can now go back into its power-save mode. This triggering mechanism is considered a more efficient

use of client power than the regular listening for beacons method, at a period controlled by the delivery traffic indication message (DTIM) interval, because the latency and jitter requirements of voice are such that a WVoIP client would either not be in power-save mode during a call, resulting in reduced talk times, or would use a short DTIM interval, resulting in reduced standby times. The use of U-APSD allows the use of long DTIM intervals to maximize standby time without sacrificing call quality. The U-APSD feature can be applied individually across access categories, allowing U-APSD can be applied to the voice ACs in the AP, but the other ACs still use the standard power save feature.

- The secondary benefit of this feature is increased call capacity. The coupling of transmission buffered data frames from the AP with the triggering data frame from the WLAN client allows the frames from the AP to be sent without the accompanying interframe spacing and random backoff, thereby reducing the contention experience by call.

Figure 5-11 shows a sample frame exchange for the standard 802.11 power save delivery process.

Figure 5-11 Standard Client Power-Save

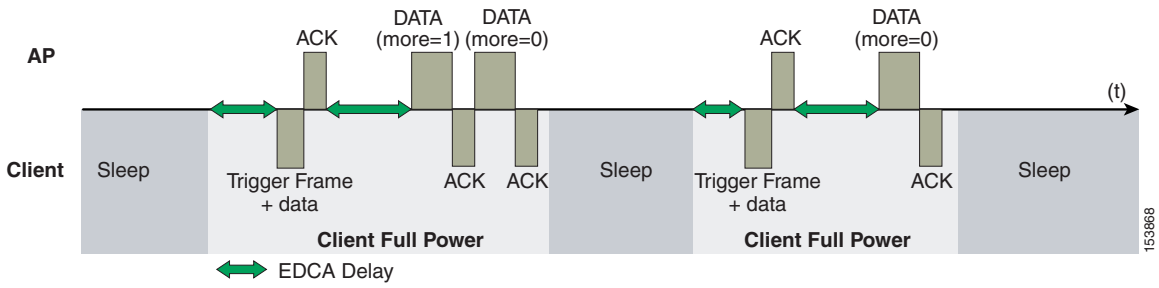


The client in power-save mode first detects that there is data waiting for it at the AP via the presence of the TIM in the AP beacon. The client must power-save poll (PS-Poll) the AP to retrieve that data. If the data sent to the client requires more than one frame to be sent, the AP indicates this in the sent data frame. This process requires the client to continue sending power-save polls to the AP until all the buffered data is retrieved by the client.

This presents two major problems. The first is that it is quite inefficient, requiring the PS-polls, as well as the normal data exchange, to go through the standard access delays associated with DCF. The second issue, being more critical to voice traffic, is that retrieving the buffered data is dependent on the DTIM, which is a multiple of the beacon interval. Standard beacon intervals are 100 ms, and the DTIM interval can be integer multiples of this. This introduces a level of jitter that is generally unacceptable for voice calls, and voice handsets switch from power-save mode to full transmit and receive operation when a voice call is in progress. This gives acceptable voice quality but reduces battery life. The Cisco Unified Wireless IP Phone 7921G addresses this issue by providing a PS-Poll feature that allows the 7921G to generate PS-Poll requests without waiting for a beacon TIM. This allows the 7921G to poll for frames when it has sent a frame, and then go back to power-save mode. This feature does not provide the same efficiency as U-APSD, but improves battery life for 7921Gs on WLANs without U-APSD.

Figure 5-12 shows an example of traffic flows with U-APSD. In this case, the trigger for retrieving traffic is the client sending traffic to the AP. The AP, when acknowledging the frame, tells the client that data is queued for it, and that it should stay on. The AP then sends data to the client typically as a TXOP burst where only the first frame has the EDCF access delay. All subsequent frames are then sent directly after the acknowledgment frame. In a VoWLAN implementation there is only likely to be one frame queued at the AP, and VoWLAN client would be able to go into sleep mode after receiving that frame from the AP.

Figure 5-12 U-APSD



This approach overcomes both the disadvantages of the previous scheme in that it is much more efficient. The timing of the polling is controlled via the client traffic, which in the case of voice is symmetric, so if the client is sending a frame every 20 ms, it would be expecting to receive a frame every 20 ms as well. This would introduce a maximum jitter of 20 ms, rather than an n * 100 ms jitter.

TSpec Admission Control

Traffic Specification (TSpec) allows an 802.11e client to signal its traffic requirements to the AP. In the 802.11e MAC definition, two mechanisms provide prioritized access. These are the contention-based EDCA option and the controlled access option provided by the transmit opportunity (TXOP). When describing TSpec features where a client can specify its traffic characteristics, it is easy to assume that this would automatically result in the use of the controlled access mechanism, and have the client granted a specific TXOP to match the TSpec request. However, this does not have to be the case; a TSpec request can be used to control the use of the various access categories (ACs) in EDCA. Before a client can send traffic of a certain priority type, it must have requested to do so via the TSpec mechanism. For example, a WLAN client device wanting to use the voice AC must first make a request for use of that AC. Whether or not AC use is controlled by TSpec requests is configurable with voice and video ACs controlled by TSpec requests, and best-effort and background ACs can be open for use without a TSpec request. The use of EDCA ACs, rather than the 802.11e Hybrid Coordinated Channel Access (HCCA), to meet TSpec requests is possible in many cases because the traffic parameters are sufficiently simple to allow them to be met by allocating capacity, rather than creating a specific TXOP to meet the application requirements.

Note Unlike the 7921G, which does have support for TSpec, the Cisco 7920 WVoIP handset does not support TSpec admission control.

Add Traffic Stream

The Add Traffic Stream (ADDTS) function is how a WLAN client performs an admission request to an AP. Signalling its TSpec request to the AP, an admission request is in one of two forms:

- ADDTS action frame—This happens when a phone call is originated or terminated by a client associated to the AP. The ADDTS contains TSpec and might contain a traffic stream rate set (TSRS) IE (Cisco Compatible Extensions v4 clients).
- Association and re-association message—The association message might contain one or more TSpecs and one TSRS IE if the STA wants to establish the traffic stream as part of the association. The re-association message might contain one or more TSpecs and one TSRS IE if an STA roams to another AP.

The ADDTS contains the TSpec element that describes the traffic request. See Figure 5-13 and Figure 5-14 for examples of an ADDTS request and response between a Cisco 7921 WLAN handset and a Cisco AP. Apart from key data describing the traffic requirements, such as data rates and frame sizes, the TSpec element also tells the AP the minimum physical rate that the client device will use. This allows the calculation of how much time that station can potentially consume in sending and receiving in this TSpec, and therefore allowing the AP to calculate whether it has the resources to meet the TSpec. TSpec admission control is used by the WLAN client (target clients are VoIP handsets) when a call is initiated and during a roam request. During a roam, the TSpec request is appended to the re-association request.

Figure 5-13 ADDTS Request Decode

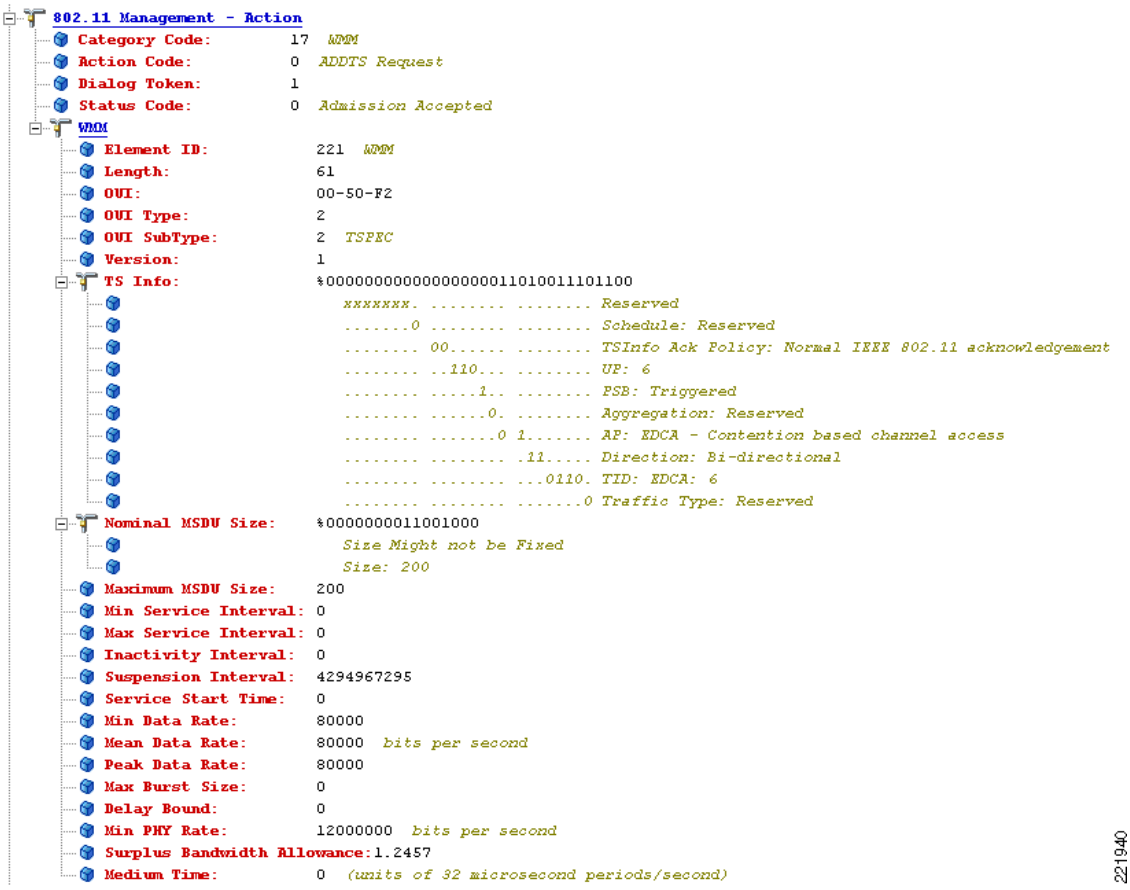
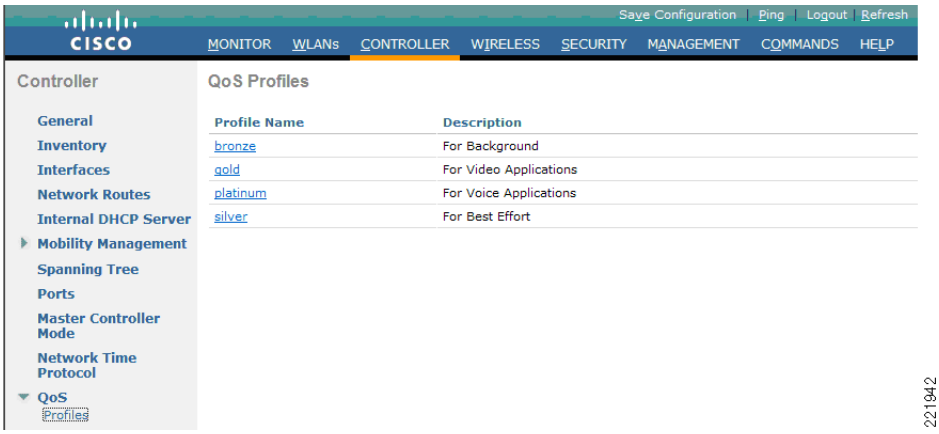


Figure 5-14 ADDTS Response Decode

QoS Advanced Features for WLAN Infrastructure

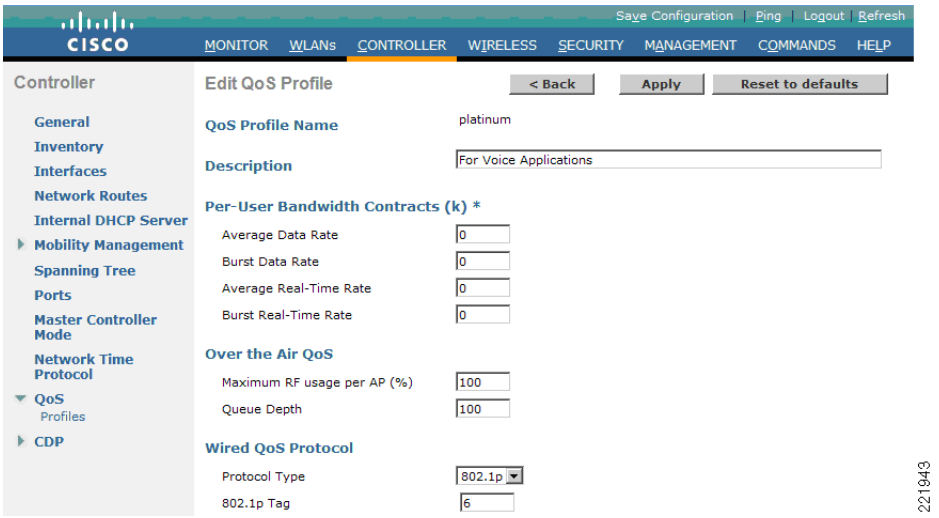
The Cisco Centralized WLAN Architecture has multiple QoS features, in addition to WMM support. Primary among these are the QoS profiles in the WLC. Four QoS profiles can be configured: platinum, gold, silver, and bronze, as shown in Figure 5-15.

Figure 5-15 QoS Profile Options



Each of the profiles shown in Figure 5-16 allows the configuration of bandwidth contracts, RF usage control, and the maximum 802.1P classification allowed.

Figure 5-16 QoS Profile Settings



It is generally recommended that the Per-User Bandwidth Contracts settings be left at their default values, and that the 802.11 WMM features be used to provide differentiated services.

For WLANs using a given profile, the 802.1P classification in that profile controls two important behaviors:

- Determines what class of service (CoS) value is used for packets initiated from the WLC.

  The CoS value set in the profile is used to mark the CoS of all LWAPP packets for WLAN using that profile. So a WLAN with a platinum QoS profile, and the 802.1P mark of 6, will have its LWAPP packets from the ap-manager interface of the controller marked with CoS of 5. The controller adjusts the CoS to be compliant with Cisco QoS baseline recommendations. The reason why it is important to maintain the IEEE CoS marking in the configuration is covered in the next point. If the network is set to trust CoS rather a DSCP at the network connection to the WLC, the CoS value determines the DSCP of the LWAPP packets received by the AP, and eventually the WMM classification and queuing for WLAN traffic, because the WLAN WMM classification of a frame is derived from the DSCP value of the LWAPP packet carrying that frame.

- Determines the maximum CoS value that can be used by clients connected to that WLAN.

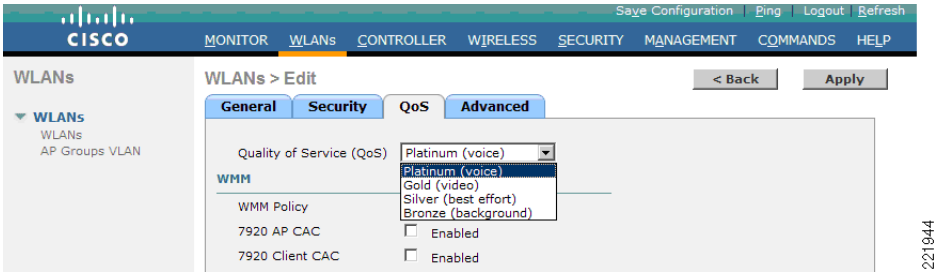
  The 802.1P classification sets the maximum CoS value that is admitted on a WLAN with that profile.

WMM voice traffic arrives with a CoS of 6 at the AP, and the AP automatically performs a CoS-to-DSCP mapping for this traffic based on a CoS of 6. If the CoS value in the WLC configuration is set to a value less than 6, this changed value is used by the WLAN QoS profile at the AP to set the maximum CoS marking used and therefore which WMM AC to use.

The key point is that with the Unified Wireless Network, you should always think in terms of IEEE 802.11e classifications, and allow the Unified Wireless Network Solution to take responsibility for converting between IEEE classification and the Cisco QoS baseline.

The WLAN can be configured with various default QoS profiles, as shown in Figure 5-17. Each of the profiles (platinum, gold, silver, and bronze) are annotated with their typical use. In addition, clients can be assigned a QoS profile based on their identity, through AAA. For a typical enterprise, WLAN deployment parameters, such as per-user bandwidth contracts and over-the-air QoS, should be left at their default values, and standard QoS tools, such as WMM and wired QoS, should be used to provide optimum QoS to clients.

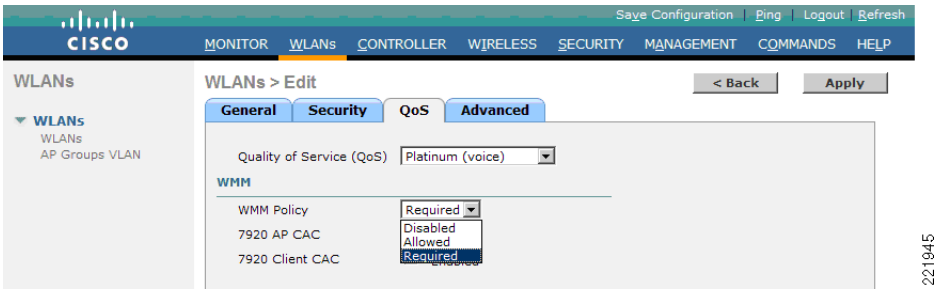
Figure 5-17 WLAN QoS Profile



In addition to the QoS profiles, the WMM policy per WLAN can also be controlled, as shown in Figure 5-18. The three WMM options are as follows:

- Disabled—The WLAN does not advertise WMM capabilities, or allow WMM negotiations,
- Allowed—The WLAN does allow WMM and non-WMM clients
- Required—Only WMM-enabled clients can be associated with this WLAN.

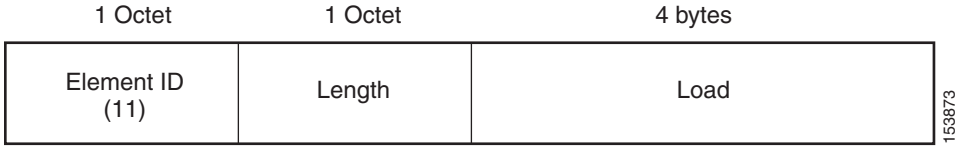
Figure 5-18 WLAN WMM Policy



IP Phones

Figure 5-19 shows the basic QoS Basis Service Set (QBSS) information element (IE) advertised by a Cisco AP. The Load field indicates the portion of available bandwidth currently used to transport data on that AP.

Figure 5-19 QBSS Information Element



There are actually three QBSS IEs that need to be supported in certain situations:

- Old QBSS (Draft 6 (pre-standard))
- New QBSS (Draft 13 802.11e (standard))
- New distributed CAC load IE (a Cisco IE)

The QBSS used depends on the WMM and 7920 settings on the WLAN.

7920 phone support, shown in Figure 5-18, is a component of the WLC WLAN configuration that enables the AP to include the appropriate QBSS element in its beacons. WLAN clients with QoS requirements, such as the 7920 and 7921G, use these advertised QoS parameters to determine the best AP with which to associate.

The WLC provides 7920 support through the client call admission control (CAC) limit, or AP CAC limit. These features provide the following:

- Client CAC limit—The 7920 uses a call admission control setting that is set on the client. This supports legacy 7920 code-pre 2.01.
- AP CAC limit—The 7920 uses CAC settings learned from WLAN advertisement.

The various combinations of WMM, client CAC limit, and AP CAC limit result in different QBSS IEs being sent:

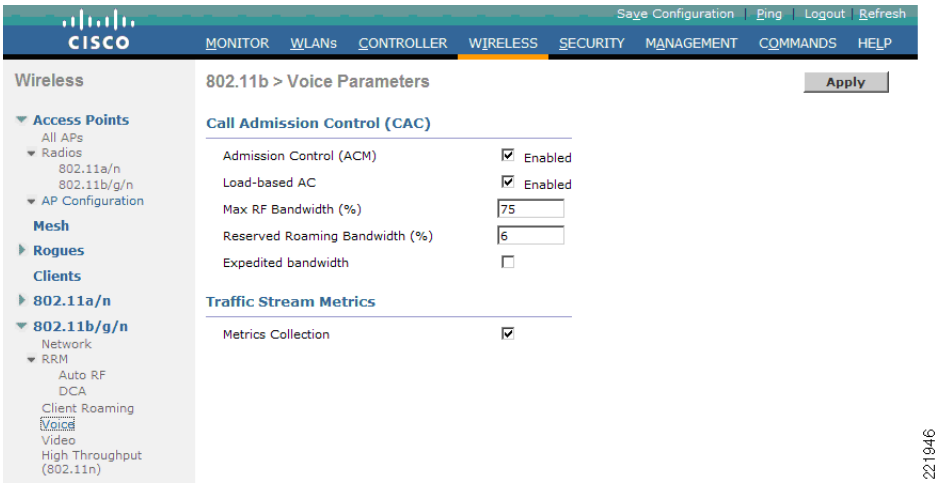
- If only WMM is enabled, IE number 2 (802.11e standard) QBSS Load IE is sent out in the beacons and probe responses.
- If 7920 client CAC limit is to be supported, IE number 1 (the pre-standard QBSS IE) is sent out in the beacons and probe responses on the bg radios.
- If 7920 AP CAC limit is to be supported, the number 3 QBSS IE is sent in the beacons and probe responses for bg radios.

Note The various QBSS IEs use the same ID, and therefore the three QBSSs are mutually exclusive. For example, the beacons and probe responses can contain only one QBSS IE.

Setting the Admission Control Parameters

Figure 5-20 shows a sample configuration screen for setting the voice parameters on the controller.

Figure 5-20 Voice Parameter Setting



The admission control parameters consist of the maximum RF Bandwidth that a radio can be using and still accept the initiation of a VoWLAN call through a normal ADDTS request.

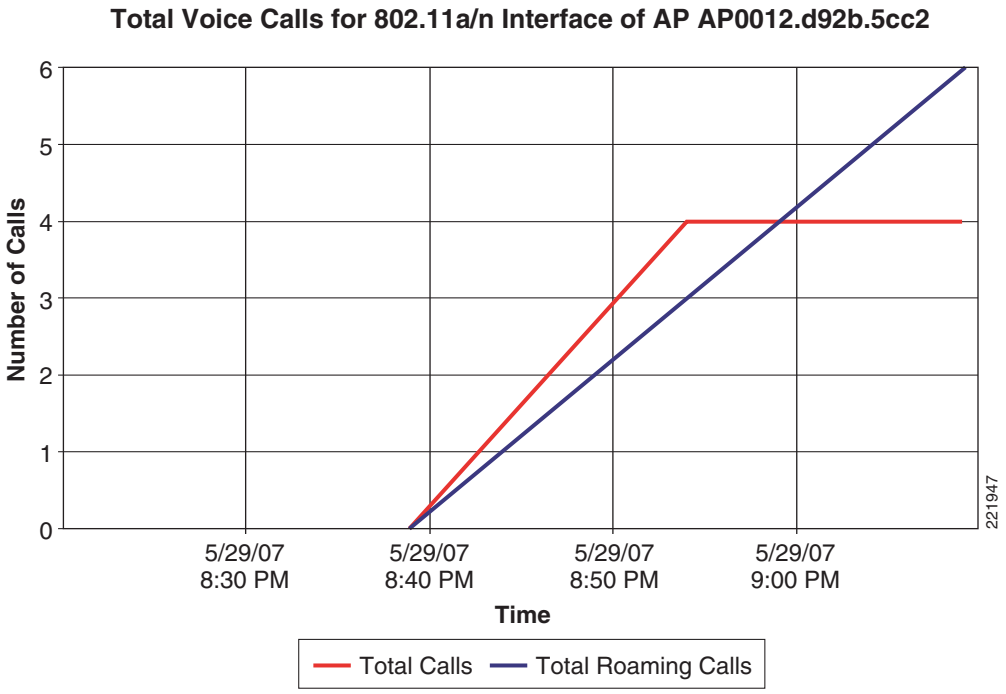
The reserved roaming bandwidth is how much capacity has been set aside to be able to respond to ADDTS requests during association or re-association, and which are VoWLAN clients with calls in progress that are trying to roam to that AP.

To enable admission control based upon these parameters to, use the Admission Control (ACM) checkbox. This enables admission control, based upon the APs capacity, but does not take into account the possible channel loading impact of other APs in the area. To include this “channel load” in capacity calculations, check the Load-Based AC checkbox as well as the Admission Control (ACM) checkbox.

The Metrics Collection option determines whether data is collected on voice or video calls for use by the WCS.

Figure 5-21 shows an example of one of the voice statistics reports available on the WCS, which shows the calls established on the radio of one AP, and the number of calls that roamed to that AP. This report and other voice statistics can be scheduled or ad-hoc, and either graphically displayed or posted as a data file.

Figure 5-21 Voice Statistics from WCS



Note Call admission control is performed only for voice and video QoS profiles.

Impact of TSpec Admission Control

The purpose of TSpec admission control is not to deny clients access to the WLAN; it is to protect the high priority resources. Therefore, a client that has not used TSpec admission control does not have its traffic blocked; it simply has its traffic re-classified if it tries to send (which it should not do if the client is transmitting WMM-compliant traffic in a protected AC).

Table 5-5 and Table 5-6 describe the impact on classification if access control is enabled and depending on whether a traffic stream has been established.

Table 5-5 Upstream Traffic

	Traffic Stream Established	No Traffic Stream
No admission control	No change in behavior; the packets go into the network as they do today-UP is limited to max= WLAN QoS setting.	No change in behavior; the packets go into the network as they do today-UP is limited to max= WLAN QoS setting.
Admission control	No change in behavior; the packets go into the network as they do today-UP is limited to max= WLAN QoS setting.	Packets are remarked to BE (both CoS and DSCP) before they enter the network for WMM clients. For non-WMM clients, packets are sent with WLAN QoS.

Table 5-6 Downstream Traffic

	Traffic Stream Established	No Traffic Stream
No admission control	No change	No change
Admission control	No change	Remark UP to BE for WMM client. For non-WMM clients, use WLAN QoS.

802.11e, 802.1P, and DSCP Mapping

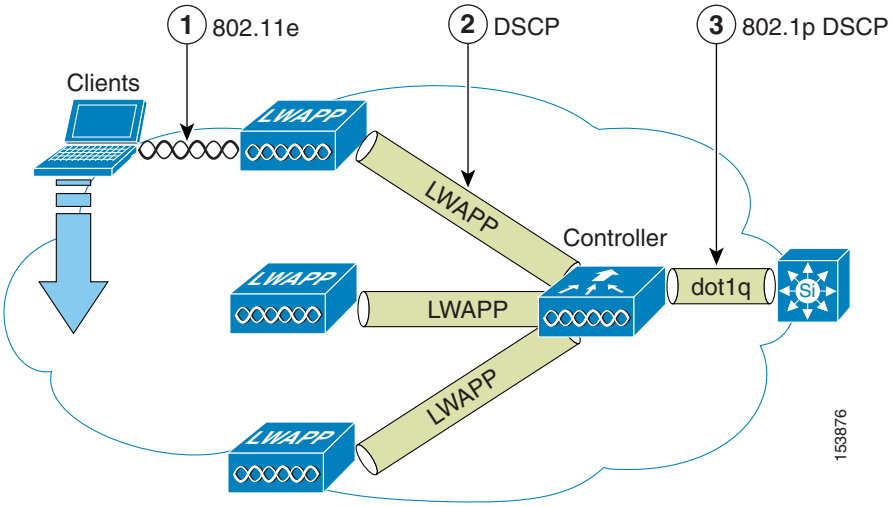
WLAN data in a Unified Wireless network is tunneled via LWAPP (IP UDP packets). To maintain the QoS classification that has been applied to WLAN frames, a process of mapping classifications to and from DSCP to CoS is required.

For example, when WMM classified traffic is sent by a WLAN client, it has an 802.1P classification in its frame. The AP needs to translate this classification into a DSCP value for the LWAPP packet carrying the frame to ensure that the packet is treated with the appropriate priority on its way to the WLC. A similar process needs to occur on the WLC for LWAPP packets going to the AP.

A mechanism to classify traffic from non-WMM clients is also required, so that their LWAPP packets can also be given an appropriate DSCP classification by the AP and the WLC.

Figure 5-22 shows the various classification mechanisms in the LWAPP WLAN network.

Figure 5-22 WMM and 802.1P Relationship



The multiple classification mechanisms and client capabilities require multiple strategies:

- LWAPP control frames require prioritization, and LWAPP control frames are marked with a DSCP classification of CS6.
- WMM-enabled clients have the classification of their frames mapped to a corresponding DSCP classification for LWAPP packets to the WLC. This mapping follows the standard IEEE CoS-to-DSCP mapping, with the exception of the changes necessary for QoS baseline compliance. This DSCP value is translated at the WLC to a CoS value on 802.1Q frames leaving the WLC interfaces.

- Non-WMM clients have the DSCP of their LWAPP tunnel set to match the default QoS profile for that WLAN. For example, the QoS profile for a WLAN supporting 7920 phones would be set to platinum, resulting in a DSCP classification of EF for data frames packets from that AP WLAN.
- LWAPP data packets from the WLC have a DSCP classification that is determined by the DSCP of the wired data packets sent to the WLC. The 80211.e classification used when sending frames from the AP to a WMM client is determined by the AP table converting DSCP to WMM classifications.

Note The WMM classification used for traffic from the AP to the WLAN client is based on the DSCP value of the LWAPP packet, and not the DSCP value of the contained IP packet. Therefore, it is critical that an end-to-end QoS system is in place.

QoS Baseline Priority Mapping

The LWAPP AP and WLC perform QoS baseline conversion, so that WMM values as shown in Table 5-7 are mapped to the appropriate QoS baseline DSCP values, rather than the IEEE values.

Table 5-7 Access Point QoS Translation Values[1]

AVVID 802.1 UP-Based Traffic Type	AVVID IP DSCP	AVVID 802.1p UP	IEEE 802.11e UP
Network control	-	7	-
Inter-network control (LWAPP control, 802,11 management	48	6	7
Voice	46 (EF)	5	6
Video	34 (AF41)	4	5
Voice Control	26 (AF31)	3	4
Background (gold)	18 (AF21)	2	2
Background (gold)	20 (AF22)	2	2
Background (gold)	22 (AF23)	2	2
Background (silver)	10 (AF11)	1	1
Background (silver)	12 (AF12)	1	1
Background (silver)	14 (AF13)	1	1
Best Effort	0 (BE)	0	0, 3
Background	2	0	1
Background	4	0	1
Background	6	0	1

1. The IEEE 802.11e UP value for DSCP values that are not mentioned in the table is calculated by considering 3 MSB bits of DSCP. For example, the IEEE 802.11e UP value for DSCP 32 (100 000 in binary), would be the decimal converted value of the MSB (100) which is 4. The 802.11e UP value of DSCP 32 is 4.

Deploying QoS Features on LWAPP-based APs

When deploying WLAN QoS on the APs, consider the following:

- The wired LWAPP AP interface does read or write Layer 2 CoS (802.1P) information, the WLC and the APs depend on Layer 3 classification (DSCP) information to communicate WLAN client traffic classification. This DSCP value may be subject to modification by intermediate routers, and therefore the Layer 2 classification received by the destination might not reflect the Layer 2 classification marked by the source of the LWAPP traffic.
- The APs no longer use NULL VLAN ID. As a consequence, L2 LWAPP does not effectively support QoS because the AP does not send the 802.1P/Q tags, and in L2 LWAPP there is no outer DSCP on which to fall back.
- APs do not re-classify frames; they prioritize based on CoS value or WLAN profile.
- APs carry out EDCF-like queuing on the radio egress port only.
- APs do FIFO queueing only on the Ethernet egress port.

WAN QoS and the H-REAP

For WLANs that have data traffic forwarded to the WLC, the behavior is same as non-hybrid remote edge access point (H-REAP) APs. For locally-switched WLANs with WMM traffic, the AP marks the dot1p value in the dot1q VLAN tag for upstream traffic. This occurs only on tagged VLANs; that is, not native VLANs.

For downstream traffic, the H-REAP uses the incoming dot1q tag from the Ethernet side and uses this to queue and mark the WMM values on the radio of the locally-switched VLAN.

The WLAN QoS profile is applied both for upstream and downstream packets. For downstream, if an 802.1P value that is higher than the default WLAN value is received, the default WLAN value is used. For upstream, if the client sends an WMM value that is higher than the default WLAN value, the default WLAN value is used. For non-WMM traffic, there is no CoS marking on the client frames from the AP.

Note Bug CSCsi78368 currently impacts the CoS Marking of traffic from the WLC and the CoS marked on frames sent by the WLC represents the value set by the QoS profile and not the WMM CoS marked by the client.

Guidelines for Deploying Wireless QoS

The same rules for deploying QoS in a wired network apply to deploying QoS in a wireless network. The first and most important guideline in QoS deployment is to know your traffic. Know your protocols, the sensitivity to delay of your application, and traffic bandwidth. QoS does not create additional bandwidth; it simply gives more control over where the bandwidth is allocated.

Throughput

An important consideration when deploying 802.11 QoS is to understand the offered traffic, not only in terms of bit rate, but also in terms of frame size, because 802.11 throughput is sensitive to the frame size of the offered traffic.

Table 5-8 shows the impact that frame size has on throughput: as packet size decreases, so does throughput. For example, if an application offering traffic at a rate of 3 Mbps is deployed on an 11 Mbps 802.11b network, but uses an average frame size of 300 bytes, no QoS setting on the AP allows the

application to achieve its throughput requirements. This is because 802.11b cannot support the required throughput for that throughput and frame size combination. The same amount of offered traffic, having a frame size of 1500 bytes, does not have this issue.

Table 5-8 Throughput Compared to Frame Size

	300	600	900	1200	1500	Frame Size (bytes)
11g–54 Mbps	11.4	19.2	24.6	28.4	31.4	Throughput Mbps
11b–11 Mbps	2,2	3.6	4.7	5.4	6	Throughput Mbps

QoS Example LAN Switch Configuration

AP Switch Configuration

The QoS configuration of the AP switch is relatively trivial because the switch must trust the DSCP of the LWAPP packets that are passed to it from the AP. There is no CoS marking on the LWAPP frames coming from the AP. The following is an example of this configuration. Note that this configuration addresses only the classification, and that queueing commands may be added, depending on local QoS policy.

```
interface GigabitEthernet1/0/1
 switchport access vlan 100
 switchport mode access
 mls qos trust dscp
 spanning-tree portfast
end
```

In trusting the AP DSCP values, the access switch is simply trusting the policy set for that AP by the WLC. The maximum DSCP value assigned to client traffic is based on the QoS policy applied to the WLANs on that AP.

WLC Switch Configuration

The QoS classification decision at the WLC-connected switch is a bit more complicated than at the AP-connected switch, because the choice can be to either trust the DSCP or the CoS of traffic coming from the WLC. In this decision there are a number of points to consider:

- Traffic leaving the WLC can be either upstream (to the WLC or network) or downstream (the AP and WLAN client). The downstream traffic is LWAPP encapsulated, and the upstream traffic is from AP and WLAN clients, either LWAPP encapsulated or decapsulated WLAN client traffic, leaving the WLC.
- DSCP values of LWAPP packets are controlled by the QoS policies on the WLC; the DSCP values set on the WLAN client traffic encapsulated by the LWAPP tunnel header has not been altered from those set by the WLAN client.
- CoS values of frames leaving the WLC are set by the WLC QoS policies, regardless of whether they are upstream, downstream, encapsulated, or decapsulated.

The following example chooses to trust the CoS of settings of the WLC, because this allows a central location for the management of WLAN QoS, rather than having to manage the WLC configuration and an additional policy at the WLC switch connection. Other customers wishing to have a more precise degree of control may wish to implement QoS classification policies on the WLAN-client VLANs.

```
interface GigabitEthernet1/0/13
```

```
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 11-13,60,61
 switchport mode trunk
 mls qos trust cos
end
```

Traffic Shaping, Over the Air QoS, and WMM Clients

Traffic shaping and over-the-air QoS are useful tools in the absence of WLAN WMM features, but they do not address the prioritization of 802.11 traffic directly. For WLANs that support WMM clients or 7920 handsets, the WLAN QoS mechanisms of these clients should be relied on; no traffic shaping or over-the-air QoS should be applied to these WLANs.

WLAN Voice and the Cisco 7921G and 7920

The Cisco 7921G and the Cisco 7920 are Cisco VoWLAN handsets. Their use is one of the most common reasons for deploying QoS on a WLAN.

For more information on each of these handsets, see the following:

- Cisco Unified Wireless IP Phone 7921G Version 1.0(2)—http://www.cisco.com/en/US/products/hw/phones/ps379/products_data_sheet0900aecd805e315d.html
- Cisco Unified Wireless IP Phone 7920 Version 3.0—http://www.cisco.com/en/US/products/hw/phones/ps379/products_data_sheet09186a00801739bb.html

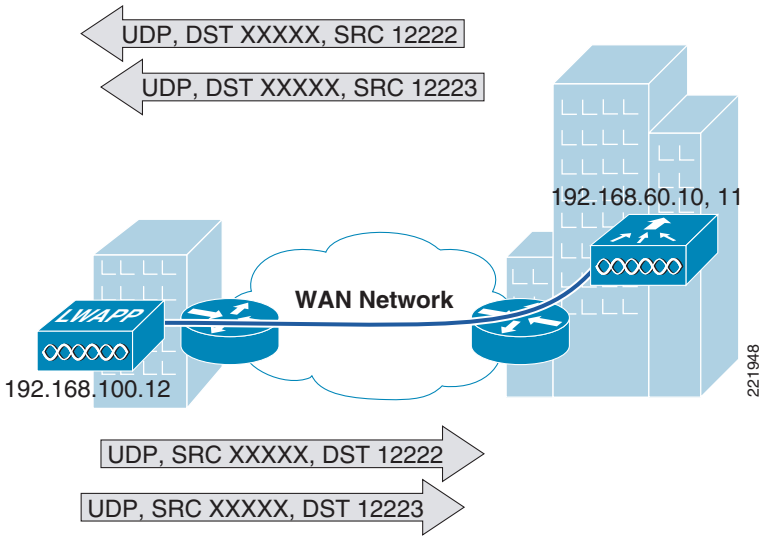
Deploying VoWLAN infrastructure involves more than simply providing QoS on WLAN. A voice WLAN needs to consider site survey coverage requirements, user behavior, roaming requirements, and admission control. These are covered in the following guides:

- Design Principles for Voice Over WLAN—http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/net_implementation_white_paper0900aecd804f1a46.html
- Cisco Wireless IP Phone 7920 Design and Deployment Guide—http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7920/5_0/english/design/guide/7920ddg.html

LWAPP over WAN Connections

This section describes QoS strategies when LWAPP APs are deployed across WAN links, as illustrated in Figure 5-23.

Figure 5-23 LWAPP Traffic Across the WAN



LWAPP Traffic Classification

LWAPP APs can be generally separated into the following two types:

- LWAPP control traffic—Identified by UDP port 12223
- LWAPP 802.11 traffic—Identified by UPD port 12222

LWAPP Control Traffic

LWAPP control traffic can be generally divided into the following two additional types:

- Initialization traffic—Generated when an LWAPP AP is booted and joins an LWAPP system. For example, the traffic generated by controller discovery, AP configuration, and AP firmware updates.

Note LWAPP image packets from the controller are marked best-effort, but their acknowledgement is marked CS6. Note that there is no windowing of the protocol, and each additional packet is sent only after an acknowledgement. This type of handshaking minimizes the impact of downloading files over a WAN

- Background traffic—Generated by an LWAPP AP when it is an operating member of a WLAN network. For example, LWAPP heartbeat, RRM, rogue AP measurements. Background LWAPP control traffic is marked CS6.

Figure 5-24 and Figure 5-25 show examples of the initial LWAPP control messages. Figure 5-26, Figure 5-27, and Figure 5-28 show examples of background LWAPP control messages.

A full list of initial LWAPP control messages includes the following:

- LWAPP discovery messages
- LWAPP join messages
- LWAPP config messages

- Initial LWAPP RRM messages

Although AP image download is also discussed in this section, it is not typically part of an AP initialization, and would only occur during firmware changes.

Figure 5-24 LWAPP Discovery Message

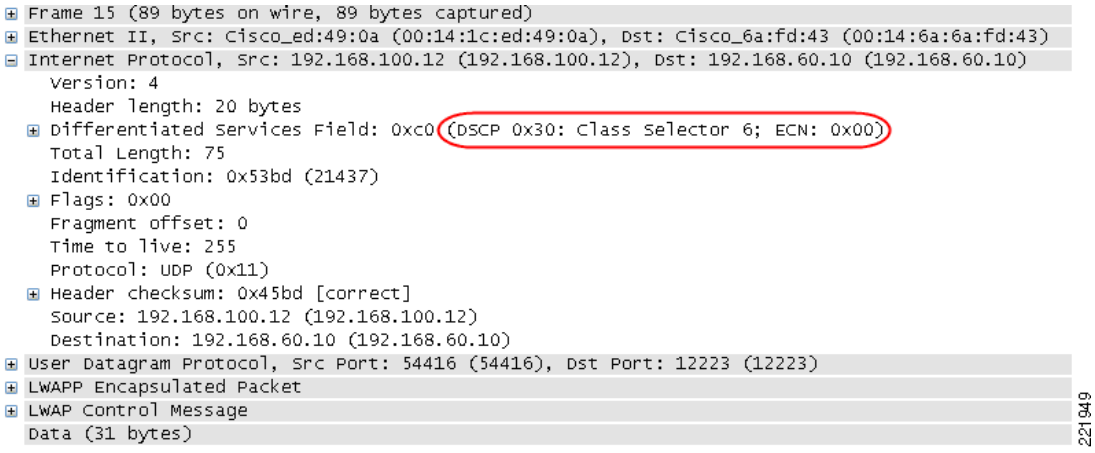


Figure 5-25 LWAPP Image Response

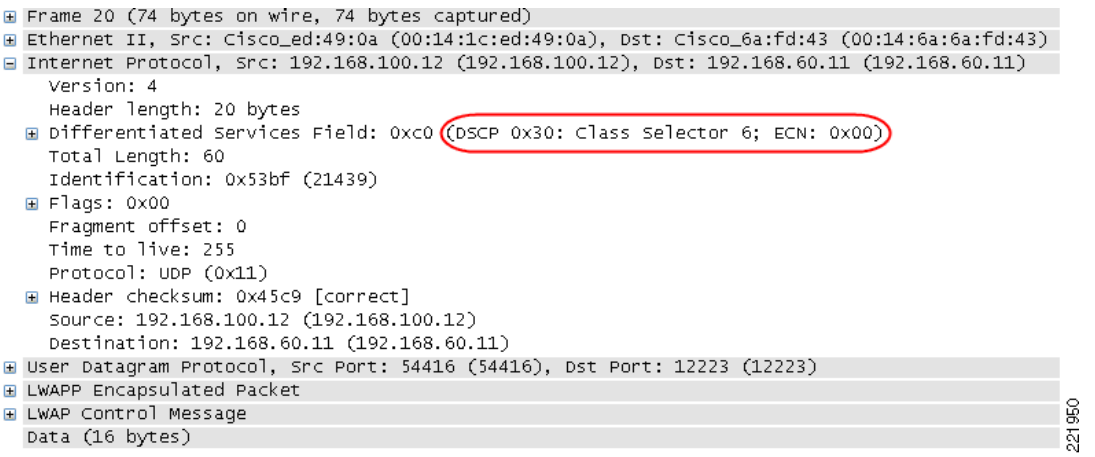


Figure 5-26 LWAPP Heartbeat Messages

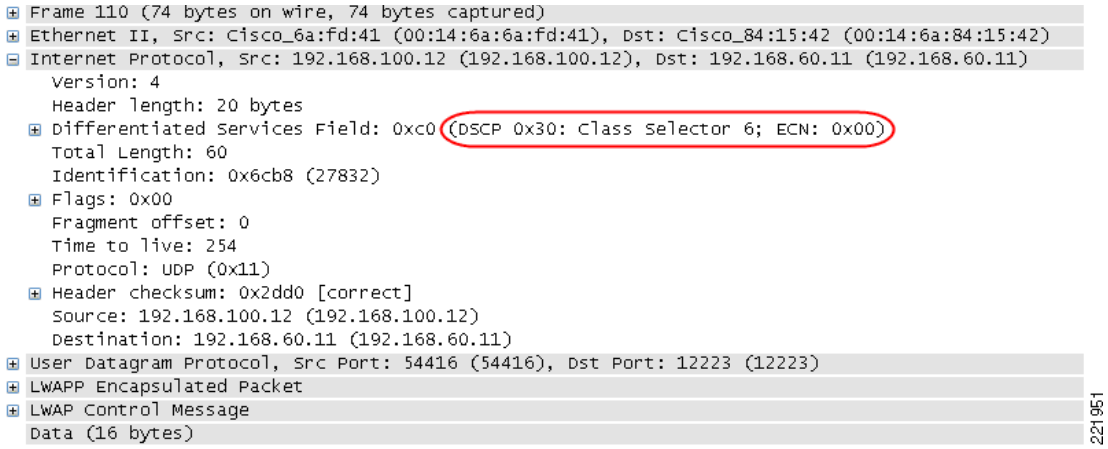


Figure 5-27 LWAPP Statistics

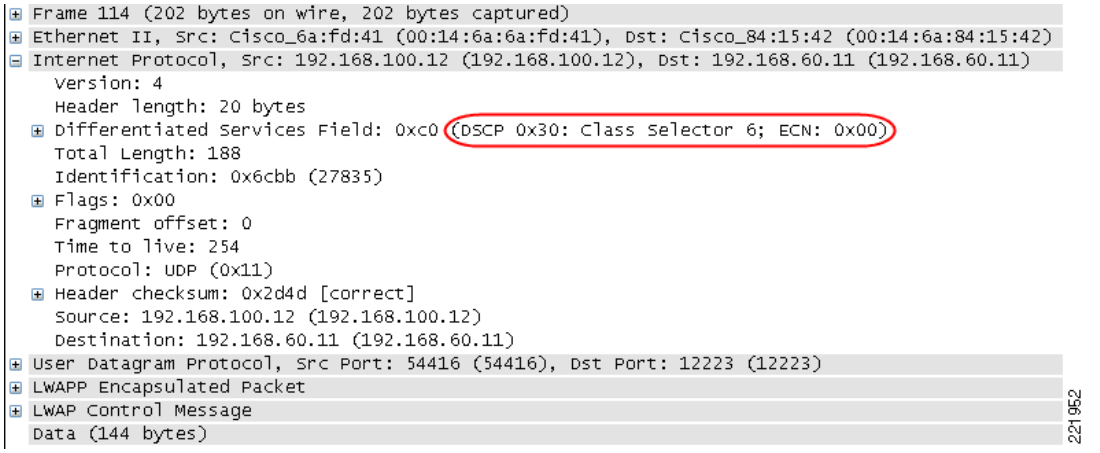
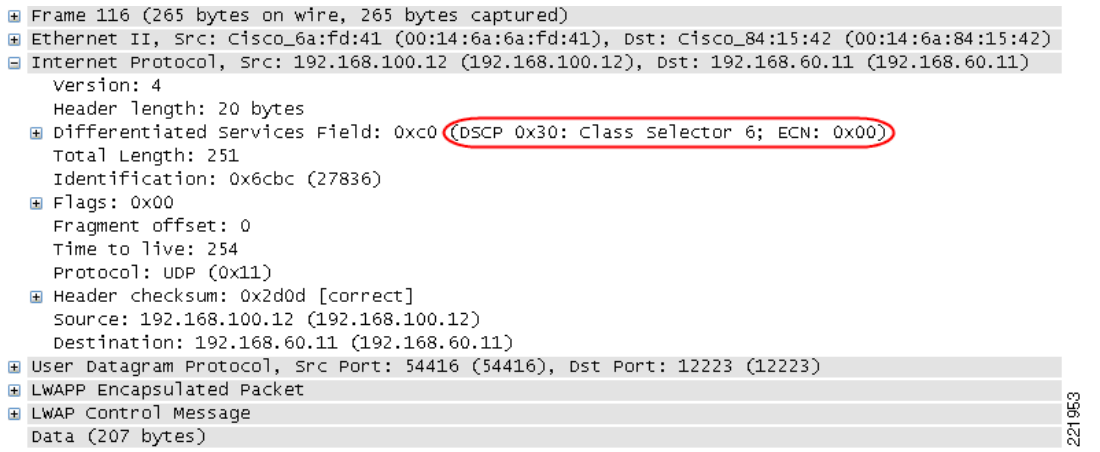


Figure 5-28 LWAPP RRM



LWAPP 802.11 Traffic

LWAPP 802.11 traffic can be divided generally into the following two additional types:

- 802.11 management frames—802.11 management frames such as probe requests, and association requests and responses are classified automatically with a DSCP of CS6.
- 801.11 data frames—Client data and 802.1X data from the client is classified according to the WLAN QoS settings, but packets containing 802.1X frames from the WLC are marked CS4. 802.11 data traffic classification depends on the QoS policies applied in the WLAN configuration, and is not automatic. The default classification for WLAN data traffic is best-effort.

Classification Considerations

The DSCP classification of used LWAPP control traffic is CS6, which is an IP routing class, and is intended for IP routing protocols such as Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), and so on.

The current LWAPP DSCP classification represents a classification that, although optimal for the WLAN system, may not align with the QoS policies and needs of each customer.

In particular, a customer may wish to minimize the amount of CS6-classified traffic generated by the WLAN network. They may wish to stop CS6 traffic generated by client activity such as probe requests. The simplest mechanism to do this would be to reclassify the LWAPP 802.11 CS6 traffic to a different DSCP. The fact that the LWAPP UDP port used is different from that used by LWAPP data, and the default DSCP marking allow for remarking this traffic without resorting to deep packet inspection.

In addition, a customer may wish to ensure that LWAPP initialization traffic does not impact routing traffic. The simplest mechanism for ensuring this is to mark LWAPP control traffic that is in excess of the background rate with a lower priority.

LWAPP Traffic Volumes

Cisco testing has found that the average background traffic per AP is approximately 305 bits/sec.

Calculating the average initial traffic per AP is more difficult, because the average time taken for an AP to go from rebooted to operational is a function of the WAN speed, as well as that of the WLC and AP. In reality, the difference is minimal. While on a lab test network, the best of initial traffic might average 2614 bit/sec over 18 seconds. With a WAN link with a 100 ms RTT, the average is 2318 bits/sec over 20.3 seconds.

Example Router Configurations

This section contains router configuration examples to be used as guides when addressing CS6 remarking or LWAPP control traffic load.

This example uses LWAPP APs on the 192.168.101.0/24 subnet, and two WLCs with ap-managers at 192.168.60.11, and 192.168.62.11.

Remarking Client Generated CS6 Packets

The following shows a sample configuration for remarking LWAPP data packets marked as CS6 to a more appropriate value of CS3. This moves the traffic to a more suitable classification, at the level of call control, rather than at the level of network control.

```
class-map match-all LWAPPDATACS6
 match access-group 110
 match  dscp cs6
!
policy-map LWAPPDATACS6
 class LWAPPDATACS6
  set dscp cs3
!
interface FastEthernet0
 ip address 192.168.203.1 255.255.255.252
service-policy input LWAPPDATACS6
!
access-list 110 remark LWAPP Data
access-list 110 permit udp 192.168.101.0 0.0.0.255 host 192.168.60.11 eq 12222
access-list 110 permit udp 192.168.101.0 0.0.0.255 host 192.168.62.11 eq 12222
access-list 111 remark LWAPP Control
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.60.11 eq 12223
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.62.11 eq 12223
```

Changing the DSCP of LWAPP Control Traffic above a predefined rate

The following shows an example of rate limiting the LWAPP control traffic from the WAN site to minimize the impact of the CS6-marked control traffic on routing traffic. Note that the rate limit configuration does not drop non-conforming traffic, but simply reclassifies that traffic.

Note Note that this is an example, and not a recommendation. Under normal circumstances, and following the design guidelines for deploying APs over a WAN connection, it is unlikely that LWAPP control traffic would impact the WAN routing protocol connection.

```
interface Serial0
 ip address 192.168.202.2 255.255.255.252
 rate-limit output access-group 111 8000 3000 6000 conform-action transmit exceed-action
set-dscp-transmit 26
access-list 111 remark LWAPP Control
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.60.11 eq 12223
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.62.11 eq 12223
!
```

For more information on WLAN QoS and 802.11e, refer to the IEEE 802.11 Handbook, A designers companion (second edition), Bob O'Hara and Al Petrick.

CHAPTER 6

Cisco Unified Wireless Multicast Design

Introduction

This chapter describes the Cisco Unified Network Multicast in IP multicast forwarding and provides information on how to deploy multicast in a wireless environment. A prerequisite for using the multicast performance functionality is that a multicast-enabled network must be configured on all routers between the controllers and the APs. To accommodate networks that do not support multicast, the controller continues to support the original unicast packet forwarding mechanism.

IP multicast is a delivery protocol for information to a group of destinations. It uses the most efficient strategy to deliver the information over each link of the network. It sends only one copy of the information at each hop of the network, creating copies only when the links to the destinations split. Typically, many of today's networks applications use unicast packets i.e., from one source to one destination. However when multiple receivers require the same data, replicating the data from the source to all the receivers as individual unicast packets increases the network load. IP multicast enables efficient transfer of data from a set of sources to a dynamically formed set of receivers.

IP multicast is typically used today for one way streaming media, such as video to large groups of receivers. Many cable TV operators, educational institutions and large enterprises have deployed IP multicast for their content delivery needs. Additionally, there have been some uses of audio and video conferencing using multicast. Another widespread use of multicast within campus and commercial networks is for file distribution, particularly to deliver operating system images and updates to remote hosts. IP multicast has also seen deployment within the financial sector for applications such as stock tickers and hoot-n-holler systems.

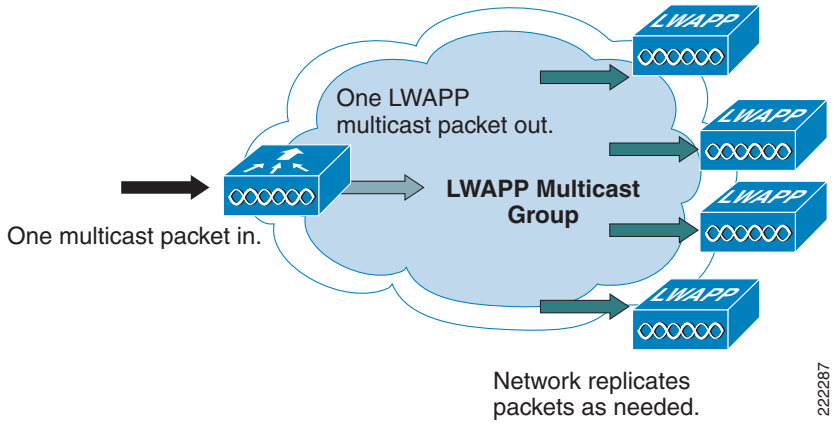
Overview of Multicast Forwarding in Cisco Unified Wireless Networks

With Cisco Unified Wireless Network Software Release 4.1, significant enhancements are made to support the effective use of multicast in a wireless network. In 3.1 and prior software releases, packets intended to be multicast were actually unicast on the wireless network. Multicast support was added in 3.2, but there were some configuration limitations that required broadcast to be enabled. With 4.1, controller software release separate broadcast and multicast support is enabled, allowing networks to be configured with just multicast, broadcast, or the use of both multicast and broadcast.

With the current Cisco Unified Wireless multicast support, each multicast frame received by the controller from a VLAN on the first hop router was copied and sent to the multicast group configured on the controller for the AP that are associated, as shown in Figure 6-1. The multicast LWAPP packet containing the multicast packet uses a WLAN bitmap, which tells the receiving AP which WLAN it must

forward the packet to. When the AP receives the LWAPP packet, it strips off the outer LWAPP encapsulation and transmits the multicast packet to the WLAN (on all radios associated to the WLAN) identified in the LWAPP WLAN ID bitmask.

Figure 6-1 Multicast Forwarding Mechanism in Version 4.1 and Below



Effectively, an LWAPP multicast group is used to deliver the multicast packet to each access point. This allows the routers in the network to use standard multicast techniques to replicate and deliver multicast packets to the APs. For the LWAPP multicast group, the controller becomes the multicast source and the APs become the multicast receivers.

Note A prerequisite for using the new multicast performance functionality is that a multicast enabled network is configured on all routers between the controllers and the APs. To accommodate networks that do not support multicast, the controller continues to support the original unicast packet forwarding mechanism.

Note With multicast enabled, any kind of multicast packet received on the VLAN from the first hop router is transmitted over the wireless including HSRP hellos, all router, EIGRP, and PIM multicast packets.

After the administrator enables multicast (multicast mode is disabled by default) and configures an LWAPP multicast group, the access points downloads the controller's LWAPP multicast group address during the normal join process (at boot time) to the controller. After an access point joins a controller and downloads its configuration, the AP issues an Internet Group Management Protocol (IGMP) join request to join the controller's LWAPP multicast group. This triggers the normal setup for the multicast state in the multicast-enabled routers between the controller and APs. The source IP address for the multicast group is the controller's management interface IP address, not the AP-manager IP address used for Layer 3 mode. Once the AP has joined the controllers LWAPP multicast group, the multicast algorithm for client multicast traffic works as described below.

When the source of the multicast group is on the wired LAN:

- When the controller receives a multicast packet from any of the client VLANs on the first hop router, it transmits the packet to the LWAPP multicast group via the management interface at the best effort QoS classification. The QoS bits for the LWAPP multicast packet are hard coded at the lowest level and are not user changeable.

- The multicast-enabled network delivers the LWAPP multicast packet to each of the access points that have joined the LWAPP multicast group, using the normal multicast mechanisms in the routers to replicate the packet along the way as needed so that the multicast packet reaches all APs (Figure 6-1). This relieves the controller from replicating the multicast packets.
- Access points may receive other multicast packets but will only process the multicast packets that are sourced from the controller they are currently joined to; any other copies are discarded. If more than one WLAN is associated to the VLAN interface where the original multicast packet was sourced, the AP transmits the multicast packet over each WLAN (following the WLAN bitmap in the LWAPP header). Additionally, if that WLAN is on both radios (802.11g and 802.11a), both radios transmit the multicast packet on the WLAN if there are clients associated, even if those clients did not request the multicast traffic.

When the source of the multicast group is a wireless client:

- The multicast packet is unicast (LWAPP encapsulated) from the AP to the controller similar to standard wireless client traffic.
- The controller makes two copies of the multicast packet. One copy is sent out the VLAN associated with the WLAN it came on, enabling receivers on the wired LAN to receive the multicast stream and the router to learn about the new multicast group. The second copy of the packet is LWAPP-encapsulated and is sent to the LWAPP multicast group so that wireless clients may receive the multicast stream.

Wireless Multicast Roaming

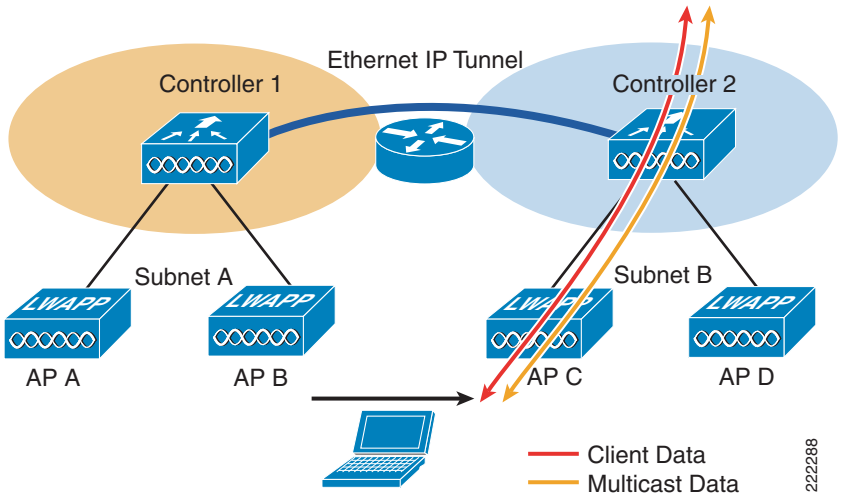
A major challenge for a multicast client in a wireless environment is maintaining its multicast group membership when moving about the WLAN. Drops in the wireless connection moving from AP-to-AP can cause a disruption in a client's multicast application. Internet Group Management Protocol (IGMP) plays an important role in the maintenance of dynamic group membership information.

A basic comprehension of IGMP is important for understanding what happens to a client's multicast session when it roams about the network. In a Layer 2 roaming case, sessions are maintained simply because the foreign AP, if configured properly, already belongs to the multicast group and traffic is not tunneled to a different anchor point on the network. Layer 3 roaming environments are a little more complex in this manner and depending on what tunneling mode you have configured on your controllers, the IGMP messages sent from a wireless client will be affected. The default mobility tunneling mode on a controller is asymmetrical. As discussed in the Chapter 2, "Cisco Unified Wireless Technology and Architecture," this means that return traffic to the client is sent to the anchor WLC then forwarded to the foreign WLC where the associated client connection resides. Outbound packets are forwarded out the foreign WLC interface. In symmetrical mobility tunneling mode, both inbound and outbound traffic are tunneled to the anchor controller. For more information on mobility tunneling, see Chapter 2, "Cisco Unified Wireless Technology and Architecture."

Asymmetric Multicast Tunneling

In asymmetric multicast tunneling, when a client roams to a new AP associated to a different WLC and on a different subnet, it is queried for its multicast group memberships by the foreign WLC and send out an IGMP group membership report. This is forwarded out the foreign WLC dynamic interface assigned to the VLAN and the client rejoins the multicast stream through the foreign subnet. Figure 6-2 illustrates the traffic flow for normal data and multicast data.

Figure 6-2 Asymmetric Tunneling



Note In the event of a client roam there is a slight disruption in the multicast session; in some applications it may be considered unsuitable for use.

Multicast Enabled Networks

A prerequisite for using this new multicast performance functionality is that a multicast enabled network is configured on all routers between the controllers and the APs. A multicast-enabled network allows for an efficient way to deliver a packet to many hosts across the network. IP multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients. Packets are replicated as necessary at each Layer 3 point in the network. A multicast routing protocol, such as PIM, is required if there is more than one router between the controllers and APs. For more information on setting up a multicast-enabled network, refer to the following URL: http://www.cisco.com/go/multicast.

LWAPP Multicast Reserved Ports and Addresses

The controller blocks all multicast packets sent to any multicast group that have a destination port of 12222 through 12224. Additionally, all packets with a multicast group address equal to the controller's LWAPP multicast group address are blocked at the controller. This is to prevent fragmented LWAPP encapsulated packets from another controller being retransmitted (see the "Fragmentation and LWAPP Multicast Packets" section on page 6-6 for more information). Ensure that the multicast applications on your network do not use these reserved ports or LWAPP multicast group addresses.

Enabling Multicast Forwarding on the Controller

IP Multicast traffic through the controller is disabled by default. WLAN clients cannot receive multicast traffic when it is disabled. If you wish to turn on multicast traffic to the WLAN clients, follow these steps:

Step 1 If you *have* a multicast enabled network, select **multicast** under Ethernet Multicast Mode to use the method where the network replicates the packets

Step 2 You *do not have* a multicast enabled network, select **unicast** under Ethernet Multicast Mode to use the method where the controller replicates the packets.

Step 3 On the controller general webpage, ensure the LWAPP transport mode is set to Layer 3. The multicast performance feature only works in this mode.

Step 4 Select multicast in the drop down menu for the Ethernet Multicast Mode and type in a multicast group address. This option is shown in Figure 6-3.

Figure 6-3 Commands to turn on Ethernet Multicast Mode via the GUI.

CLI Commands to Enable Ethernet Multicast Mode

Step 1 Enable the CLI command: **configure network multicast global enable**

Step 2 Enable the CLI command: **config network multicast mode multicast** *<IP Address>*

Use the **show network** command to verify the multicast mode on the controller and **show lwapp mcast** to verify the group on the AP. Other useful commands are **show ip mroute** and **show ip igmp membership** on the routers.

Multicast Deployment Considerations

Recommendations for Choosing an LWAPP Multicast Address

Caution Although not recommended, any multicast address can be assigned to the LWAPP multicast group including the reserved link local multicast addresses used by OSPF, EIGRP, PIM, HSRP, and other multicast protocols.

Cisco recommends that multicast addresses be assigned from the administratively scoped block 239/8. IANA has reserved the range of 239.0.0.0-239.255.255.255 as administratively scoped addresses for use in private multicast domains (see the note below for additional restrictions). These addresses are similar in nature to the reserved private IP unicast ranges (such as 10.0.0.0/8) defined in RFC 1918. Network administrators are free to use the multicast addresses in this range inside of their domain without fear of conflicting with others elsewhere in the Internet. This administrative or private address space should be used within the enterprise and blocked from leaving or entering the autonomous domain (AS).

Note Do not use the 239.0.0.*X* address range or the 239.128.0.*X* address range. Addresses in these ranges overlap with the link local MAC addresses and will flood out all switch ports even with IGMP snooping turned on.

Cisco recommends that enterprise network administrators further subdivide this address range into smaller geographical administrative scopes within the enterprise network to limit the “scope” of particular multicast applications. This is used to prevent high-rate multicast traffic from leaving a campus (where bandwidth is plentiful) and congesting the WAN links. It also allows for efficient filtering of the high bandwidth multicast from reaching the controller and the wireless network.

For more information on multicast address guidelines, refer to the document at the following URL:

http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a00802d4643.shtml

Fragmentation and LWAPP Multicast Packets

When a controller receives a multicast packet, it encapsulates it inside of LWAPP using the LWAPP multicast group as a destination address and forward it to the APs via the management interface (source address). If the packet exceeds the MTU of the link, the controller fragments the packet and send out both packets to the LWAPP multicast group. If another controller were to receive this LWAPP encapsulated multicast packet via the wired network, it would re-encapsulate it again, treating it as a normal multicast packet and forward it to its APs.

There are two different options to prevent this from happening, either of which is effective by itself. One, you may assign all controllers to the same LWAPP multicast group address. Or two, you can apply standard multicast filtering techniques to ensure that LWAPP encapsulated multicast packets do not reach any other controller. Table 6-1 lists the pros and cons of these two techniques.

Table 6-1 Pros and Cons of using the same Multicast Group or Different Groups

	PROS	CONS
All controllers have the same LWAPP multicast group	No need to do any additional fragmentation protection measures	Each controller's multicast traffic is flooded throughout the network (APs will drop multicast packets that don't have a source IP address equal to their controller management interface)
Standard multicast techniques are used to block LWAPP multicast fragments	Can use a range of addresses thus preventing flooding throughout the network.	ACL filtering must be applied on first hop router on all VLANs configured on multicast enabled controllers

All Controllers have the Same LWAPP Multicast Group

To prevent the second controller from retransmitting these LWAPP encapsulated packets, the controllers blocks incoming multicast packets to the LWAPP multicast group and the LWAPP reserved ports. By blocking the reserved ports, the controller blocks the first part of a fragmented packet in an encapsulated LWAPP multicast packet. However, the second packet does not contain port numbers and can only be blocked by filtering it on the multicast group address (destination address). The controller blocks any packets where the destination address is equal to the LWAPP multicast group address assigned to the controller.

However, assigning every controller to the same LWAPP multicast group creates other problems. IGMP version 1 and 2 used by the APs to join the LWAPP multicast group use Any Source Multicast (ASM) and the APs will receive multicast traffic from all sources of the multicast group in the network. This means the APs will receive multicast packets from all of the controllers on the network if the controllers are configured with the same multicast group address, and no multicast boundaries have been applied. One controller's multicast traffic will flood out to all of the APs across the network and every APs receive (and drop it if the source address is not equal to its controller's management address) the multicast traffic that is being received from any wireless multicast client in the entire network. Additionally, locally sourced multicast packets from any client VLAN such as HSRP, PIM, and EIGRP and OSPF multicast packets will also be flooded throughout the network.

Note Cisco IOS APs (e.g. 1240) use IGMPv2 while VxWorks APs (e.g. 1030) use IGMPv1.

Controlling Multicast on the WLAN Using Standard Multicast Techniques

Normal boundary techniques should be used in your multicast enabled network. These include using the **ip multicast boundary** interface mode command, which filters IP multicast traffic and also Auto-RP messages.

Note A wired client anywhere in the network may request the LWAPP multicast stream and receive it from all sources (if multicast boundaries are not applied). Multicast streams are not encrypted when they are encapsulated in the LWAPP multicast packet. Therefore, it is recommended that multicast boundaries be implemented to block this type of access.

In the past, Time To Live field in the IP Multicast datagram was used for creating Auto-RP administrative boundaries using the **ttl-threshold** command. This has been superseded by the **ip multicast boundary** interface mode command, which filters IP multicast traffic and also Auto-RP messages. Cisco recommends using the new command.

Other useful commands include the **ip multicast rate-limit interface** command. This command enforces low rates on the wireless VLANs. Without it, even if the network engineer filters the high rate multicast addresses, a low rate multicast address cannot exceed its rate.

A typical example on a wireless client VLAN is given below. For more information on other multicast commands for a multicast enabled network refer to http://www.cisco.com/go/multicast. Filtering for multicast-enabled traffic also allows you to prevent propagation of certain worms like the sasser worm which relied on the TCP and ICMP transports with multicast addresses. Blocking these types of traffic with multicast group addresses does not affect most applications since they typically use UDP or TCP for streaming.

In the following example, packets to the multicast group range 239.0.0.0 to 239.127.255.255 from any source will have their packets rate-limited to 128 kbps. The example also sets up a boundary for all multicast addresses not in the lower administratively scoped addresses. In addition, hosts serviced by Vlan40 can only join the lower administrative groups 239.0.0.0 to 239.127.255.255.

```
mls qos
!
class-map match-all multicast_traffic
  description Permit Low Rate Multicast Range of 239.0.0.0 to 239.127.0.0
  match access-group 101
!
policy-map multicast
 description Rate Limit Multicast traffic to 2.56mps with burst of 12800 bytes
  class multicast_traffic
   police cir 2560000 bc 12800 be 12800 conform-action transmit exceed-action drop
!
interface Vlan40
 description To Wireless Clients
 ip address 10.20.40.3 255.255.255.0
 ip pim sparse-mode
 ip multicast boundary 1
 ip igmp access-group 30
 standby 40 ip 10.20.40.1
 standby 40 preempt
 service-policy output multicast
!
access-list 1 remark Permit Low Rate Multicast Range of 239.0.0.0 to 239.127.0.0 for
multicast boundary
access-list 1 permit 239.0.0.0 0.127.255.255
!
access-list 30 remark Only Allow IGMP joins to this Multicast Group Range
access-list 30 permit 239.0.0.0 0.127.255.255
!
access-list 101 remark Permit Low Rate Multicast Range of 239.0.0.0 to 239.127.0.0 for
class-map
access-list 101 permit ip any 239.0.0.0 0.127.255.255
```

How Controller Placement Impacts Multicast Traffic and Roaming

Note The multicast stream in either deployment, distributed or collocated, is not rate-limited and there is no way to put ACLs on it. Once enabled, all multicast traffic is forwarded to the wireless including HSRP, EIGRP, OSPF, and PIM packets

We look at two different deployments (distributed and centralized) and how they impact roaming with multicast clients. In a centralized deployment, WLC WLAN interfaces are attached to the same VLANs/subnets, the multicast streams is uninterrupted when a multicast client roams from APs on one WLC to an AP on another WLC. The centralized deployment creates a flat WLC client multicast network. The reason centralized WLCs do not affect multicast roaming is because once the multicast stream is requested from a single multicast client on a WLAN, it streams out all APs on that WLAN, on all radios (802.11g and 802.11a), on all WLCs, even if that access point WLAN has no clients associated with it that have requested the multicast traffic. If you have more than one WLAN associated to the VLAN, the AP transmits the multicast packet over each WLAN. Both the unicast mode LWAPP packet and the multicast mode LWAPP packet contain a WLAN bitmap that tells the receiving AP which WLAN it must forward the packet over.

The distributed deployment does not have this problem because while the WLANs are the same, the WLCs are attached to different VLANs. This means that when the multicast client roams to a new WLC, the WLC will first query the client for its multicast group memberships. At this point the client responds with its group membership report and the WLC forwards this message to the appropriate multicast group address through the VLAN associated with its local VLAN. This allows the client to resume its multicast session through the foreign WLC.

The distributed deployment reduces the amount of multicast traffic on the APs because, although the WLAN SSIDs are the same, the WLCs are attached to different VLANs. WLAN multicast traffic depends on a client request on the VLAN of that WLC. Table 6-2 lists the advantages and disadvantages of distributed and collocated deployments.

Table 6-2 Pros and Cons of Centralized WLCs and Distributed WLCs

	PROS	CONS
All centralized WLC WLANs connected to the same VLANs (subnets)	Multicast traffic started on any client VLAN will be transmitted to all APs so clients roaming to any AP will receive multicast stream	If only one client requests multicast traffic, all APs attached to all controllers will receive the stream and transmit it if they have any clients associated even if those clients did not request the multicast stream
Distributed WLCs on different VLANs and subnet	Multicast streams are isolated to APs attached to controller	Disruptions caused by multicast stream establishments after client roam

Additional Considerations

Two areas for additional consideration in multicast deployment are when implementing AP groups, and H-REAPs and REAPs. AP groups allow APs on the same controller to map the same WLAN (SSID) to different VLANs. If a client is roaming between APs in different groups, the multicast session will not function properly as this is currently not supported. Currently, the WLC forwards multicast only for the VLAN configured on the WLAN and does not take into consideration VLANs configured in AP groups.

REAP and H-REAP APs allow the local termination of WLANs at the network edge rather than at the WLC, and the multicast behavior is controlled at that edge. If an H-REAP WLAN is terminated on a WLC and multicast is enabled on that WLC, multicast is delivered to that H-REAP WLAN, if the LWAPP multicast group is allowed to extend to the H-REAP network location.

Even if the LWAPP multicast packets are not able to transit the network to the H-REAP, WLAN clients on that H-REAP are able to send IGMP joins to the network connected to the WLC, as these are unicast messages.

CHAPTER 7

Cisco Unified Wireless Hybrid REAP

As discussed earlier in this guide, the Cisco Unified Wireless solution uses the Lightweight Access Point Protocol (LWAPP) between LWAPP APs (LAPs) and a WLAN WLC (WLC) to both manage the APs and carry WLAN client traffic.

LAP deployments with one or more localized WLCs is typical for medium-to-large campus environments. However, there may be cases in small branch locations where wireless connectivity is required, but it is not practical to deploy a WLC. If a standard LAP is deployed at a branch with a centralized WLC located at the main campus, the LAP establishes LWAPP connectivity across the WAN to the main campus. All wireless user traffic at the branch traverses the WAN to the central WLC. This may work well if a majority of the services being accessed by the branch resides at the main campus. However, if wireless clients at the branch need to access local network resources (such as printers and servers), this approach may not be desirable, as client traffic would have to traverse the WAN twice (branch to central and central to branch) to reach a local device. Remote edge AP (REAP) and Hybrid REAP (H-REAP) were developed for this reason.

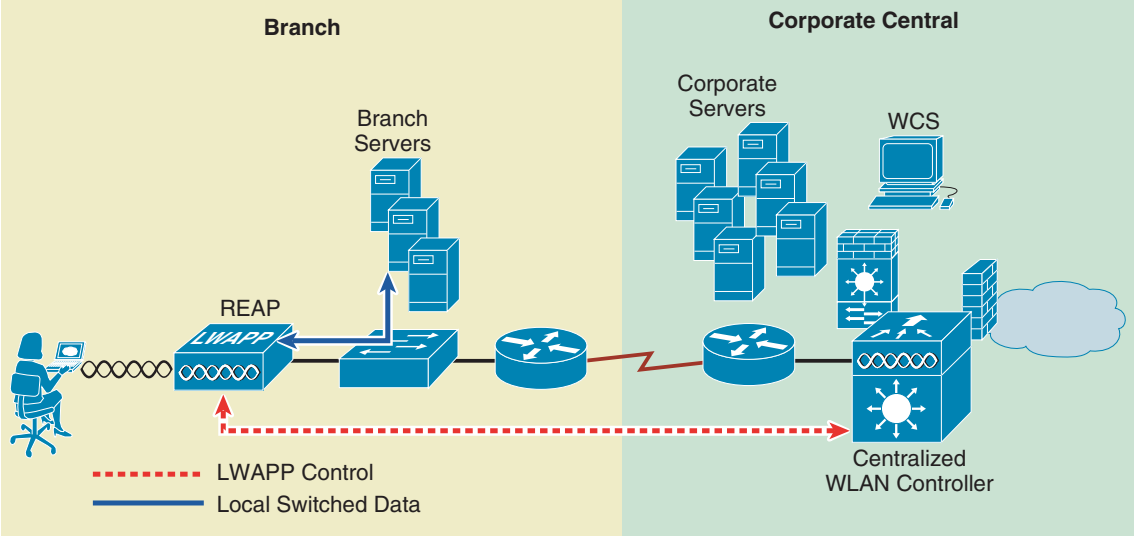
Remote Edge AP

Remote edge APs (REAPs) are special purpose LWAPP-based APs that are designed to be deployed in remote (branch) locations where:

- Wireless users at a branch or remote location require access to local network resources, and/or local wireless connectivity needs to be preserved during WAN link outages.
- Limited WAN bandwidth exists between the central site and a remote location where local connectivity is required. In this scenario, it would be impractical to tunnel all wireless user traffic to a centralized WLC, only to be routed back (in standard IP packets) across a bandwidth-constrained WAN link to the remote site.
- Only a few APs are needed to provide adequate wireless coverage for a given location. This is often more cost-effective than deploying and managing WLCs at every location, especially if there are large numbers of small remote sites requiring wireless coverage.

REAP APs are designed to address these remote branch needs by decoupling the LWAPP control plane from the WLAN data plane. This allows WLANs to be terminated locally on a Layer 2 switch while LWAPP control and management data is sent back to a centralized WLC. In this way, the benefits of a centralized architecture are preserved. Figure 7-1 provides a high level REAP topology diagram.

Figure 7-1 High Level REAP Topology



The Cisco REAP AP, the 1030, is capable of supporting up to 16 WLANs. Although all WLANs can be locally switched, the 1030 (when configured for REAP operation) has the following limitations compared to an LWAPP AP that is deployed in a regular centralized topology:

- It does not support 802.1Q trunking. All WLANs terminate on a single local VLAN/subnet.
- In the event of a WAN link outage, all WLANs except WLAN 1 become disabled and are no longer broadcasted (if enabled).

Cisco addressed these limitations with the introduction of a new version of REAP called Hybrid Remote Edge AP (H-REAP), which offers the ability to map WLANs to VLANs via 802.1Q trunking. Additionally, an H-REAP AP can support local switched and centrally switched WLANs concurrently. The remainder of this chapter focuses on application, features, limitations, and configuration of the H-REAP APs and, when applicable, highlights the differences between H-REAP and the older 1030 REAP platform.

Hybrid REAP

Supported Platforms

WLAN WLCs

H-REAP APs are supported by the following WLAN WLC platforms with version 4.0 and later software images:

- Cisco 2100 Series
- Cisco 4400 Series
- Cisco 6500 Series WiSM
- Cisco WLAN WLC modules for Integrated Service routers (ISR)
- Cisco Catalyst C3750G-24WS

Access Points

The following LWAPP-capable APs support H-REAP functionality:

- Cisco 1131 Series
- Cisco 1242 Series

See APs, page 2-10 for additional information on Cisco 1130 and 1240 series APs.

H-REAP functionality is not supported on Cisco 1000 Series LWAPP APs. However, basic REAP functionality is still supported on the 1030.

H-REAP Terminology

This section provides a summary of H-REAP terminology and definitions.

Switching Modes

Unlike the 1030 Series REAP AP, which can map wireless user traffic to only a single VLAN, H-REAP APs are capable of supporting the following switching modes concurrently, on a per-WLAN basis:

- Local Switched—Local switched WLANs map wireless user traffic to discrete VLANs via 802.1Q trunking, either to an adjacent router or switch. If so desired, one or more WLANs can be mapped to the same local 802.1Q VLAN.

  A branch user who is associated to a local switched WLAN has their traffic forwarded by the on-site router. Traffic destined off-site (to the central site) is forwarded as standard IP packets by the branch router.

  All AP control/management-related traffic is sent to the centralized WLC separately via LWAPP.

- Central Switched—Central switched WLANs tunnel both the wireless user traffic and all control traffic via LWAPP to the centralized WLC where the user traffic is mapped to a dynamic interface/VLAN on the WLC. This represents the normal LWAPP mode of operation.

  The traffic of a branch user who is associated to a central switched WLAN will be tunneled directly to the centralized WLC. If that user needs to communicate with computing resources within the branch (where that client is associated), their data is forwarded as standard IP packets back across the WAN link to the branch location. Depending on the WAN link bandwidth, this might not be desirable behavior.

Operation Modes

There are the following two modes of operation for an H-REAP AP:

- Connected mode—The WLC is reachable. In this mode the H-REAP AP has LWAPP connectivity with its WLC.
- Standalone mode—The WLC is unreachable. The H-REAP has lost or failed to establish LWAPP connectivity with its WLC; for example, when there is a WAN link outage between a branch and its central site.

H-REAP States

An H-REAP WLAN, depending on its configuration and network connectivity, can be classified as being in one of the following states:

- Authentication-central/switch-central—This state represents a WLAN that uses a centralized authentication method such as 802.1x, VPN, or web. User traffic is sent to the WLC via LWAPP. This state is supported only when H-REAP is in Connected mode (see Figure 7-2). 802.1X is used in this example, but other mechanisms are equally applicable.
- Authentication down/switching down—Central switched WLANs (above) no longer beacon or respond to probe requests when the H-REAP is in standalone mode. Existing clients are disassociated.
- Authentication-central/switch-local—This state represents a WLAN that uses centralized authentication, but user traffic is switched locally. This state is supported only when H-REAP is in Connected mode (see Figure 7-3). 802.1X is used in this example, but other mechanisms are equally applicable.
- Authentication-down/switch-local—A WLAN that requires central authentication (see above) rejects new users. Existing authenticated users continue to be switched locally until session timeout (if configured). The WLAN continues to beacon and respond to probes until there are no more (existing) users associated to the WLAN. This state occurs as a result of the AP going into standalone mode. (see Figure 7-4).
- Authentication-local/switch-local—This state represents a WLAN that uses open, static WEP, shared, or WPA2 PSK security methods. User traffic is switched locally. These are the only security methods supported locally if an H-REAP goes into standalone mode. The WLAN continues to beacon and respond to probes (see Figure 7-5). Existing users remain connected and new user associations are accepted. If the AP is in connected mode, authentication information for these security types is forwarded to the WLC.

Figure 7-2 Authentication-Central/Switch-Central WLAN

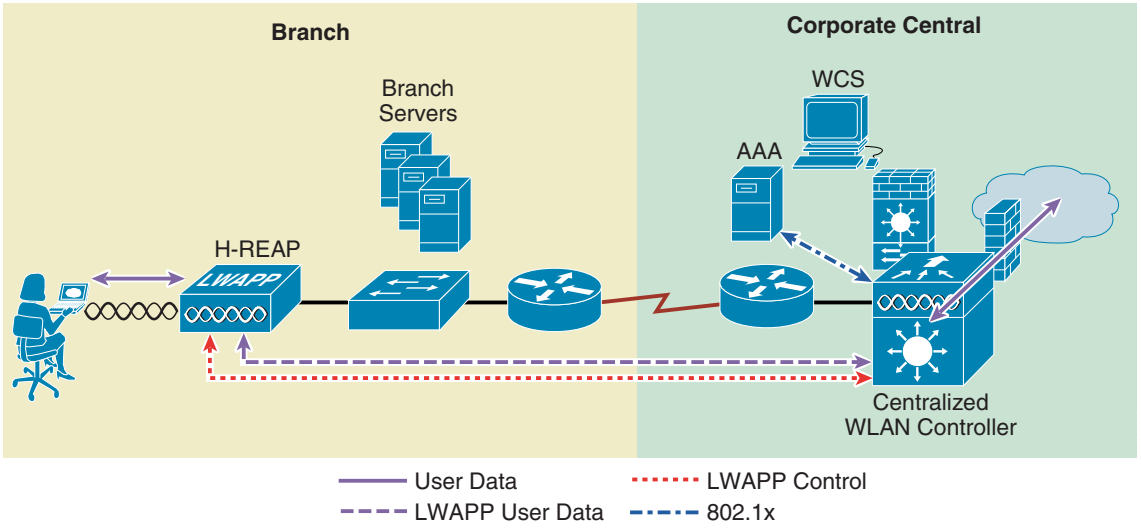


Figure 7-3 Authentication-Central/Switch-Local WLAN

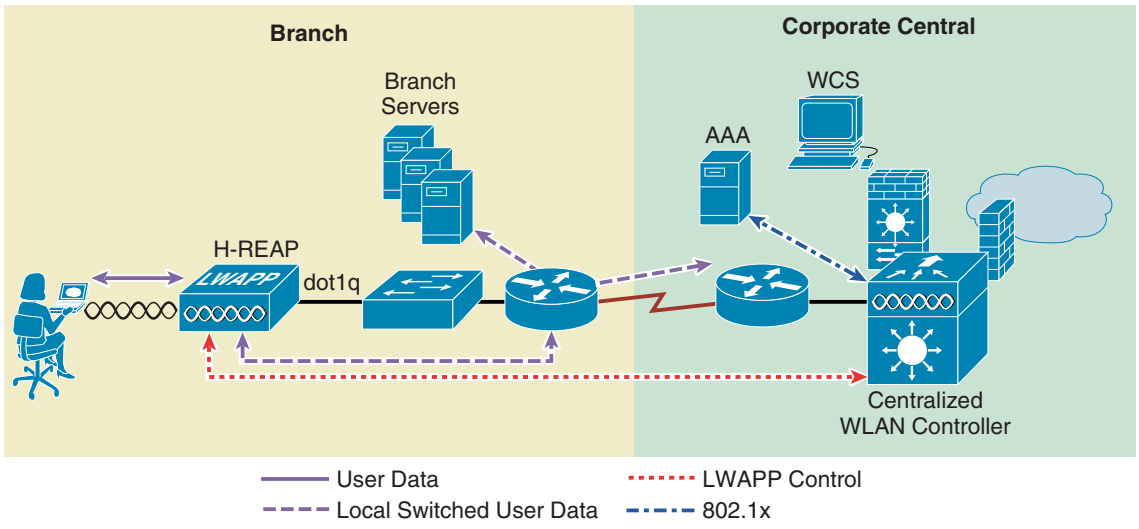


Figure 7-4 Authentication-Down/Local Switch

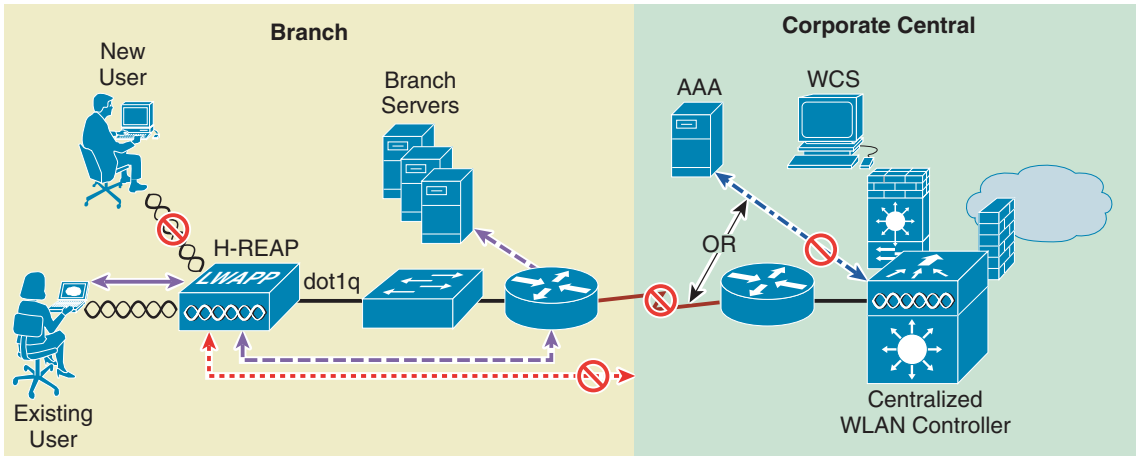
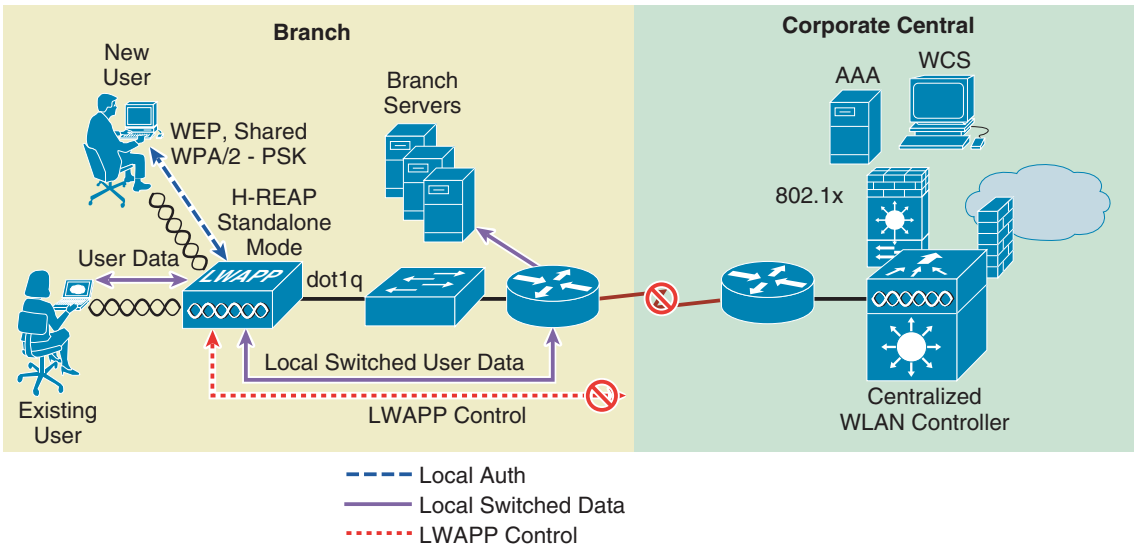


Figure 7-5 Authentication-Local/Switch-Local WLAN



Note All 802.11 authentication and association processing occurs at the H-REAP, regardless of which operational mode the AP is in. When in Connected mode, the H-REAP forwards all association/authentication information to the WLC. When in Standalone mode, the AP cannot notify the WLC of such events, which is why WLANs that make use of central authentication/switching methods are unavailable.

The hybrid-REAP access point maintains client connectivity for local switched WLANs after entering standalone mode. However, after the access point re-establishes a connection with the WLC, it disassociates all existing clients, applies updated configuration information from the WLC (if applicable), and re-allows client connectivity.

Applications

With its expanded capabilities, the H-REAP AP offers greater flexibility in how it can be deployed, such as:

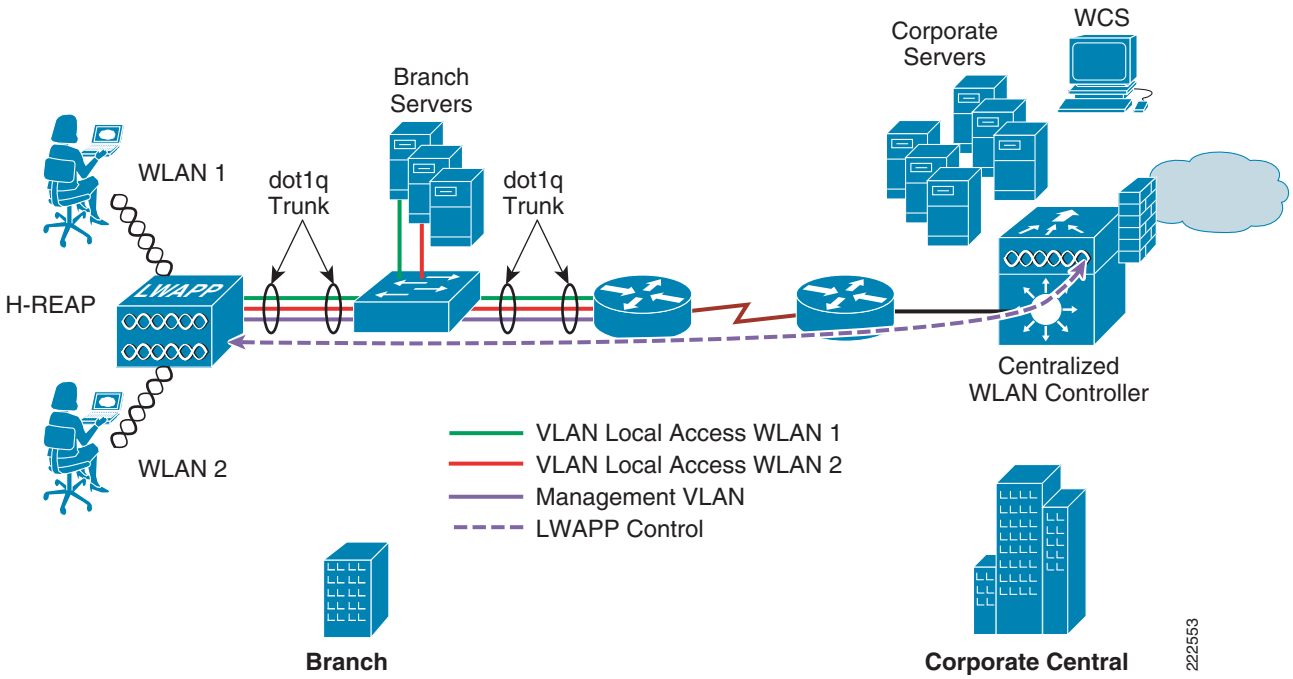
- Branch Wireless Connectivity
- Branch Guest Access
- Public WLAN Hotspot

Branch Wireless Connectivity

The primary goal of REAP and H-REAP is to address the wireless connectivity needs in branch locations, permitting wireless user traffic to be terminated locally rather than be tunneled across the WAN to a central WLC.

Because H-REAP can map individual WLANs to specific 802.1Q VLANs, branch locations can more effectively implement segmentation, access control, and QoS policies on a per-WLAN basis. See Figure 7-6.

Figure 7-6 H-REAP Typology



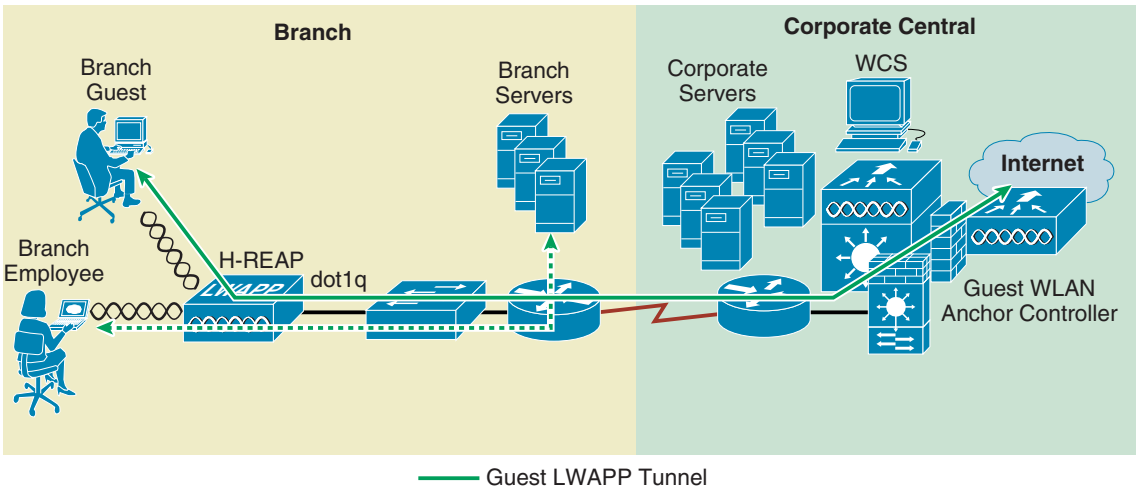
Branch Guest Access

One of the challenging aspects of using standard REAP APs in the branch is the implementation of guest access, which is difficult to implement for the following reasons:

- All WLANs map to the same local VLAN, thereby making it difficult to differentiate and segment guest users from branch users.
- All user traffic is switched locally; therefore, guest access traffic must somehow be segmented and routed back to the central site for access control and authentication, or if local Internet access is available at the branch, both segmentation and access control must be implemented locally.

The H-REAP AP helps overcome some of these challenges with the introduction of concurrent local and central switching. In an H-REAP topology, an SSID/WLAN designated for guest access can be tunneled via LWAPP to a central WLC where its corresponding interface/VLAN can be switched directly to an interface of an access control platform, such as Cisco SSG/ISG or Cisco NAC Appliance. Alternatively, the centralized WLC itself can perform web authentication for the guest access WLAN. In either case, the guest user's traffic is segmented (isolated) from other branch office traffic. Figure 7-7 provides an example of guest access topology using the H-REAP AP. For more information, see Chapter 10, "Cisco Unified Wireless Guest Access Services."

Figure 7-7 Branch Guest Access using H-REAP Central Switching



It is also possible to configure a (guest) WLAN, which uses central web authentication, to be switched locally at the branch. In this case, the branch client is redirected to the central WLC (virtual address 1.1.1.1) for web authentication only. Upon authenticating, all client traffic is subsequently switched via the local VLAN interface based on the HREAP settings. Any traffic associated with web login or logoff (destined to the WLC virtual address) is tunneled via LWAPP directly to the central WLC.

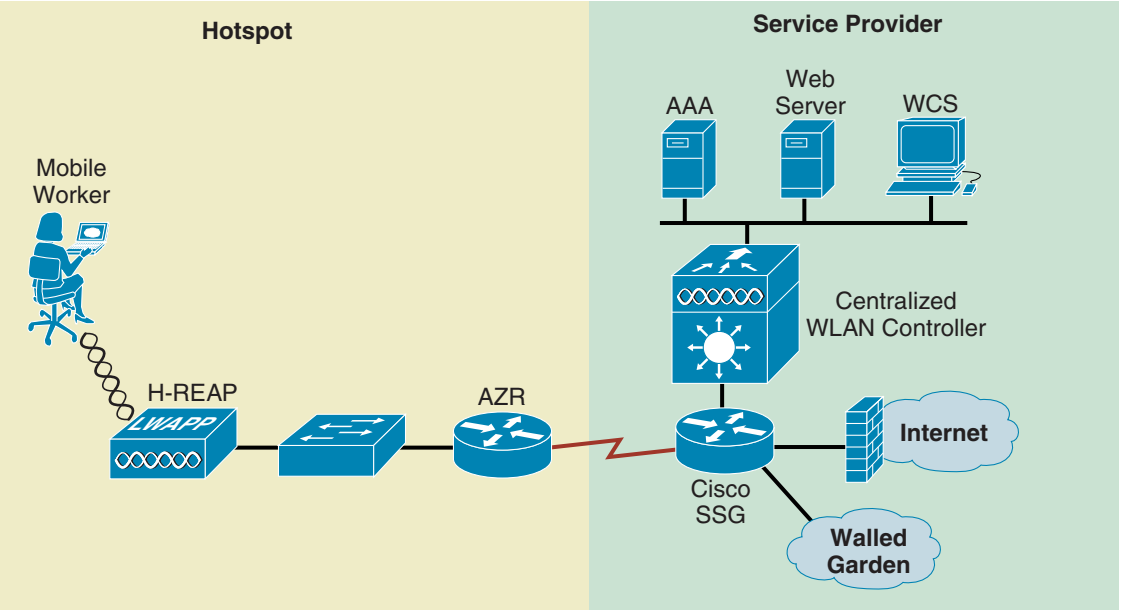
Public WLAN Hotspot

Many public hotspot service providers are beginning to implement multiple SSID/WLANs. One reason for this is because an operator might want to offer an open authentication WLAN for web-based access and another WLAN that uses 802.1x/EAP for more secure public access.

The H-REAP AP, with its ability to map WLANs to separate VLANs, is now an alternative to an standalone AP for small venue hotspot deployments where only one, or possibly two, APs are needed.

Figure 7-8 provides an example of hotspot topology using an H-REAP AP.

Figure 7-8 Hotspot Access using H-REAP Local Switching



Unified Wireless Feature Support

See Table 7-1 for a matrix of supported features and authentication types based on the H-REAP mode of operation.

Table 7-1 Supported Features and Authentication Types

Features	Connected Mode Central Switched	Connected Mode Local Switched	Standalone Mode	Notes
Authentication Open	Yes	Yes	Yes	
Authentication Shared	Yes	Yes	Yes	
Authentication WPA/2-802.1x	Yes	Yes	No	If the AP transitions to standalone mode, existing authenticated client sessions remain connected but no new authentications are possible. WLAN beacon/probe responses are supported until the last client disassociates if WLC connectivity is not restored.
Authentication WPA/2-PSK	Yes	Yes	Yes	If the AP transitions to standalone mode, existing authenticated clients remain connected, new client connections are permitted.
Authentication Guest Access (Web Auth)	Yes	Yes	No	
VPN	Yes	Yes	No	
L2TP	Yes	Yes	No	

Table 7-1 Supported Features and Authentication Types (continued)

NAC	Yes	Yes	No	
CCKM Fast Roaming	No	No	No	
PKC Fast Roaming	No	No	No	
CAC and TSPEC	Yes	Yes	No	
Client load balancing	No	No	No	
Peer-to-peer blocking	Yes	No	No	
WIDS	Yes	Yes	No	
RLDP	Yes	Yes	No	
RADIUS/TACACS authentication	Yes	Yes	No	
Radius/TACACS accounting	Yes	Yes	No	

Deployment Considerations

The following section covers the various implementation and operational caveats associated with deploying H-REAP APs.

WAN Link

For the H-REAP AP to function predictably, keep in mind the following with respect to WAN link characteristics:

- Latency—A given WAN link should not impose latencies greater than 100 ms. The AP sends heartbeat messages to the WLC once every thirty seconds. If a heartbeat response is missed, the AP sends five successive heartbeats (one per second) to determine whether connectivity still exists. If connectivity is lost, the H-REAP AP switches to standalone mode (see Operation Modes, page 7-3 for operation mode definitions). The AP itself is relatively delay tolerant. However, at the client, timers associated with authentication are sensitive to link delay, and thus a constraint of ≤ 100 ms is required. Otherwise, the client can timeout waiting to authenticate, which can cause other unpredictable behaviors, such as looping.
- Bandwidth—WAN links should be at least 128 kbps for deployments where up to eight H-REAPs are being deployed at a given location. If more than eight H-REAPs are deployed, proportionally more bandwidth should be provisioned for the WAN link.
- Path MTU—WLC software Release 4.0 and later require an MTU no smaller than 500 bytes; this applies to both the 1030 REAP and H-REAP APs

Roaming

As stated earlier, when an H-REAP AP is in connected mode, all client probes, association requests, 802.1x authentication requests, and corresponding response messages are exchanged between the H-REAP and the WLC via the LWAPP control plane. This is true for open, static WEP, and WPA PSK-based WLANs even though LWAPP connectivity is not required to use these authentication methods when the AP is in standalone mode.

- Dynamic WEP/WPA—A client that roams between H-REAP APs using one of these key management methods performs full authentication each time it roams. After successful authentication, new keys are passed back to the AP and client. This behavior is no different than a standard centralized WLAN deployment, except that in an H-REAP topology, there can be link delay variations across the WAN, which can in turn impact total roam time. Depending on the WAN characteristics, RF design, backend authentication network, and authentication protocols being used, roam times may vary from 50 ms to 1500 ms.
- WPA2—To improve client roam times, WPA2 introduced key caching capabilities, based on the IEEE 802.11i specification. Cisco created an extension to this specification called Proactive Key Caching (PKC). PKC today is supported only by the Microsoft Zero Config Wireless supplicant and the Funk (Juniper) Odyssey client. Cisco's CCKM is also compatible with WPA2.

  H-REAP does not support PKC, regardless of whether a WLAN is centrally or locally switched. As such, PKC-capable clients that roam between H-REAP APs undergo full 802.1x authentication. Remote branch locations requiring predictable, fast roaming behavior in support of applications such as wireless IP telephony should consider deploying a local WLC (Cisco WLC2100 or NM-WLC for Integrated Service routers).
- Cisco Centralized Key Management (CCKM)—CCKM is a Cisco-developed protocol in which the WLC caches the security credentials of CCKM-capable clients and forwards those credentials to other APs within a mobility group. When a client roams and associates with another AP, their credentials are forwarded to that AP, which allows the client to re-associate and authenticate in a two-step process. This eliminates the need for full authentication back to the AAA server. H-REAP APs currently do not support CCKM fast roaming. Therefore, CCKM-capable clients undergo full 802.1x authentication each time they roam from one H-REAP to another.
- Layer 2 switch CAM table updates—When a client roams from one AP to another on a locally switched WLAN, the H-REAP currently does not announce to a Layer 2 switch that the client has changed ports. The switch will not discover that the client has roamed until the client performs an ARP request for its default router. This behavior, while subtle, can have an impact on roaming performance.

Note A client that roams (for a given local switched WLAN) between HREAPs that map the WLAN to a different VLAN/subnet will renew their IP addresses to ensure that they have an appropriate address for the network to which they have roamed.

Radio Resource Management

While in connected mode, all Radio Resource Management (RRM) functionality is fundamentally available. However, because typical H-REAP deployments comprise a smaller number of APs, RRM functionality may not be operational at a branch location. For example, in order for transmit power control (TPC) to work, there must be a minimum of four H-REAPs in proximity to each other. Without TPC, other features such as coverage hole protection will be unavailable. For more information regarding Cisco Auto RF functionality, see Chapter 3, "WLAN Radio Frequency Design Considerations."

Location Services

As stated above, H-REAP deployments typically consist of only a handful of APs at a given location. Cisco maintains strict guidelines regarding the number and placement of APs to achieve the highest level of location accuracy. As such, although it is possible to obtain location information from H-REAP deployments, the level of accuracy can vary greatly across remote location deployments. Therefore, it is unlikely that the Cisco optimal location accuracy specification can be achieved in a typical H-REAP deployment unless Cisco's stated location design recommendations can be followed. For more information, see the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html.

QoS Considerations

For WLANs that are centrally switched, the H-REAP handles QoS is the same way as standard LAPs. Locally switched WLANs implement QoS differently.

For locally switched WLANs with WMM traffic, the AP marks the dot1p value within the dot1q VLAN tag for upstream traffic. This happens only for tagged VLANs, not the native VLAN.

For downstream traffic, the H-REAP uses the incoming dot1p tag from the locally switched Ethernet and uses this to queue and mark the WMM values associated with frames destined to a given user across the RF link.

The WLAN QoS profile is applied both for upstream and downstream packets. For downstream, if an 802.1p value that is higher than the default WLAN value is received, the default WLAN value is used. For upstream, if the client sends an WMM value that is higher than the default WLAN value, the default WLAN value is used. For non-WMM traffic, there is no CoS marking on the client frames from the AP.

For more information see Chapter 5, "Cisco Unified Wireless QoS."

Cisco strongly recommends that appropriate queuing/policing mechanisms be implemented across the WAN to ensure proper handling of traffic based on its DSCP setting. An appropriate priority queue should be reserved for LWAPP control traffic (which is marked DSCP CS6) to ensure that an H-REAP does not inadvertently cycle between connected and standalone modes because of congestion.

General WLC Deployment Considerations with H-REAP

Although it is possible for any WLC within the campus to support H-REAPs, depending on the number of branch locations and subsequently the total number of H-REAPs being deployed, it makes sense (from an administrative standpoint) to consider using a dedicated WLC(s) to support the H-REAP deployment.

H-REAPs typically do not share the same policies as the LAPs within a main campus; each branch location is essentially an RF and mobility domain unto itself. Even though a single WLC cannot be partitioned into multiple logical RF and mobility domains, a dedicated WLC allows branch-specific configuration and policies to be logically separate from the campus.

If deployed, a dedicated H-REAP WLC should be configured with a different mobility and RF network name than that of the main campus. All H-REAPs joined to the "dedicated" WLC become members of that RF and mobility domain.

From an auto-RF standpoint, assuming there are enough H-REAPs deployed within a given branch (see Radio Resource Management, page 7-11), the WLC attempts to auto manage the RF coverage associated with each branch.

There is no advantage (or disadvantage) by having the H-REAPs consolidated into their own mobility domain. This is because client traffic is switched locally. EoIP mobility tunnels are not invoked between WLCs (of the same mobility domain) where client roaming with H-REAPs is involved.

If a dedicated WLC is going to be used for an H-REAP deployment, a backup WLC should also be deployed to ensure network availability. As with standard LAP deployments, the WLC priority should be set on the H-REAPs to force association with the designated WLCs.

WAN Link Disruptions

As described in sections Operation Modes, page 7-3 through H-REAP States, page 7-4, certain H-REAP modes and functionality require LWAPP control plane connectivity to the WLC. Following is a summary of the features and functions that are impacted when the H-REAP is in Standalone mode.

EAP 802.1x and Web Auth WLANs

Existing local switched clients remain connected until the client roams or session re-authentication. No new client authentications are permitted.

Existing central switched clients are disconnected; no new client authentications are permitted.

As mentioned in H-REAP States, page 7-4, open, static WEP, and WPA/2-PSK configured WLANs can function in either Connected or Standalone modes and therefore are not impacted in the same way as WLANs requiring RADIUS services, such 802.1x or web authentication. If there is a requirement for a remote branch location to maintain wireless connectivity during WAN link disruptions, Cisco recommends that a backup WLAN be implemented based on one of the three Layer 2 security polices above. Of these, WPA2-PSK offers the strongest security and therefore is strongly recommended.

Other Features

The following features are unavailable when an H-REAP is in standalone mode:

- Radio resource management except for DFS support, which is controlled locally at the H-REAP
- Wireless intrusion detection
- Location-based services
- NAC
- Rogue detection
- AAA override

Radio Configuration

The following radio configuration information is maintained when an H-REAP is in standalone mode:

- DTIM
- Beacon period
- Short preamble
- Power level
- Country code
- Channel number
- Blacklist

H-REAP Limitations and Caveats

Local Switching Restrictions

If one of the following security methods is configured on the WLC for a specific WLAN, then that WLAN cannot be configured for local switching on an H-REAP AP:

- IPSEC
- CRANITE
- FORTRESS[1]

Note VPN pass-through to external aggregation platforms is permitted. However, WLC-imposed VPN passthrough restriction is not permitted.

Max Supported WLANs

H-REAP APs support eight WLANs. Therefore, any WLAN that is expected to be supported by an H-REAP AP must fall within WLAN IDs 1–8. WLAN IDs 9–16 are not propagated.

Network Address Translation (NAT/PAT)

WLC

A WLC cannot reside behind a NAT boundary when communicating with APs because LAPs communicate with the WLC in two phases using two different IP addresses:

- WLC discovery—A LAP initially queries a list of WLCs using the management IP address of a WLC. The management IPs are learned via DHCP Option 43, DNS, or they can be configured manually (see Initial Configuration, page 7-17). The discovery phase is used to determine which WLC, within the list of eligible WLCs, the AP will join. This is conveyed by sending an LWAPP control message containing the eligible WLC AP management IP address.
- WLC join—The AP joins the eligible WLC using the learned AP management IP address. The AP management IP address cannot be supported by NAT because the AP learns this address during the discovery phase. Even if 1:1 NAT relationships are established, the WLC is not capable of passing the outside NAT address of the AP manager as the IP address the AP should use to join the WLC.

AP

Standard 1:1 static NAT can be used to support one or more APs behind a NAT boundary. Also, multiple LAPs (H-REAP or standard) can use PAT. In this scenario, a single IP NAT pool is configured with “overload” or a WAN interface (or loopback I/F) is used with “overload”. Following is a summary of the behavior when the overload (PAT) method is used:

1. When an AP boots up, it obtains an “inside local” IP address from DHCP and then use a random source port (5xxxx) to initiate the WLC discovery process using LWAPP control port 12223. Cisco IOS PAT preserves the inside local source port number selected by the AP and makes a translation using the “NAT pool” IP address or interface IP address (inside global). See the following example:

```
Pro Inside global    Inside local       Outside local      Outside global
udp 10.20.3.19:54417 192.168.1.121:54417 10.15.9.253:12223  10.15.9.253:12223
```

2. After the AP has joined a WLC and 802.11 data is sent upstream, the IOS PAT process sources the 802.11 data traffic using the same inside local port number and sends it to the WLC using LWAPP port 12222. See the following example:

```
Pro Inside global       Inside local        Outside local      Outside global
udp 10.20.3.19:54417   192.168.1.121:54417 10.15.9.253:12222 10.15.9.253:12222
```

3. All traffic sent from the WLC to the AP, regardless of whether it is control or 802.11 data, is sent to the inside global IP address and port number 54417 (assuming the example above), where IOS PAT translates it to the proper inside local address. Multiple APs can be supported because each AP uses a unique source port to communicate with the WLC.

The PAT translation examples above occur when the AP boots up for the first time. However, often times the AP may reset a second and possibly a third time and if it does, it obtains a new IP address each time (assuming DHCP is used). This creates a problem for the PAT process because now the AP is attempting to use the same inside local source port number, but with a different inside local IP address. Because the first translation entries still exist, PAT creates new (unique) inside global source ports. See the following example:

```
Pro Inside global       Inside local        Outside local      Outside global
udp 10.20.3.19:54417   192.168.1.121:54417 10.15.9.253:12222 10.15.9.253:12222
udp 10.20.3.19:54417   192.168.1.121:54417 10.15.9.253:12223 10.15.9.253:12223
udp 10.20.3.19:1322    192.168.1.122:54417 10.15.9.253:12222 10.15.9.253:12222
udp 10.20.3.19:1323    192.168.1.122:54417 10.15.9.253:12223 10.15.9.253:12223
```

In the example above, note the translations that PAT creates after the AP resets the second time. The first translation entries for inside local 192.168.1.121 are no longer used because the AP has reset with a new IP. In this scenario, the AP is now communicating with the WLC using inside local IP 192.168.1.122 and source port 1323, which works. The problem arises when 802.11 data is sent to the WLC. In the example above, instead of being sourced by the same inside global port (1323) as the LWAPP control data, PAT sources the 802.11 data using yet another port: 1322. The WLC receives the 802.11 data, but it sends all 802.11 data back to the AP using 1323. Because of the port mismatch, the AP does not receive the 802.11 data, effectively breaking the LWAPP data plane.

Note This is a problem only for centrally switched WLANs. Those WLANs that are switched locally are not impacted because no 802.11 data is being sent to the WLC on port 12222 for those WLANs.

Workarounds are as follows:

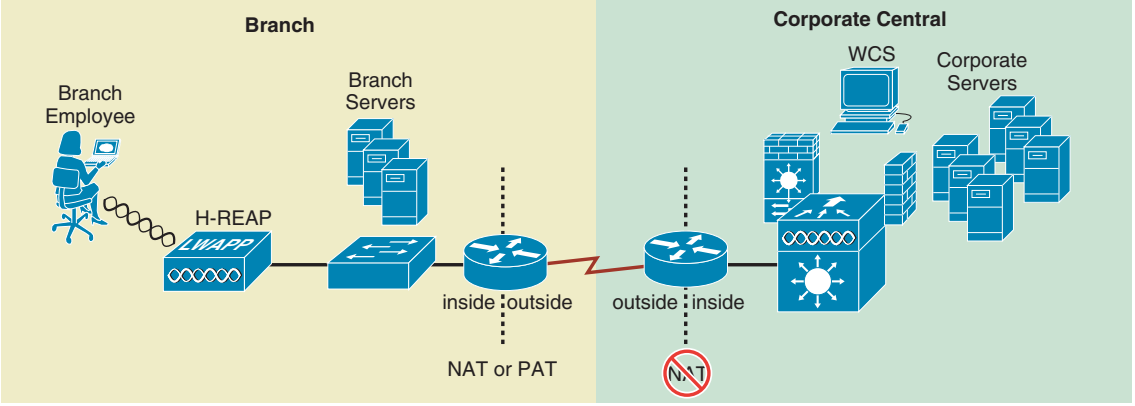
- If dynamic DHCP is used, establish more aggressive NAT translation entry timeouts for UDP ports 12222 and 12223. Set the translation timeout for these ports between 20 and 25 seconds. With anything less than 20 seconds, there is a risk that the APs will lose association with the WLC. If set too long, the stale entries may not timeout quick enough and the AP will continue to use the undesired ports. See the following configuration example:

```
ip nat translation port-timeout udp 12222 20
ip nat translation port-timeout udp 12223 20
```

- Create static DHCP reservations for each AP. If the AP undergoes sequential resets, it continues to use the same IP, so PAT does not create secondary or tertiary source port bindings. This option is practical only if DHCP is implemented locally at the remote/branch location.
- Manually assign IP addresses to those APs subject to PAT. See H-REAP Configuration, page 7-17 for IP configuration options. Again, if the AP undergoes sequential resets, it continues to use the same IP, and PAT does not create secondary or tertiary source port bindings.

Figure 7-9 shows H-REAP with NAT/PAT.

Figure 7-9 H-REAP with NAT/PAT



RADIUS Assigned VLANs

RADIUS-based VLAN assignment is supported for those H-REAP WLANs that are central-switched. This feature is not available when the H-REAP is in Standalone mode.

Web Authentication (Guest Access)

WLC-based web authentication may be used with local switched WLANs so long as the H-REAP is in Connected mode. Otherwise, those WLANs using web authentication are unavailable when the H-REAP is in Standalone mode.

Restricting Inter-Client Communication

Two or more clients, associated to a WLAN that is locally switched (by an H-REAP), are not prevented from communicating with one another even if Peer-to-Peer Blocking mode is enabled on the WLC. This is because locally switched wireless traffic does not go through the WLC.

Those H-REAP WLANs that are central switched have inter-client communication restricted based on the Peer-to-Peer Blocking mode setting on the WLC.

H-REAP Scaling

- Per-Site—There is no limit to the number of H-REAPs that may be deployed per remote location. However, keep in mind that deployment of a local WLC is strongly recommended if:
  - A remote location is planning to deploy VoWLAN. As described in Roaming, page 7-11, roaming performance can be impacted by the availability and link characteristics of the WAN backhaul. This is true even when key caching methods, such as 802.11i or Cisco CCKM, are employed because they are not currently supported with H-REAP.
  - WAN reliability/performance—Branch WLAN topologies that depend on authentication, radio resource management, and other upstream services are only as good as the availability of the WAN backhaul. Roundtrip delays must limited to no more than 100 ms and proper QoS queuing mechanisms must be available to manage congestion.
- Per-WLC—There are no restrictions with regard to the number of APs that can operate in H-REAP mode. The total number of H-REAP APs per WLC is bound only by the maximum number of LAPs that are supported for a given WLC model.

Inline Power

The Cisco 1130 and 1240 Series APs support both the Cisco inline power specification and conform to the 802.3af standard, whereas the former Cisco 1030 Series REAP APs support 802.3af only.

Management

H-REAP APs can be managed and monitored either through the WLC GUI or Cisco Wireless Control System (WCS) in the same way that regular LWAPP APs are managed. The only exception is when the H-REAPs become un-reachable because of WAN outages. For more information on management and WCS, refer to the following URLs:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html

http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

H-REAP Configuration

Initial Configuration

An eligible Cisco 1130 or 1240 series AP requires the following minimum information to join a WLC so that it can be configured for H-REAP operation:

- An IP address
- A default gateway address
- Management interface IP address of one or more WLCs

The above information can be obtained in one of four ways:

- Static configuration via serial console port
- DHCP with statically configured WLC addresses
- DHCP with Option 43, as discussed in Chapter 2, “Cisco Unified Wireless Technology and Architecture.”
- DHCP with DNS resolution for WLC addresses, as discussed in Chapter 2, “Cisco Unified Wireless Technology and Architecture.”

Serial Console Port

Unlike the earlier 1030 series REAPs, The 1130 and 1240 series APs offer a serial console port that can be used to establish basic parameters for connectivity. Use the following steps to establish initial configuration using the console port method. The serial console port method can be used only when the AP is not actively joined with a WLC and is running LWAPP image 12.3(11)JX or later.

Note Complete Step 4 a.through d. only if DHCP will not be used at the branch to assign an IP address to the H-REAP AP. Care must be taken to ensure that the addresses used conform to the addressing scheme being used at a given branch location.

Note The following serial console procedure can be performed only for new LAPs being deployed "out of the box" for the first time. The following procedure cannot be used on any LAP that has previously joined/communicated with a WLC.

Step 1 Using a standard Cisco DB9/RJ45 console cable connect the AP to a laptop running Hyper Terminal or other compatible terminal communications software. As with all Cisco devices, the serial parameters need to be set at 9600bps, 8 data bits, 1 stop bit and No flow control.

Step 2 Power on the AP. To configure the AP through the console port, it should not be connected to the network. Otherwise, if the AP discovers a WLC and joins it, you will not be able to run the configurations below. Therefore, the AP must remain disconnected from the network until the initial configuration has been completed.

Step 3 After the AP has completed loading its local image, establish an exec session by typing **enable** and then entering **Cisco** for the enable password.

Step 4 At the <ap-mac-address># prompt, use the following commands to configure the IP, mask, gateway, hostname, and the primary WLC:

a. **lwapp ap ip address** *ip-addr subnet-mask*

b. **lwapp ap ip default-gateway** *ip-addr*

c. **lwapp ap hostname** *ap-hostname* (optional)

d. **lwapp ap controller ip address** *ip-addr*

Note If DHCP is going to be used (see DHCP with Statically Configured WLC IPs, page 7-19) and you do not want to use DHCP Option 43 or DNS methods to define WLC management IP addresses, enter only the **lwapp ap controller ip address** *ip-addr* command from Step 4.

The preceding commands are saved directly to NVRAM.

Step 5 To review the static configuration, type the following command:

show lwapp ip config

Output similar to the following is displayed:

```
AP0014.1ced.494e# sho lwapp ip config
LWAPP Static IP Configuration
IP Address         10.20.104.50
IP netmask         255.255.255.0
Default Gateway    10.20.104.1
Primary Controller 10.20.30.41

AP0014.1ced.494e#
```

If an error has been made, repeat the commands listed in Step 4 to correct.

Step 6 To clear one or more static entries, use the following commands:

a. **clear lwapp ap ip address**

b. **clear lwapp ap ip default-gateway**

c. **clear lwapp ap controller ip address**

d. **clear lwapp ap hostname**

Once connected to the branch network, the AP boots and sends discovery requests to each WLC defined in Step 4 d. The AP then joins the least used WLC.

Note If the AP being configured has previously joined (associated) with a WLC for any reason, the above commands are rejected and the following error is seen: "ERROR!!! Command is disabled." Once the AP has joined a WLC, the above commands can no longer be used. This is by design, for security reasons. If a previously connected LAP requires static IP parameters to be configured, those parameters must be established from the GUI or command line interface of the WLC.

DHCP with Statically Configured WLC IPs

This method uses DHCP to dynamically configure the AP with an IP address and default gateway. The DHCP service can be implemented locally or remotely using an external server or locally using DHCP services resident within IOS. The WLC management interface IP addresses can be manually configured using the APs console interface; this can either be done before shipping to the branch office or on site. See Serial Console Port, page 7-17. After connecting to the branch network, the AP boots and sends discovery requests to each WLC defined. The AP then joins the least used WLC.

Note The option above can be performed only for new LAPs being deployed "out of the box" for the first time. This option cannot be used on any LAP that has previously joined/communicated with a WLC.

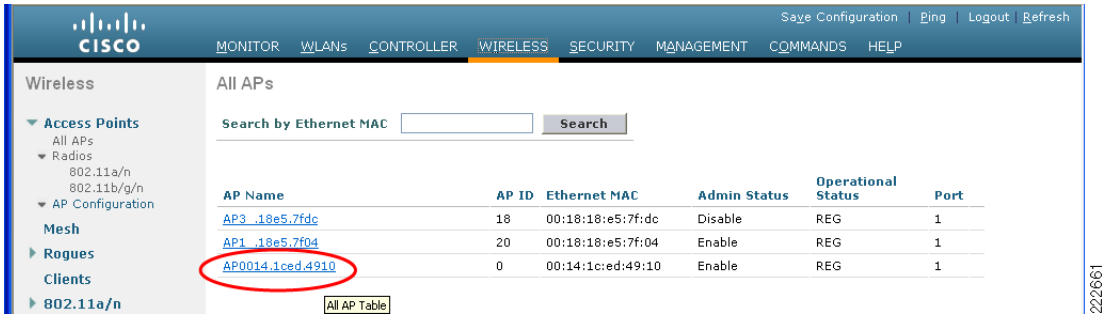
Configuring LAP for H-REAP Operation

The following configuration tasks are accomplished using the WLC GUI interface.

When an H-REAP-capable LAP joins the WLC for the first time it defaults to local AP mode. The LAP must be set for H-REAP mode before local switching parameters can be established.

Step 1 From the WLC Wireless configuration tab, locate the newly joined LAP and click on its name under AP Name. (See Figure 7-10):

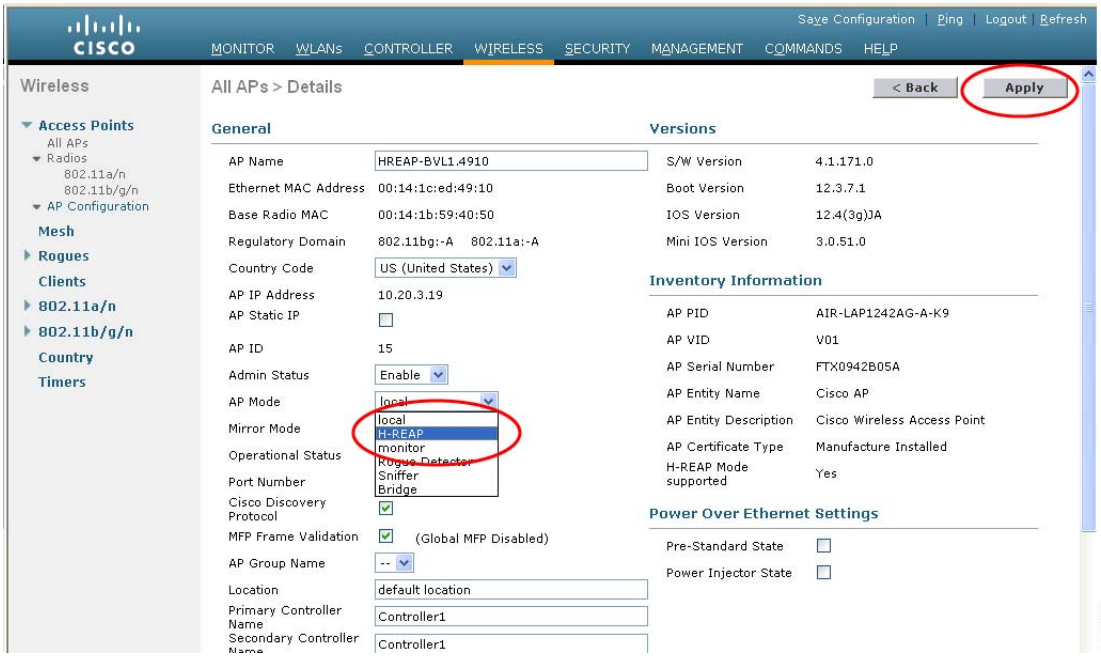
Figure 7-10 Wireless Configuration Tab



Step 2 Define AP Mode.

From the AP Mode drop-down list, choose **H-REAP**. (See Figure 7-11.)

Figure 7-11 Wireless Configuration—AP Mode



Step 3 Configure an AP name and optionally configure a location name.

Step 4 Identify the primary WLC the AP should join and, optionally, a secondary and tertiary WLC in the event the primary (or secondary) WLC becomes unreachable.

These names are case-sensitive and correspond to the system name. If none of the named WLCs are available, the AP will join one of the other WLCs that belong to the mobility group based on automatic load balancing.

Step 5 Click **Apply**.

The AP reboots and re-joins the WLC in H-REAP mode.

Note When the H-REAP AP reboots, its interface is not yet configured for 802.1q trunking mode. Therefore, you must ensure that the DHCP scope used for assigning addresses to H-REAP APs is configured for the native VLAN because the AP originates DHCP requests with no VLAN tag.

Enabling VLAN Support

After the H-REAP AP has re-joined the WLC in H-REAP mode:

Step 1 Find the AP under the WLC Wireless settings and click on the AP Name.

Note that there are new H-REAP configuration settings presented in the AP details window. (See Figure 7-12.)

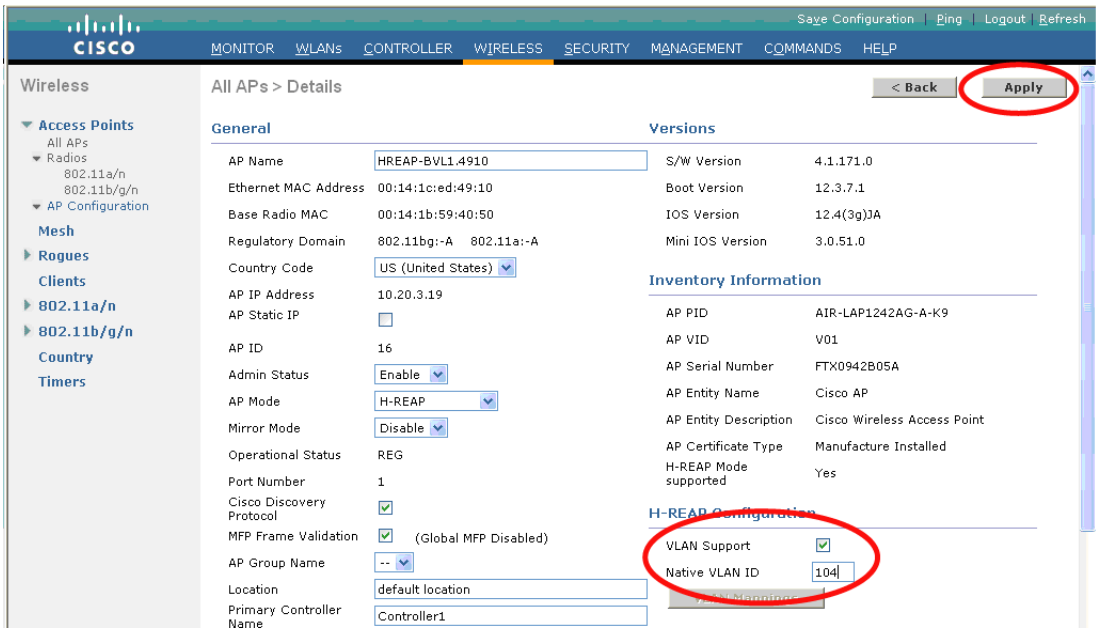
Step 2 Place a check mark in the **VLAN Support** check box.

Note that a Native VLAN ID definition window and a VLAN Mappings button are added.

Step 3 Enter the VLAN number defined as the native VLAN.

Step 4 Click **Apply**.

Figure 7-12 Wireless Settings



Advanced Configuration

The following steps outline how to configure an H-REAP AP to perform local and or central switching in addition to highlighting any caveats associated with the configuration process.

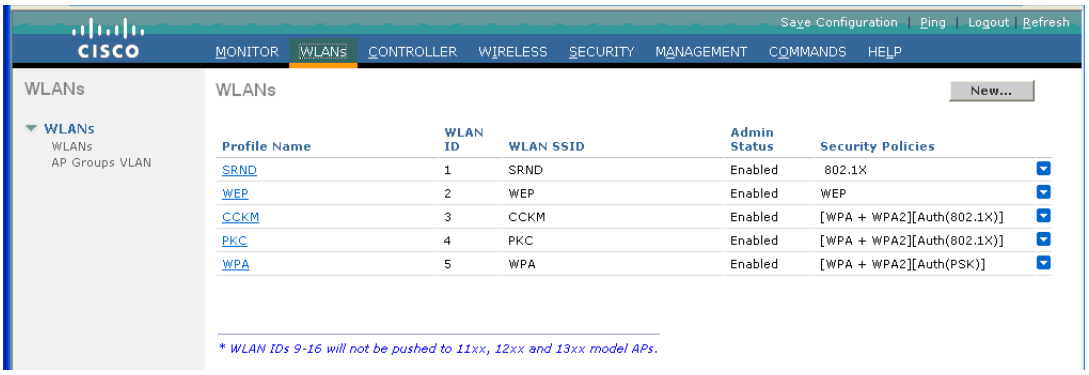
Choosing WLANs for Local Switching

Before a WLAN can be mapped to a local VLAN on the H-REAP AP, the WLAN must first be made eligible for H-REAP local switching.

Step 1 From the WLC web GUI, click the **WLANs** tab.

Step 2 Find the WLAN(s) that need to be locally switched and click on its Profile Name. (See Figure 7-13.)

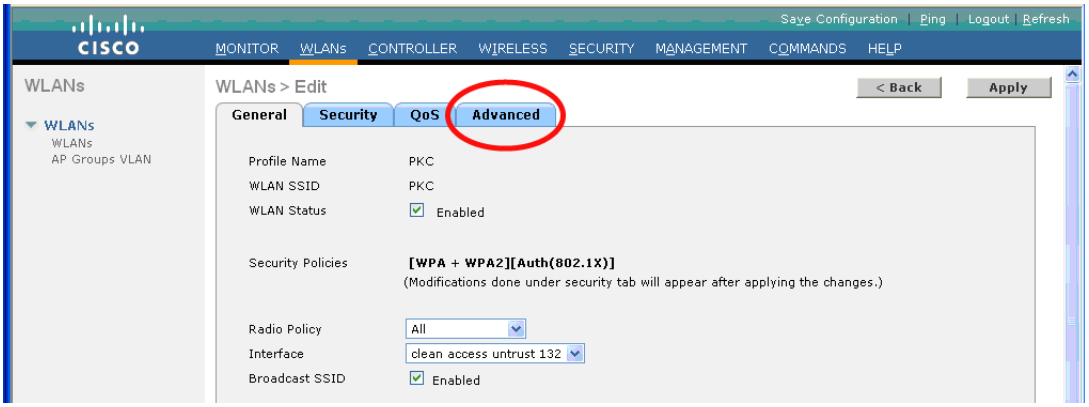
Figure 7-13 WLANs Tab



Configuring H-REAP Support on a WLAN

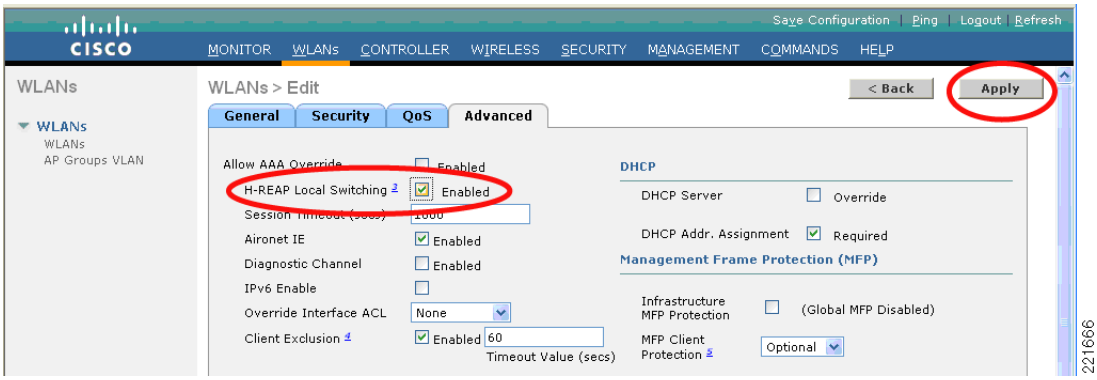
Step 3 From the WLANs edit page, click on the **Advanced** tab. (See Figure 7-14.)

Figure 7-14 WLANs—Edit



Step 4 Within the Advanced configuration window, click the box next to H-REAP Local Switching. (See Figure 7-15.)

Figure 7-15 Enabling H-REAP Local Switching



Step 5 Click **Apply**.

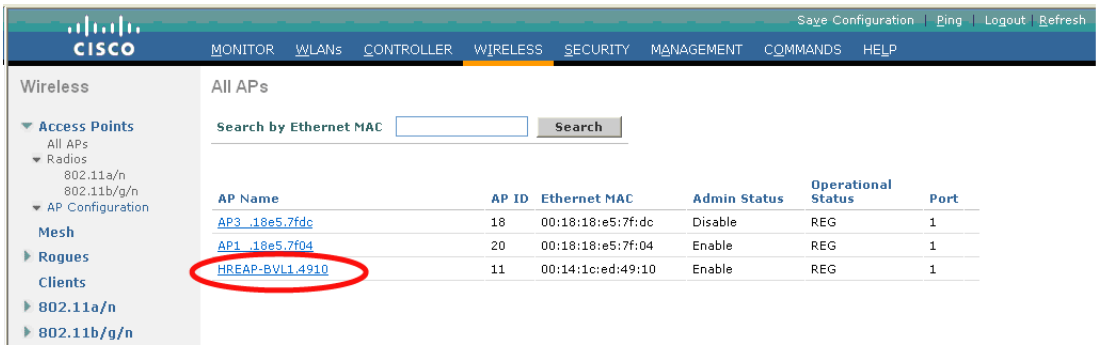
H-REAP Local Switching (VLAN) Configuration

After the WLANs is configured to support H-REAP, perform the following procedure.

Step 1 Click the **Wireless** tab.

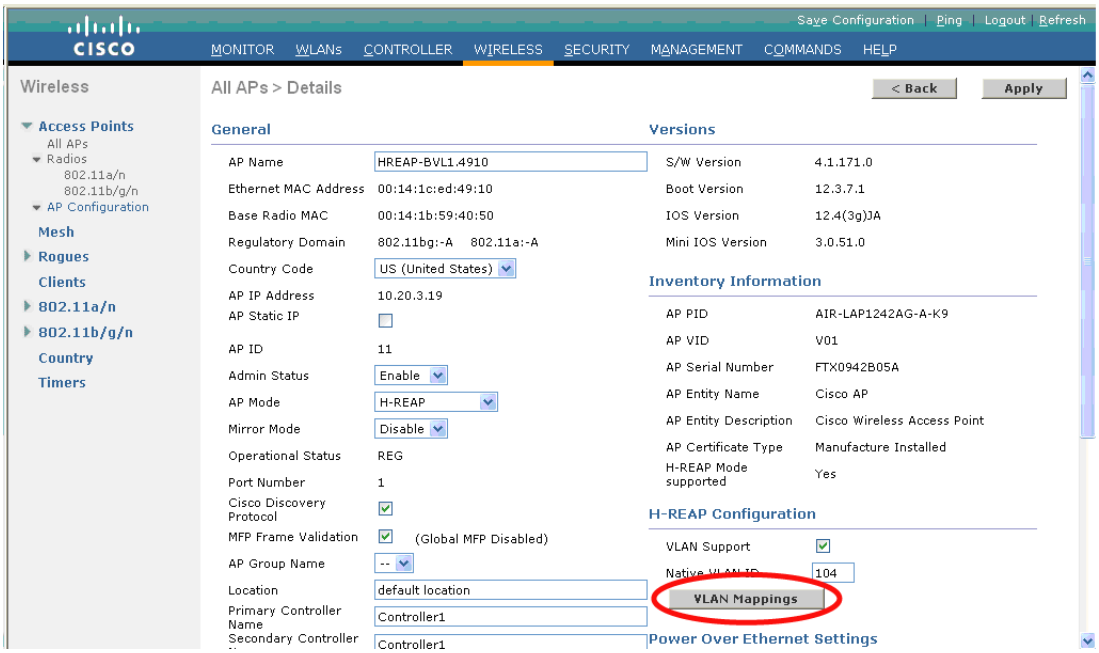
Step 2 From the list of APs, find the H-REAP and click the AP Name. (See Figure 7-16.)

Figure 7-16 Wireless Tab—APs



Step 3 From the AP Details configuration page, click **VLAN Mappings**. (See Figure 7-17.)

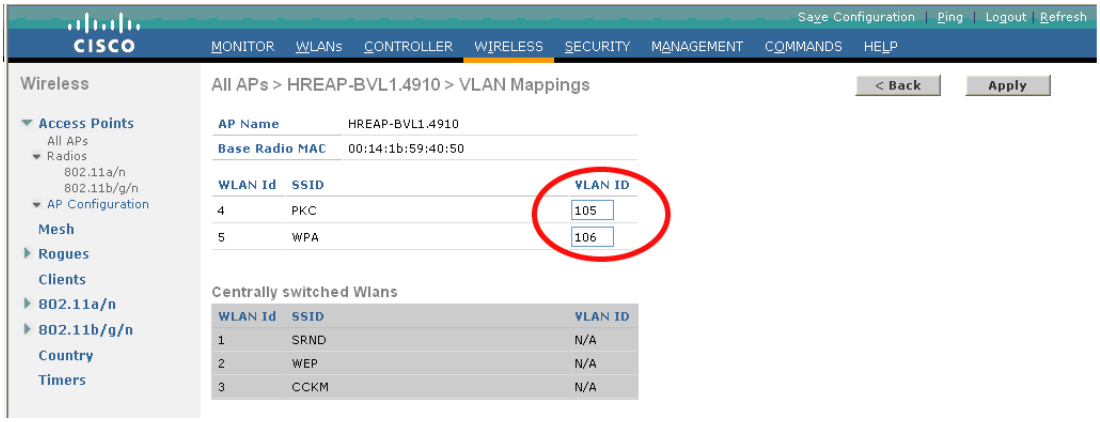
Figure 7-17 All APs—Details



Establishing a WLAN to Local VLAN Mapping

The VLAN Mappings page displays all WLANs that have been configured for H-REAP local switching, along with a configurable VLAN ID field. (See Figure 7-18.)

Figure 7-18 VLAN Mappings



Note The VLAN IDs that are displayed initially are inherited from the central WLC WLAN interface settings.

Step 1 For each WLAN/SSID, configure a locally relevant VLAN ID.

More than one WLAN can be mapped to the same local VLAN ID.

Step 2 Click **Apply**.

Note All WLANs shown in the grey box are centrally switched and may or may not be active, depending on whether the WLAN is administratively enabled at the WLC. All user traffic associated with a centrally switched WLAN is tunneled back to the WLC.

Centrally switched WLANs can be excluded from the H-REAP by using the WLAN override feature to hide any WLANs that are not required.

Note For each locally switched WLAN, there must be a DHCP helper address or local DHCP pool configured for its associated VLAN.

WLC Dynamic Interface Configuration for Remote Only WLANs

The sample configurations above assume that a given WLAN is being used at both the main campus and one or more remote site locations. However, there may be instances where a WLAN needs to be defined exclusively for use by one or more remote sites, where only H-REAP local switching is used.

In this scenario, a WLAN is created on the WLC that must be mapped to a local dynamic interface, even though the WLAN will not be used at the main campus. The default behavior of the WLC is to map a newly created WLAN to the management interface. Even though the (remote) WLAN will be switched

locally at each site, precautions should be taken at the WLC to map the WLAN to a “dummy” interface/VLAN. The WLAN should not be left mapped to the WLC management interface. This is to prevent wireless client traffic from inadvertently accessing the management subnet due to misconfiguration.

The quickest way to mitigate against this vulnerability is to create a dynamic interface on the WLC that maps to an isolated VLAN where no DHCP services or logical connectivity exists with the rest of the Enterprise network. This VLAN could even map to a NAC appliance or firewall as an added precaution.

H-REAP Verification

Verifying the H-REAP AP Addressing

- If using DHCP to assign an address, verify DHCP server configuration settings, correct subnet, mask, and default gateway.
- Ensure AP DHCP scope is defined for the native VLAN.
- If AP was configured with a static addresses, ensure AP address, subnet, mask and gateway are consistent with addressing scheme used within the branch location using the **show lwapp ip config** command. See Serial Console Port, page 7-17 for more information.

Verifying the WLC Resolution Configuration

- If using DHCP Option 43 for WLC resolution, verify that the VCI and VSA string format on the DHCP server is correct.
- Verify that the correct WLC management IP address is configured in the DHCP server.
- If using DNS resolution, verify that a DNS query of CISCO-LWAPP-CONTROLLER@localdomain can be made from the branch location and resolves to one or more valid WLC management IP address.
- Verify valid DNS server addresses are being assigned via DHCP
- If the WLC IP was configured manually, verify the configuration via the serial console port with the AP disconnected from the network using the **show lwapp ip config** command. See Serial Console Port, page 7-17 for more information.

Troubleshooting

This section provides troubleshooting guidelines for some common problems.

H-REAP Does Not Join the WLC

If an H-REAP AP is not joining the expected WLC:

- Verify routing from the branch location to the centralized WLC. Check that you can ping the WLC management IP address from the AP subnet.
- Verify that the LWAPP protocol (UDP ports 12222 and 12223) is not being blocked by an ACL or firewall
- Verify that the H-REAP hasn't joined another WLC in the mobility group

Check to see whether a WLC within the mobility group has been designated as “master controller”, which could cause an H-REAP to join a WLC other than the one expected.

Client Associated to Local Switched WLAN Cannot Obtain an IP Address

- Verify that 802.1q trunking is enabled (and matches the AP configuration) on the switch and or router ports to which the AP is connected.
- Verify that an IP helper address or local DHCP pool has been configured for the VLAN (sub-interface) at the first Layer 3 hop for the WLAN in question.

Client Cannot Authenticate or Associate to Locally Switched WLAN

If local switched WLAN uses central authentication:

- Verify H-REAP is not in Standalone mode (WAN backhaul down).
- Verify a valid RADIUS authentication server has been configured for the WLAN.
- Verify reachability to the RADIUS authentication server from the WLC.
- Verify that the RADIUS server is operational.
- Verify that the authentication service and user credentials are configured on the RADIUS server.

If the local switched WLAN uses a pre-shared key:

- Verify that the WPA or WEP configuration on the client matches that of the WLAN.
- Verify if wireless client requires WLAN SSID to be broadcast (if disabled) to authenticate/associate.

Client Cannot Authenticate or Associate to the Central Switched WLAN

If the central switch WLAN uses central authentication:

- Verify H-REAP is not in Standalone mode (WAN backhaul down)
- Verify a valid RADIUS authentication server has been configured for WLAN
- Verify reachability to RADIUS authentication server from the WLC
- Verify that the RADIUS server is operational.
- For AAA authenticated clients, verify that authentication service and user credentials are configured on the RADIUS server.

If local switched WLAN uses a pre-shared key:

- Verify that the WPA or WEP configuration on the client matches that of the WLAN.
- Verify if wireless client requires WLAN SSID to be broadcast (if disabled) to authenticate / associate.

H-REAP Debug Commands

This section contains debug commands that can be used for advanced troubleshooting.

WLC Debug Commands

The following commands are entered through, and their output can be viewed using, the WLC's serial console interface:

debug lwapp events enable

debug lwapp packets enable

H-REAP AP Debug Commands

The following commands are entered through, and their output can viewed using, the H-REAP serial console interface:

debug lwapp client packet

debug lwapp client mgmt

debug lwapp client config

debug lwapp client event

debug lwapp reap load

debug lwapp reap mgmt

CHAPTER 8

Cisco Wireless Mesh Networking

This chapter summarizes the design details for deploying a Cisco Wireless mesh network for outdoor environments. It focuses primarily on design considerations for mesh deployment, but also covers the solution components and interworkings. For further details about the Cisco Wireless Mesh solution, refer to the *Cisco Aironet 1500 Series Wireless Mesh AP Version 5.0 Design Guide* at: http://www.cisco.com/en/US/docs/wireless/technology/mesh/design/guide/MeshAP.html.

Introduction

The Cisco Wireless Mesh solution enables cost-effective and secure deployment of outdoor Wi-Fi networks. Outdoor wireless access takes advantage of the growing popularity of inexpensive Wi-Fi clients, enabling new service opportunities and applications that improve user productivity and responsiveness.

As the demand for outdoor wireless access increases, customers faced with tight budgets and reduced resources must respond with wireless LAN (WLAN) solutions that take full advantage of existing tools, knowledge, and network resources to address ease of deployment and WLAN security issues in a cost-effective way. The Cisco Wireless Mesh solution is an outdoor WLAN solution that excels in the unique attributes of wireless mesh technology, effectively supports current networking requirements, and lays the foundation for the integration of business applications.

Outdoor wireless solutions offer a number of challenges compared to a standard indoor WLAN, particularly in these areas:

- Environment
- Coverage
- Total cost of ownership (TCO)
- Physical device security

The outdoor environment is harsher than the indoor environment and so requires specialized equipment or enclosures to contain and protect indoor equipment that is deployed outdoors.

Outdoor WLAN deployments attempt to cover wider areas than indoor wireless networks, while addressing the challenges of less control over sources of interference, finding a suitable wired connection to connect the wireless mesh network to the wired network, and the availability of power for the mesh network devices.

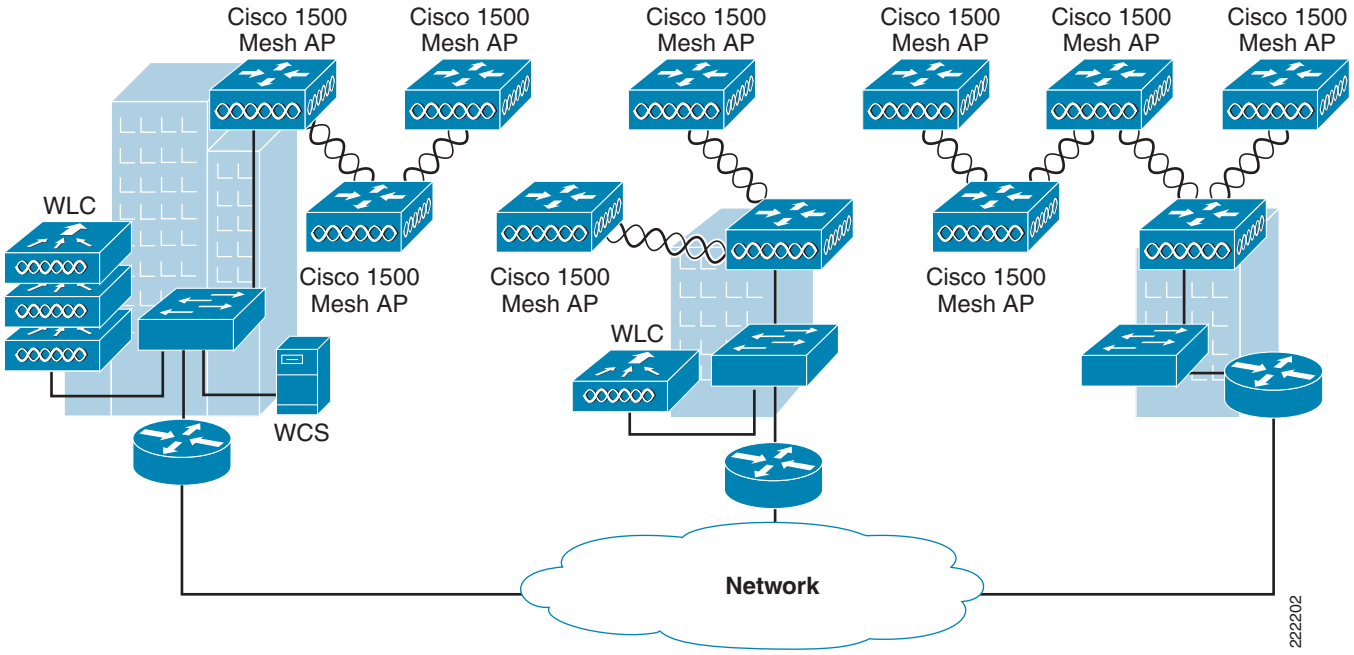
Outdoor deployments also require specialized radio frequency (RF) skills, may have a lower user density than indoor deployments, and may be deployed in environment that is less regulated than inside a building. These features put pressure on the TCO of the outdoor solutions and require a solution that is easy to deploy and maintain.

The Cisco Wireless Mesh solution has three core components:

- Cisco 1500 Series Mesh AP—Outdoor access point that provides WLAN client access in the mesh and backhaul client connections
- Cisco Wireless LAN controller (WLC)—Provides a central point for AP control functions
- Cisco Wireless Control System (WCS)—Management platform for enhanced scalability, manageability, and visibility of large-scale implementations

Figure 8-1 shows a simple mesh network deployment made up of mesh APs, WLCs, and a WCS. In this example deployment, there are three mesh APs connected to the wired network. These APs are designated as roof-top APs (RAPs); all other APs in the mesh network are known simply as mesh APs (MAPs). All mesh APs, both MAP and RAP, can provide WLAN client access, however in most cases because of the RAPs location it is not well suited for providing client access. In the following example the RAPs are located on the roof of each of the buildings and are connected to the network at each location. Some of the buildings have WLCs located at them to terminate LWAPP sessions from the mesh APs, but it is not necessary for every building to have a WLC. LWAPP sessions can be back hauled across the WAN if needed to other locations where a WLC resides.

Figure 8-1 Mesh Solution Diagram



Cisco 1500 Series Mesh AP

The Cisco 1500 Series Mesh AP shown in Figure 8-2 is the core component of the wireless mesh solution and leverages existing and new features and functionality in the Wireless LAN controllers and the WCS.

Figure 8-2 Cisco 1510 and 1520 Wireless mesh APs

There are three types of Cisco 1500 Series Mesh APs:

- The AP1520—An outdoor access point consisting of two simultaneous operating radios:
  - One 2.4 GHz radio that is used for client access.
  - One 5.8/4.9 GHz radio that is used for data backhaul to other 1500 Series Mesh APs.
- The AP1520 also has a modular design and can be configured with the following optional uplink interfaces:
  - Cable Modem DOCSIS 2.0 with Cable Power Supply
  - Fiber Interface with 100BaseBX SFP
  - 1000BaseT Gig Ethernet
- The AP1510—An outdoor access point consisting of two simultaneous operating radios:
  - One 2.4 GHz radio that is used for client access.
  - One 5.8/4.9 GHz radio that is used for data backhaul to other 1500 Series Mesh APs.

  The AP1510 also has an Ethernet port which can be used for connectivity to the WLC or for a connected LAN segment for bridging.
- The AP1505—An outdoor access point consisting of a single 2.4 GHz radio:
  - One 2.4 GHz radio that is used for client access and backhaul.
  - Like the AP1510, the AP1505 also has a wired Ethernet port.

A wide variety of antennas are available to provide flexibility when deploying the 1500 Series Mesh AP over various terrain. The 5.8 GHz frequency radio uses 802.11a technology and is used in the system as the backhaul or relay radio. Wireless LAN client traffic arrives at the AP via the 2.4GHz radio passes either through the AP backhaul radio or is relayed through other 1500 Series Mesh APs until it reaches the WLC Ethernet connection.

The 1500 Series Mesh AP also has a 10/100 Ethernet connection to provide bridging functionality. This Ethernet connection supports power over Ethernet (PoE) through a separate power injection system.

Note The power injector is unique for this product; other Cisco power injection solutions are not suitable for use with the Cisco 1500 Series Mesh AP.

The Cisco 1500 Series Mesh AP uses LWAPP to communicate to a wireless controller and other 1500 Series Mesh APs in the wireless mesh.

The 1500 Series Mesh AP is designed to be mounted upside-down with its antenna oriented vertically, as shown in Figure 8-3.

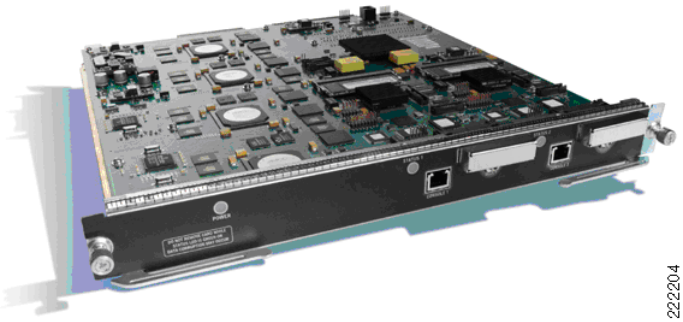
Figure 8-3 1500 Series Mesh AP Installation

Cisco Wireless LAN Controllers

The wireless mesh solution is supported by the Cisco 4400 Series Wireless LAN Controller (WLC) (shown in Figure 8-4) and the Cisco Wireless Services Module (WiSM) (shown in Figure 8-5). Either platform is recommended for wireless mesh deployments because they can both scale to large numbers of access points and can support both Layer 2 and Layer 3 LWAPP connections.

Figure 8-4 Cisco 4400 Wireless LAN Controller

Figure 8-5 Cisco Wireless Services Module



For more information on Cisco Wireless LAN controllers, see: http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps6548/prod_brochure0900aecd8036884a_ns621_Networking_Solutions_Brochure.html.

Wireless Control System (WCS)

The Cisco Wireless Control System (WCS) is the platform for wireless mesh planning, configuration, and management. It provides the tools to allow network managers to design, control, and monitor wireless mesh networks from a central location.

With the Cisco WCS, network administrators have a solution for RF prediction, policy provisioning, network optimization, troubleshooting, user tracking, security monitoring, and WLAN systems management. Graphical interfaces make wireless LAN deployment and operations simple and cost-effective. Detailed trending and analysis reports make Cisco WCS vital in supporting ongoing network operations.

Wireless Mesh Operation

In a wireless mesh deployment, there are multiple 1500 Mesh APs deployed as part of the same network. Mesh APs form parent, child, and neighbor relationships with each other to form the mesh and establish a LWAPP tunnel back to their specified primary WLC. Parent, child, and neighbor relationships are discussed further in Mesh Neighbors, Parents, and Children, page 8-10.

MAPs use the Adaptive Wireless Path Protocol (AWPP) to determine the best path through other 1500 Mesh APs to their WLC. The wireless links between the MAPs and RAP(s) form a wireless mesh that is used to carry traffic from WLAN clients (through LWAPP tunnels) to the WLC and also to carry bridge traffic between devices connected to the MAP Ethernet ports.

A wireless mesh can simultaneously carry two different traffic types:

- WLAN client traffic through LWAPP tunnels
- MAP bridge traffic

WLAN client traffic terminates on the WLC, but the bridge traffic terminates on the Ethernet ports of the MAPs of the wireless mesh.

MAP membership in the wireless mesh can be controlled in a variety of ways. The default mesh AP authentication is EAP, but Pre Shared Key (PSK) authentication can also be configured. Bridge Group Name (BGN) is used in addition to authentication to control mesh membership or to segment a wireless mesh.

Bridge Authentication

When a mesh AP is turned on and connected to the network via a wired Ethernet connection, it joins a WLC using the following steps:

1. When the AP booted, it optionally obtained an IP address via DHCP if a static IP has not been previously configured.
2. The mesh AP s out a LWAPP discovery request.
3. If a WLC receives the request, it responds with a discovery response.
4. At this point the mesh AP issues a LWAPP join request.
5. The WLC issues an LWAPP join response and proceeds with EAP authentication.
6. Depending on the mesh AP's current image version, it may download a new image and re-boot.
7. After the reboot, the mesh AP requests to join the WLC again and re-authenticate.

Note PSK may be used in place of EAP if configured on the WLC.

If there is no wired connection for the mesh AP to use to connect to a WLC, it uses the following procedure to join the controller.:

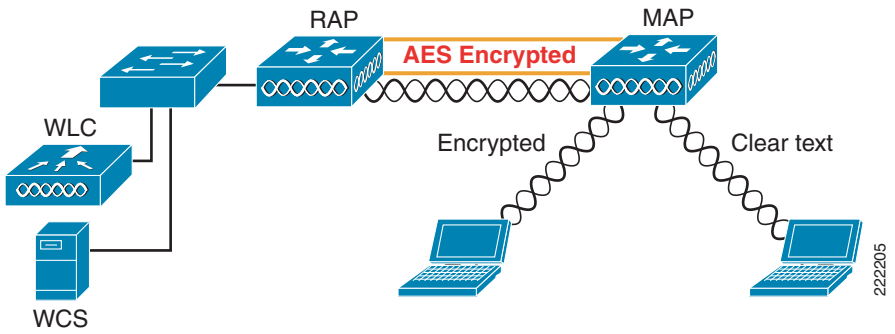
1. After boot, the mesh AP forms a 802.11 association and issues a LWAPP discovery request via its 802.11a connection.
2. When a mesh AP with a connection to the WLC is discovered, it uses DHCP to obtain an IP address if one has not been statically configured.
3. At this point the mesh AP issues a LWAPP join request.
4. The WLC issues an LWAPP join response and proceeds with EAP authentication.
5. Depending on the mesh AP's current image version, it may download a new image and re-boot.
6. After the reboot, the mesh AP rediscovers its parent and requests to join the controller again and re-authenticate.

Wireless Mesh Encryption

As discussed above, the wireless mesh bridges traffic between the MAPs and the RAPs. This traffic can be from wired devices being bridged by the wireless mesh or LWAPP traffic from the mesh APs. This traffic is always AES encrypted when it crosses a wireless mesh link (see Figure 8-6).

The AES encryption is established as part of the mesh AP neighbor relationships establishment with other mesh APs. The encryption keys used between mesh APs are derived during the EAP authentication process.

Figure 8-6 Mesh Encryption



AWPP Wireless Mesh Routing

The core of the Cisco Wireless Mesh network is the Cisco Adaptive Wireless Path Protocol (AWPP).

This protocol is designed specifically for wireless mesh networking in that its path decisions are based on both link quality and the number of Mesh AP hops. AWPP is also designed to provide ease of deployment, fast convergence, and minimal resource consumption.

For more information on AWPP, refer to:
http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps6548/prod_brochure0900aecd8036884a_ns621_Networking_Solutions_Brochure.html.

Example Simple Mesh Deployment

The key network components of a simple mesh deployment design shown in Figure 8-7 are the following:

- WCS—Key component in the management, operation, and optimization of the mesh network.
- Wireless LAN Controller— Provides real-time communication between lightweight access points and other wireless LAN controllers to deliver centralized security policies, wireless intrusion prevention system (IPS) capabilities, RF management, quality of service (QoS), and mobility.
- Router between the network and the mesh—Provides a Layer 3 boundary where security and policy enforcement can be applied. The router also provides Layer 2 isolation of the RAP. This is necessary because the RAP bridges traffic from its local Ethernet port to the mesh, so this traffic must be limited to that necessary to support the solution so that resources are not consumed by the unnecessary flooding of traffic.
- RAP— The wired network connected Mesh AP that provides the “path” home for the wireless mesh APs.
- A number of MAPs.

Note The RAP wireless connection is to the center of the MAP mesh, which is an optimal configuration that minimizes the average number of hops in the mesh. A RAP connection to the edge of a mesh would result in an increase of hops.

Figure 8-7 Simple Mesh Deployment

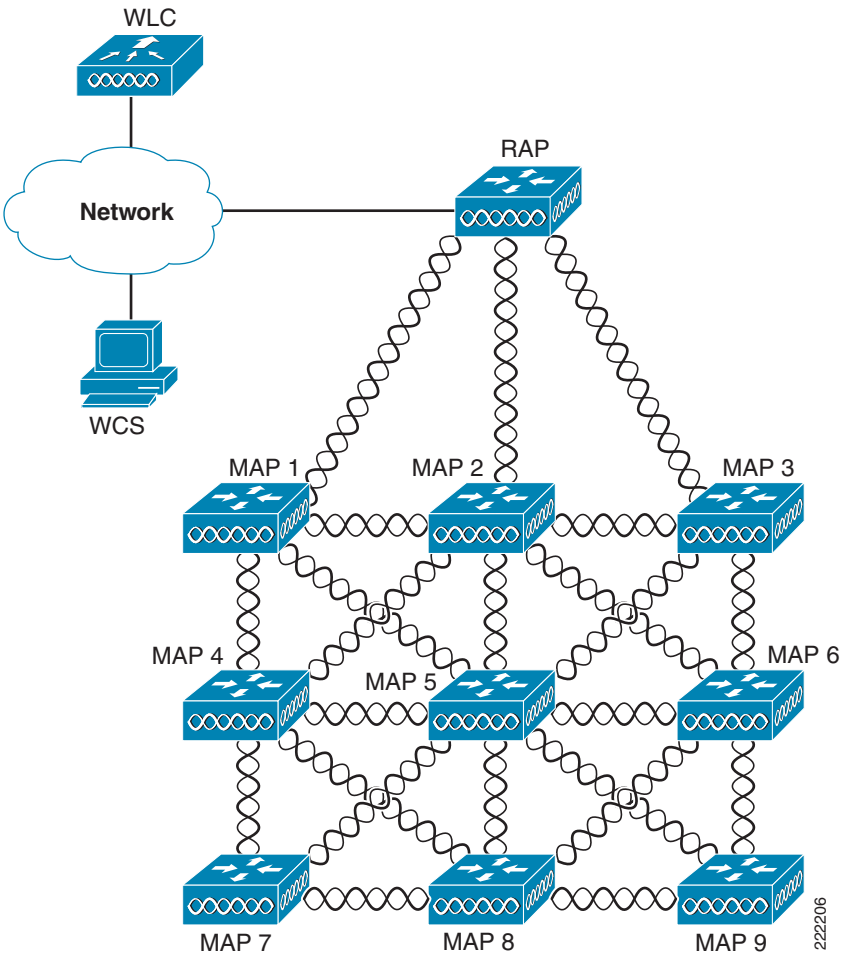


Figure 8-8 shows one possible logical view of the physical configuration, with MAP5 as the path home for all other MAPs.

Figure 8-8 Logical Mesh View

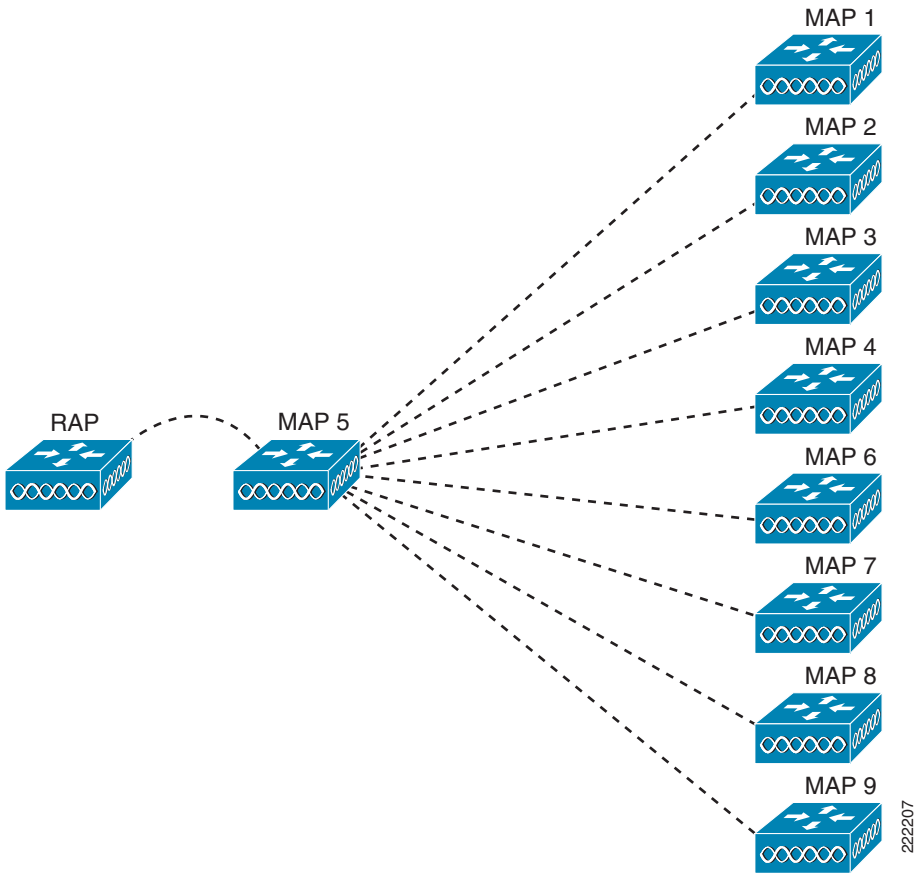
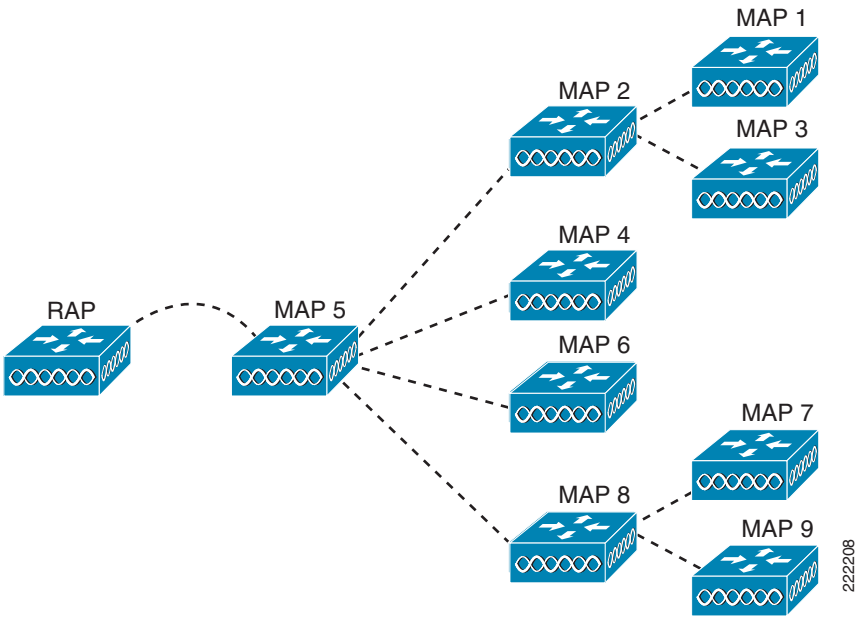


Figure 8-9 shows an alternate logical view, in which the signal-to-noise ratio (SNR) on the indirect paths to MAP5 is small enough for the other MAPs to consider taking an extra hop along a greater NSR link to get to MAP5.

Figure 8-9 Unequal Mesh Paths



In both the cases above, MAP5 is the path home for all traffic. Ideally, the coverage from the RAP should be such that other MAPs, such as MAP2 for example, have a path back to the RAP, and traffic could be routed via MAP 2 in case of a loss of signal to MAP 5.

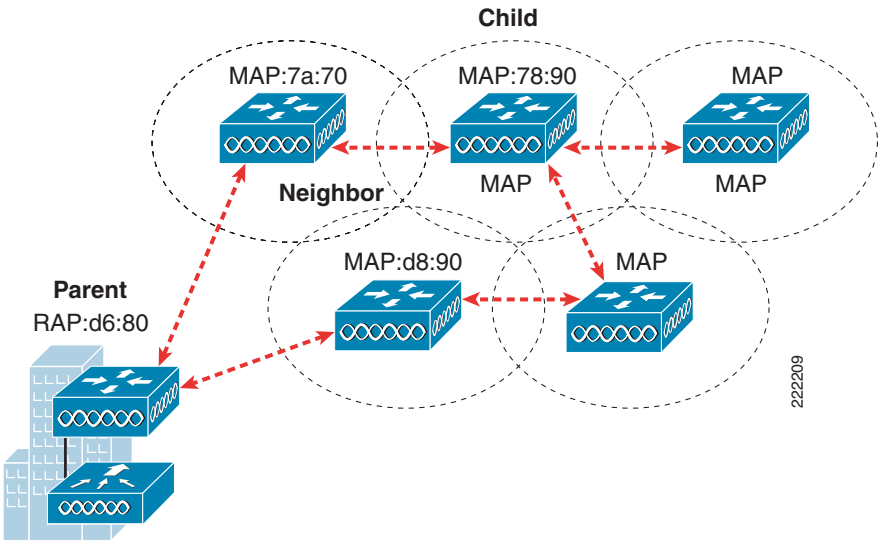
Mesh Neighbors, Parents, and Children

There are three relationships mesh APs can have with another:

- A *neighbor* within a mesh is an AP that is within RF range but has not been selected as a parent or a child because its "ease" values are lower than another neighboring AP (refer to Ease Calculation, page 8-14).
- A *parent* AP is one that is selected as the best route back to the RAP based on the best ease values. A parent can be either the RAP itself or another MAP.
- A *child* AP is one that has selected the parent AP as the best route back to the RAP. The example in Figure 8-10 illustrates a small mesh. In this example, MAP:7a:70 parent is RAP:d680 and the MAP:7a:70 child is MAP:78:90. Map:7a:70 also has a neighbor relation with MAP:d8:90.

Note A mesh AP can be both a parent other mesh APs and a child of another mesh AP, however a RAP is the only mesh AP that is not a child of any AP.

Figure 8-10 Parent, Child, and Neighbor

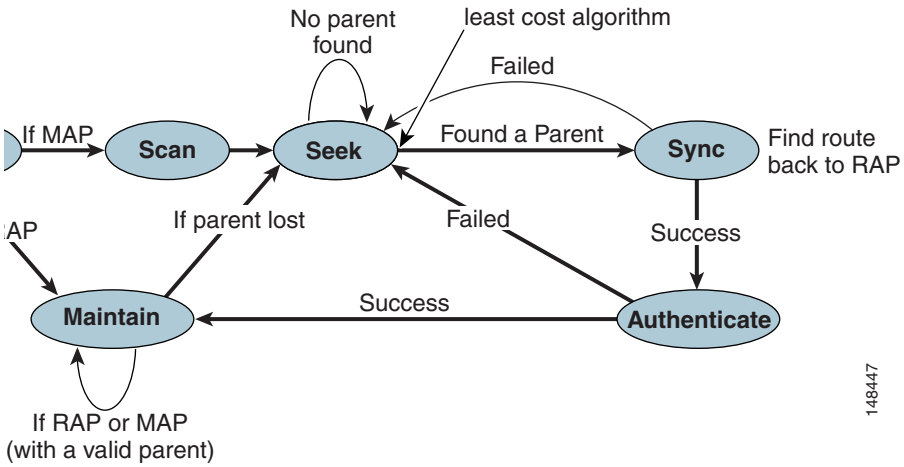


The goal of AWPP is to find the best backhaul link path for a MAP through the mesh back to a RAP. To do this, the mesh AP actively solicits for neighbor APs. During the solicitation, the mesh AP learns all of the available neighbors back to a RAP, determines which neighbor offers the best path, and then synchronizes with that neighbor.

Figure 8-11 shows the state diagram for a mesh AP when it is trying to establish a connection.

A mesh AP must first decide whether it is a RAP. A mesh AP becomes a RAP if it can communicate with an WLC through its Ethernet interface. If the mesh AP is a RAP, it can go straight to the maintain state. In the maintain state, the mesh AP has established an LWAPP connection to the controller so it does not need to seek other mesh APs, but simply responds to solicitations. If the mesh AP is not a RAP, it starts a scan process where the mesh AP scans all available channels and solicits information from other mesh APs.

Figure 8-11 Mesh AP State Diagram



This behavior has two main implications:

- The RAP does not change channels, and therefore the channel used to build the mesh from a RAP is defined in the RAP configuration. By default, the RAP uses channel 161.

- The mesh is built from the RAP out, because initially only the RAP can respond to solicitations.

If the mesh AP is not a RAP, it follows the state diagram above in the following modes:

- Scan—The AP scans all the backhaul channels using mesh beaconing. This mechanism is similar to the 802.11 beaconing mechanisms used by wireless access networks. The frame used for beaconing is called NEIGHBOR_UPDATE. Essentially, NEIGHBOR_UPDATE frames are advertised by the network so that new nodes can scan and quickly discover neighbors. Each RAP and MAP broadcast NEIGHBOR_UPDATE frames after being connected to the network (via a WLAN controller). Any neighbor updates with SNRs lower than 10 dB are discarded. This process is called passive scanning.
- Seek—Solicits other members of the mesh. Mesh APs issuing successful responses to these solicitations become neighbors.
- Sync—The mesh AP learns the path information from each of its neighbors and the neighbor with the greatest ease becomes the parent of the soliciting mesh AP. If the neighbors report multiple RAPs, the RAP with the greatest ease is chosen.
- Authenticate—The mesh AP authenticates to the WLC through a connection established via its parent AP. This is a standard certificate-based LWAPP AP authentication.
- Maintain—The mesh AP responds to other mesh AP solicitations and regularly issues solicitations to determine any changes in the mesh. It is only after entering the maintain state that the mesh AP is visible to the WLC and WCS. Note that in the maintain state, the solicitations occur only on the channel defined by the mesh RAP, whereas a mesh AP in seek mode solicits on all channels, only stopping when it has found a parent AP.

Background Scanning in Mesh Networks

Background scanning allows Cisco 1500 series APs to actively and continuously monitor neighboring channels for optimum paths and parents. Because the access point is searching on neighboring channels as well as the current channel, the list of possible alternate optimal paths and parents is greater.

Identifying this information prior to the loss of a parent results in a faster switch over and the best link possible for the access point. Additionally, access points might switch to a new channel if a link on that channel is found to have a better cost metric (fewer hops, stronger SNR) than its current channel.

Background scanning on other channels and collecting of data from neighbors on those channels is done on the backhaul between two access points:

- For 1510 access points, the backhaul (primary) operates on the 802.11a link.
- For 1505 access points, the backhaul operates on the 802.11b/g link.

Background scanning is enabled on a global basis on the controller using the command-line interface:

config mesh background-scanning {enable | disable}

Enter this command to verify background scanning is enabled.

show mesh background-scanning

It is enabled by default.

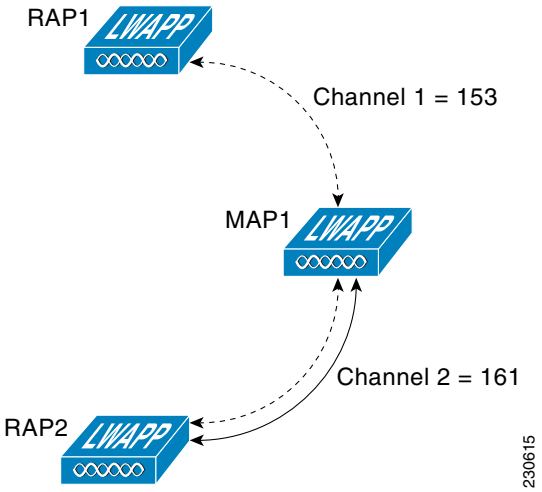
Note Latency might increase for voice calls when they are switched to a new channel.

If channels requiring Dynamic Frequency Selection (DFS) are used, locating neighbors in other channels might take longer.

A few operating scenarios are provided below to better understand the operation of background scanning. In Figure 8-12, when the mesh access point, MAP1, initially comes up it is aware of both root access points, RAP1 and RAP2, as possible parents. RAP2 is chosen as the parent for MAP1 because the route through RAP2 provides a better cost metric.

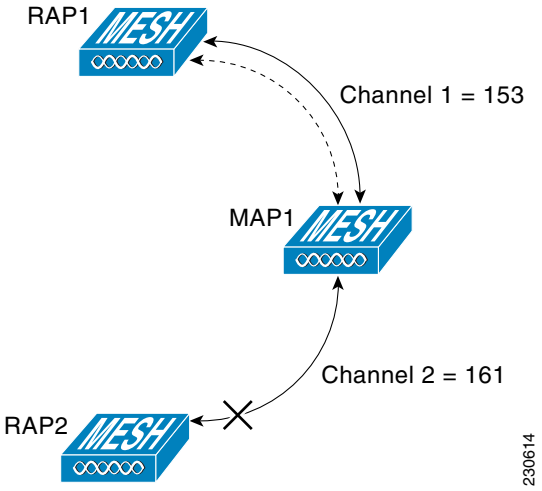
Once the link is established, background scanning continuously monitors all channels in search of a better path and parent. RAP2 continues to act as parent for MAP1 and communicates on channel 2 until either the link goes down or a better path is located on another channel.

Figure 8-12 Mesh Access Point, MAP1, Selects Parent



In Figure 8-13, the link between MAP1 and RAP2 is lost. Data from ongoing background scanning identifies RAP1 and channel 1 as the next best parent and communication path for MAP1, so that link is established immediately without the need for additional scanning after the link to RAP2 goes down.

Figure 8-13 Background Scanning Identifies New Parent



Enter this command to enable or disable background scanning on the controller:

config mesh background-scanning {enable | disable}

Enter this command to verify background scanning is enabled:

show mesh background-scanning

Ease Calculation

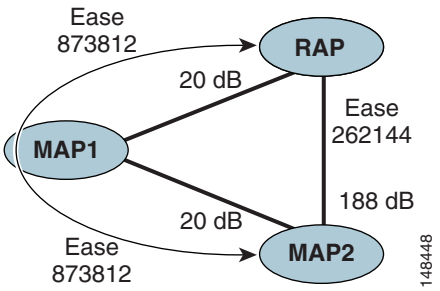
Ease is calculated using the SNR and hop value of each neighbor and applying a multiplier based on various SNR thresholds. The purpose of this multiplier is to apply a spreading function to the SNRs that reflects various link qualities.

A parent AP is chosen by using the adjusted ease, which is the ease of each neighbor divided by the number of hops to the RAP:

adjusted ease = min (ease at each hop)/Hop count

In Figure 8-14, MAP2 prefers the path through MAP1 because the adjusted ease (436906) though this path is greater then the ease value (262144) of the direct path from MAP2 to RAP.

Figure 8-14 Parent Path Selection



SNR Smoothing

One of the challenges in WLAN routing is the ephemeral nature of RF. This must be considered when determining an optimal path and deciding when a change in path is required. The SNR on a given RF link can change substantially from moment to moment; changing route paths based on these fluctuations results in an unstable network with severely degraded performance. To effectively capture the underlying SNR but remove moment-to-moment fluctuations, a smoothing function is applied that provides an adjusted SNR.

In evaluating potential neighbors against the current parent, the parent is given 20% of “bonus-ease” on top of the parent’s calculated ease to reduce flapping between parents. The assignment of a bonus-ease mandates that a potential parent must offer a significantly better route to the RAP in order for a child to make a switch. Parent switching is transparent to LWAPP and other higher-layer functions.

Loop Prevention

To ensure that routing loops are not created, AWP discards any route that contains its own MAC address. That is, routing information apart from hop information contains the MAC address of each hop to the RAP. This enables a 1500 Series mesh AP to easily detect and discard routes that loop.

Choosing the Best Mesh Parent

The OPS algorithm is implemented in the Seek state of the AWPP state machine. The basic steps of the parent selection algorithm in the AWPP (for both a RAP and MAP with radio backhaul) is as follows:

- A list of channels with neighbors is generated by passive scanning in the Scan state, which is a subset of all backhaul channels.
- The channels with neighbors present are actively scanned in the Seek state and the backhaul channel is changed to the channel with the best neighbor ease.
- The parent is set to the best neighbor and the parent-child handshake is completed in Seek state.
- Parent maintenance and optimization occurs in the Maintain state.

This algorithm is run at startup and whenever a parent is lost and no other potential parent exists, usually followed by an LWAPP network and controller discovery. All neighbor protocol frames carry the channel information. Both parent maintenance and optimization techniques remain unchanged, as described in the following:

- Parent maintenance occurs by the child node sending a directed NEIGHBOR_REQUEST to the parent and the parent responding with a NEIGHBOR_RESPONSE.
- Parent optimization and refresh occurs by the child node sending a NEIGHBOR_REQUEST broadcast on the same channel as that of its parent and evaluating all responses from neighboring nodes on this channel. In most practical mesh networks, only a single channel backhaul is designed.
- A parent MAP is the MAP that has the best path back to a RAP. AWPP uses ease to determine the best path. Ease can be considered the opposite of cost and the preferred path is the path with the higher ease.

Routing Around an Interface

This feature is optional and is user configurable via Controller CLI only. If this feature is enabled, it transmits packets on secondary backhaul (b/g radio) when there is transient interference on the primary backhaul (A radio).

There are two modes of operation for Routing Around an Interface (RAI):

- **Config mesh secondary-backhaul enable**—This enables RAI globally on all APs. In order for RAI to work properly, the user has to configure the same “b/g” channel on all APs beyond the first HOP to the one that is being used on the first HOP “b/g” radio. If RRM (auto-rf) is enabled, then it changes the channels on APs and RAI will not work.
- **Config mesh secondary-backhaul enable force-same-secondary-channel**—This forces the whole subtree rooted at one hop MAPs to have the same secondary channel. Ignore RRM or manually assigned for MAPs at two hops and deeper.

Design Details

Each outdoor wireless mesh deployment is unique, with its own challenges regarding locations, obstructions, and network infrastructure availability. Such challenges must typically be addressed in addition to design requirements that are based on users, traffic, and availability. This section discusses important design considerations and provides an example of a wireless mesh design.

Wireless Mesh Design Constraints

When designing and building a wireless mesh network with the 1500 Mesh AP, there are a number of system characteristics to consider. Some of these apply to the backhaul network design and others to the WLC design:

- Recommended backhaul is 18 Mbps—18 Mbps is chosen as the optimal backhaul rate because it aligns with the maximum WLAN coverage distances of the MAP; that is, the distance between MAPs using 18 Mbps backhaul should allow for seamless WLAN client coverage between the MAPs. A lower bit rate may allow a greater distance between 1500 Mesh APs, but there are likely to be gaps in the WLAN client coverage and the capacity of the backhaul network is reduced. An increased bit rate for the backhaul network either requires more 1500 Mesh APs or results in a reduced SNR between mesh APs, limiting mesh reliability and interconnection. The wireless mesh backhaul bit rate, like the mesh channel, is set by the RAP.
- Number of backhaul hops should be limited to three to four—The number of hops is recommended to be limited to three to four primarily to maintain sufficient backhaul throughput, because each mesh AP uses the same radio for transmission and reception of backhaul traffic. This means that throughput is approximately halved over every hop. For example, the maximum throughput for an 18 Mbps is approximately 10 Mbps for the first hop, 5 Mbps for the second hop, and 2.5 Mbps for the third hop.
- Number of MAPs per RAP—There is no current software limitation of how many MAPs per RAP you can configure. However, it is suggested that you limit this to 20 MAPs per RAP to avoid bottle necks in your mesh.
- Number of APs per controller—The number of APs per controller is determined by the controller capacity.
- Number of controllers—The number of controllers per mobility group is limited to 24.

Client WLAN

The mesh AP client WLAN delivers all the WLAN features of a standard 802.11bg LWAPP deployment with the full range of security and radio management features.

The goals of the client WLAN must be considered in the overall mesh deployment:

- What bit rates are required? Higher bit rates reduce coverage and are limited by the mesh backhaul.
- What throughput is required? What are the application throughput requirements and how many simultaneous clients are expected on a Cisco 1500 Mesh AP?
- What coverage is required? Is the coverage between different 1500 Mesh APs required to be contiguous or is the mesh deployment a collection of separate active zones?
- What security mechanisms are required? Is the WLAN intended for public consumption or private? What security is needed for client access?

Bridging Backhaul Packets

Bridging services are treated a little differently from regular controller-based services. There is no outer DSCP value in bridging packets because they are not LWAPP encapsulated. Therefore, the DSCP value in the IP header as it was received by the AP is used to index into the table as described in the path from AP to AP (backhaul).

Bridged frames received from a station on a LAN connected to a MAP are not modified in any way. There is no override value for an 802.1p classification. Therefore, in bridging mode the LAN traffic classification must be properly secured.

Frames are transmitted to the MAP LAN precisely as they are received upon the ingress to the wireless mesh bridge.

The 1500 does not tag modify DSCP:

- On the ingress port, the 1510 sees a DSCP marking and encapsulates the IP packet and applies the corresponding 802.1p priority.
- On the egress port, the 1510 decapsulates the IP packet and places it on the wire with an unmodified DSCP marking.

For this prioritization to be effective, Ethernet devices, such as IP video cameras, must have the capability to mark the DSCP of packets.

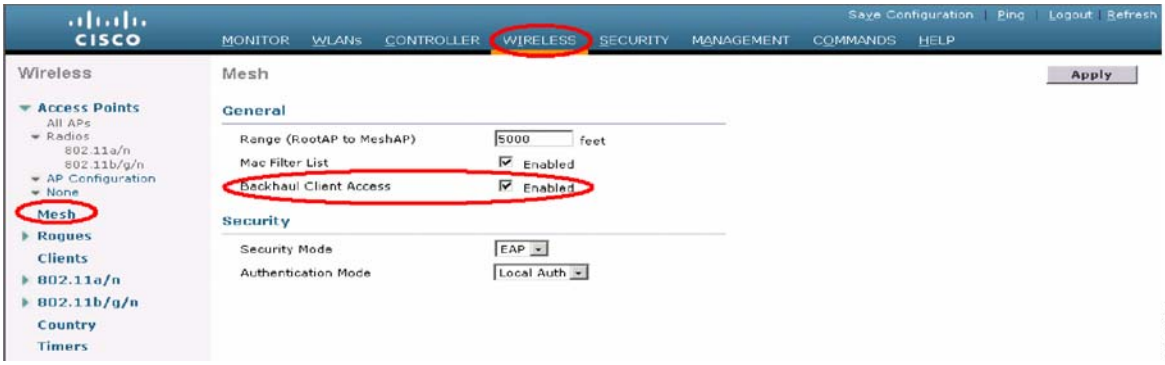
Client Access on Backhaul Connections

It is possible to allow client access on the 5.8 and 4.9 GHz backhaul connection while simultaneously transmitting backhaul traffic. This feature is particularly beneficial for deployments that need to support both 2.4 and 5GHz clients. This optional feature is turned off by default and can be enabled via the CLI command interface with the following command.

(Cisco Controller) >config mesh client-access *enable/disable*

In the GUI you can enable this feature in the mesh feature section as shown in Figure 8-15.

Figure 8-15 Client Access



Increasing Mesh Availability

A wireless mesh cell has similar properties to the cells used to create a cellular phone network. The technology may define the maximum size of the cell; smaller cells can be created to cover the same physical area, providing greater availability or capacity. This is done by adding RAPs to the cell. Just as in the larger mesh deployment, the decision is whether to use RAPs on the same channel, as shown in Figure 8-16, or use different channels, as shown in Figure 8-17. The addition of RAPs into an area adds capacity and resilience to that area.

Figure 8-16 Two RAPs per Cell with the Same Channel

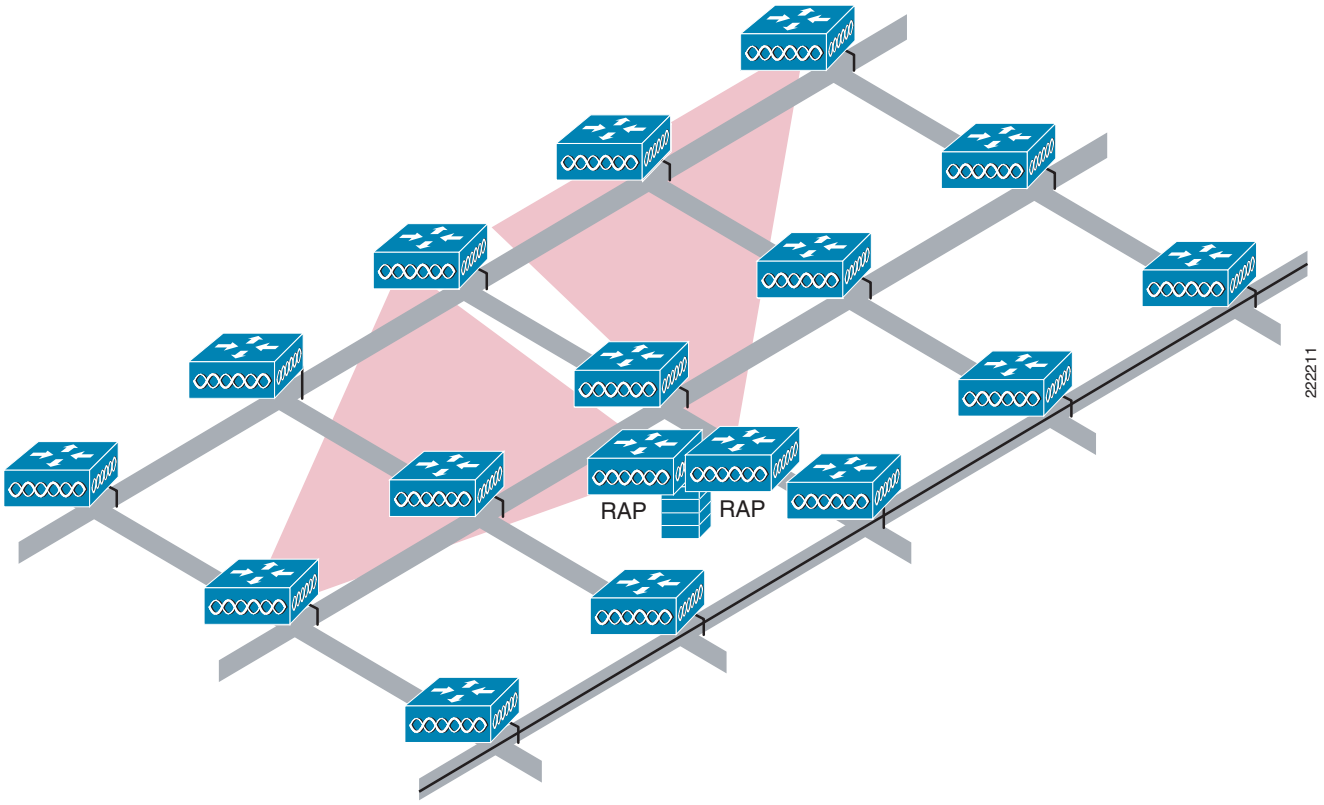
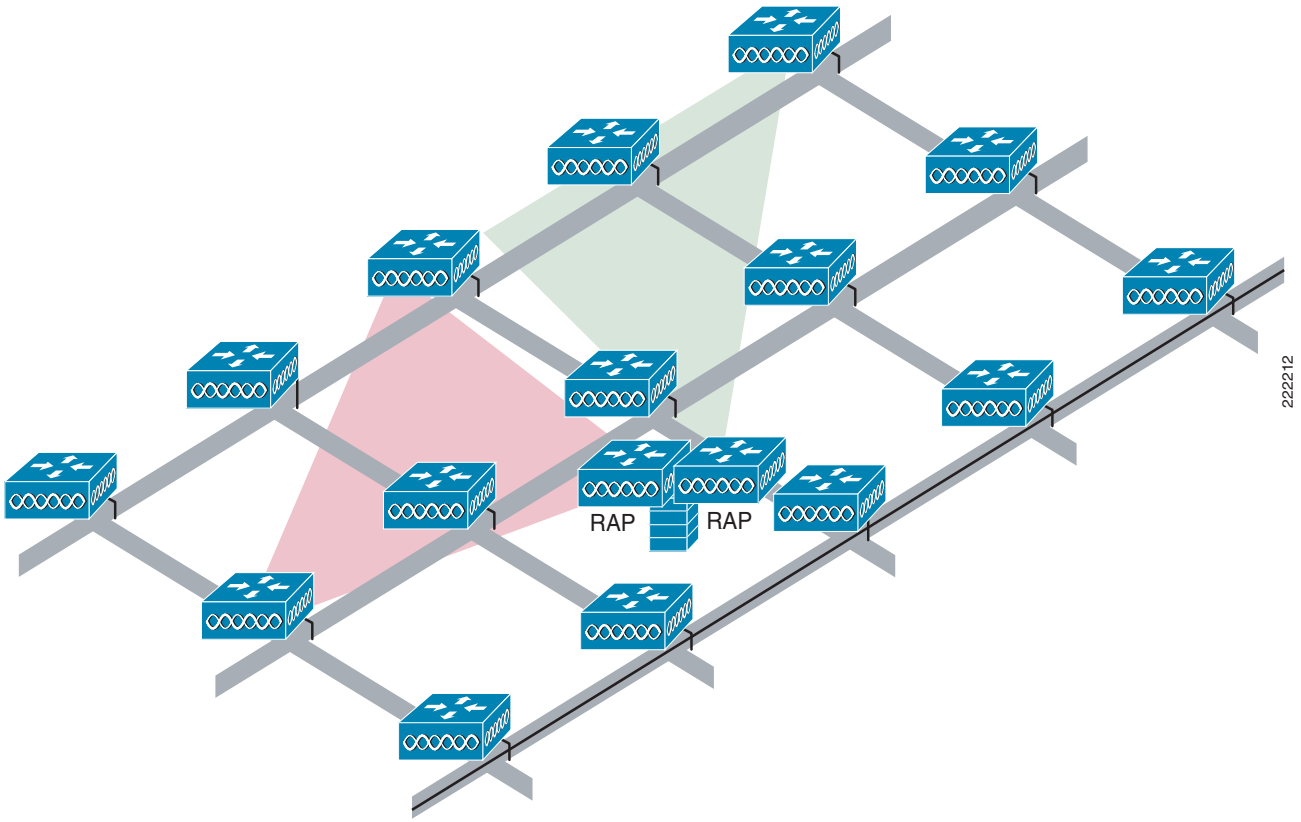


Figure 8-17 Two RAPs per Cell on Different Channels



Multiple RAPs

Before deploying multiple RAPs, the purpose for deploying these RAPs needs to be considered. If additional RAPs are being considered to provide hardware diversity, they should be deployed on the same channel as the primary RAP. The reason for this is to minimize the convergence time in a scenario where the mesh transfers from one RAP to another. When planning RAP hardware diversity, the 32 MAPs per RAP limitation should be remembered.

If the additional RAPs are being deployed primarily to provide additional capacity, the additional RAPs should be deployed on a different channel from its neighboring RAPs to minimize the interference on the backhaul channels.

When adding a second RAP on a different channel, channel planning or RAP cell splitting can be used to reduce the extent of potential collision domains. Channel planning allocates different non-overlapping channels to RAPs in the same collision domain to minimize the collision probability. RAP cell splitting is a simple, yet effective, way to reduce the collision domain. Instead of deploying one RAP with omni-directional antennas in a mesh network, two or more RAPs with directional antennas can be deployed. These RAPs are collocated but operate on different frequency channels, thus dividing a large collision domain into several smaller ones that operate independently.

If the Wireless Mesh bridging features are being used with multiple RAPs, these RAPs should all be on the same subnet to ensure that a consistent subnet is provided for bridge clients.

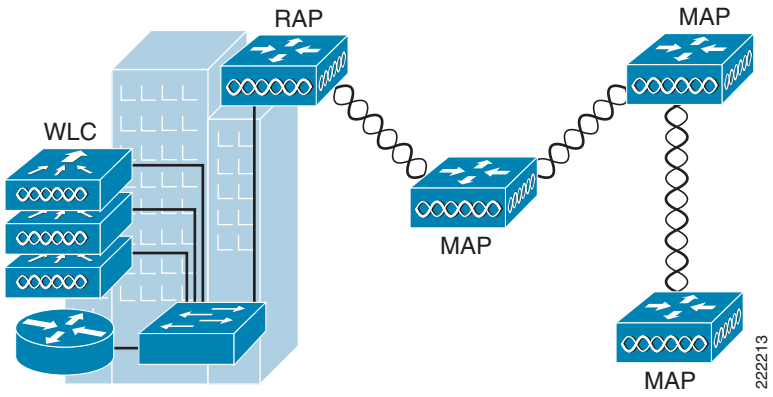
If you build your mesh with multiple RAPs on different subnets, MAP convergence times can increase in the event of a fail over as the MAP has to failover to another RAP on a different subnet and DHCP for an appropriate IP address. One way to limit this from happening is to use different BGN for segments in your network that are separated by subnet boundaries. In segmenting in this manner, MAPs do not associate with a RAP on a different subnet and you avoid slow convergence issues and the expense of the higher availability offered by the additional RAPs.

Multiple Controllers

There are operational advantages to centralizing WLCs and these advantages need to be traded off against the speed and capacity of the links to the LWAPP APs and the traffic profile of the WLAN clients using these APs.

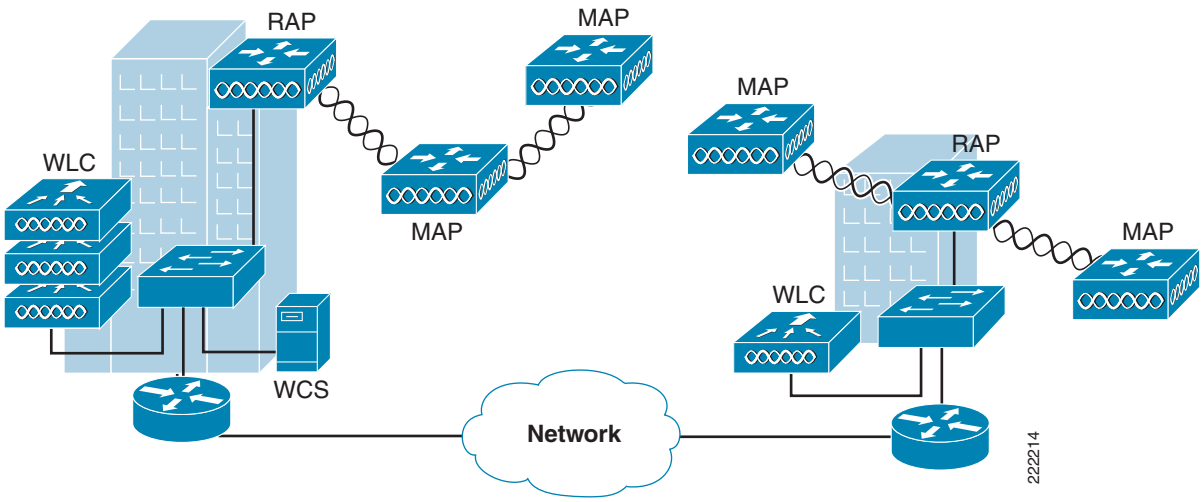
If the WLAN client traffic is expected to be focused on particular sites such as the Internet or a data center, centralizing the controllers at the same sites as these traffic focal points gives the operational advantages without sacrificing traffic efficiency (see Figure 8-18)

Figure 8-18 Centralized Controllers



If the WLAN client traffic is predominantly peer-to-peer, a distributed controller model as shown in Figure 8-19 may be a better fit. In such cases, it may be that a majority of the WLAN traffic are clients in the area, with a smaller amount of traffic going to other locations. Given that many peer-to-peer applications can be sensitive to delay and packet loss, it is best to ensure that traffic between peers takes the most efficient path.

Figure 8-19 Distributed Controllers



Given that most deployments see a mix of client server traffic and peer-to peer traffic, it is likely that a hybrid model of WLC placement is used, where points of presence (PoPs) are created with clusters of controllers placed in strategic locations in the network.

In all cases, remember that the LWAPP model used in the wireless mesh network is designed for a high-speed, low-latency network between the LWAPP APs (RAPs and MAPs in a Wireless Mesh) and the Wireless LAN Controller.

Multiple Wireless Mesh Mobility Groups

A wireless mesh WLAN coverage is not limited by the maximum number of controllers allowed in a mobility group. The WLANs that are part of a mobility group can be replicated in another mobility group and a WLAN client is able to roam between these mobility groups.

When roaming between mobility groups, the roaming may occur at Layer 2 or Layer 3, depending on the network topology behind the wireless mesh networks. When a Layer 3 roam occurs between mobility groups, mobility tunneling does not occur. Because of this the client must request a new DHCP address and will experience a session interruption.

Design Example

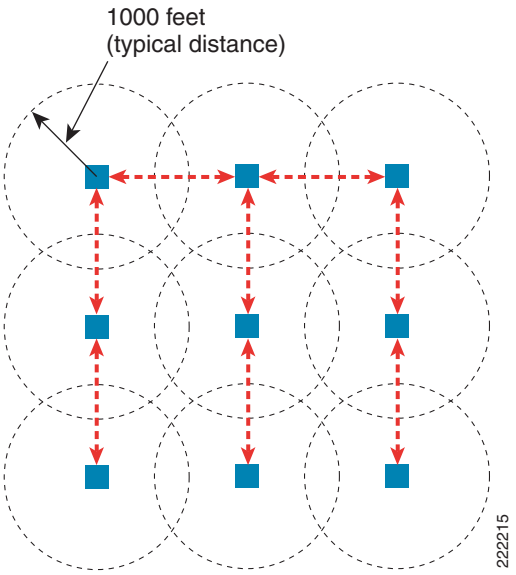
This section describes a design example of WLAN coverage in an urban/suburban area. It is important to understand cell size limitations and channel spacing for proper coverage. The following example explains how to make these preparations for a mesh deployment.

MAP Density and Distance

In cell planning there are two distances that should be considered, one in the typical backhaul radius as the other distance is the typical 2.4 client access radius. If you are simply building out a mesh to back haul data, then the 1000 foot radius is your limit. However if you are trying to provide complete client coverage, adhere to the 600 foot radius limit.

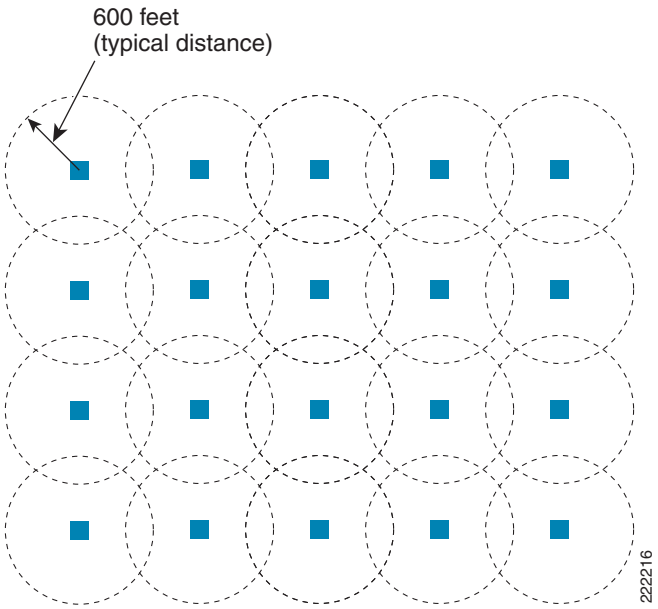
If you are designing your mesh deployment around the backhaul and do not intend to provide seamless WLAN coverage, you can have a typical cell size radius of 1000 feet. One square mile is 27,878,400 square feet; in this case, the approximate number of MAPs to cover a square mile given some cell overlap is nine and you can cover one square mile with approximately three or four hops (see Figure 8-20).

Figure 8-20 1000 Foot Distance Example



For deployments that provide seamless WLAN coverage it is suggested to have an approximate cell radius of 600 feet. One cell size comes out to be 1,130,973 square feet, so the approximate number of cells given some cell overlap is 25 cells per square mile (see Figure 8-21).

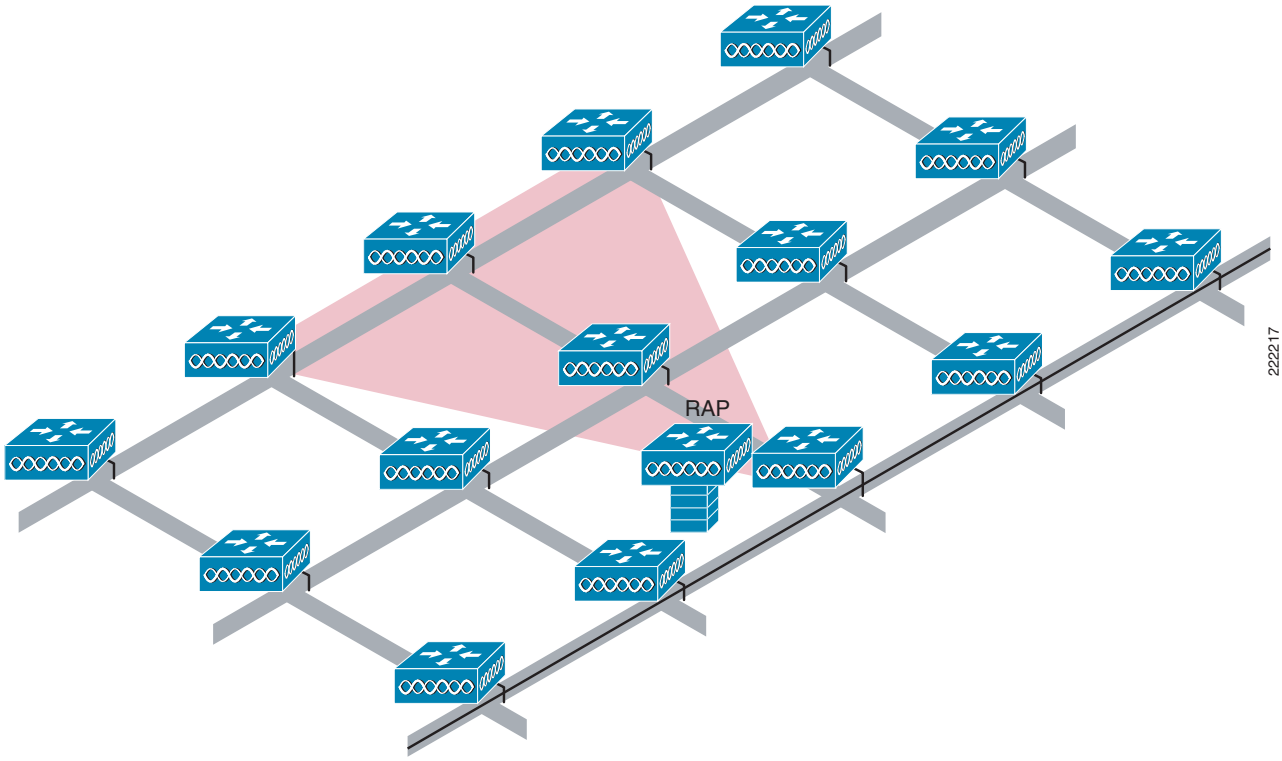
Figure 8-21 600 Foot Distance Example



When finding a location for a RAP the goal is to use the RAP location in combination with RF antenna design to ensure that there is a good RF link to the MAPs within the core of the cell.

This means that the physical location of a RAP may be on the edge of the cell and a directional antenna is used to establish a link into the center of the cell.

Figure 8-22 Schematic of the Wireless Mesh Layout



When laying out multiple cells, use channel planning similar to standard WLAN planning to avoid overlapping channels. As shown in Figure 8-23, both B2 and D3 share the same channel but do not overlap. This is the same for the other cells in the diagram that share the same channel. The cells sharing the same channels are:

- B2 and D3
- B3 and D2
- B4 and C2
- C3 and D4

If possible, the channel planning should also minimize channel overlap in cases where the mesh has expanded to cover the loss of a RAP connection, as shown in Figure 8-24.

Figure 8-23 Laying out Various Cells

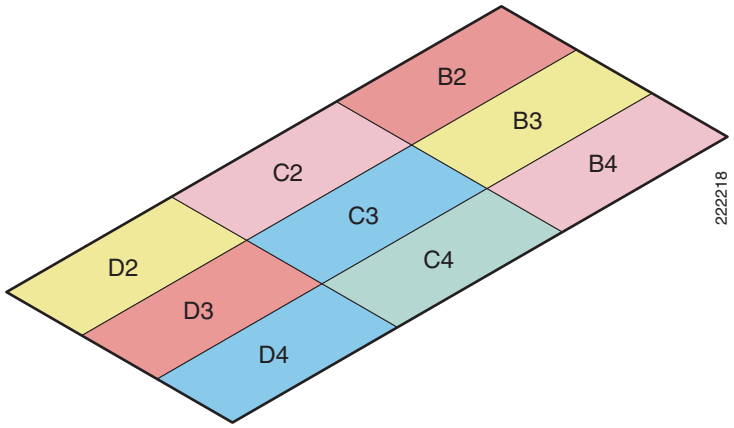
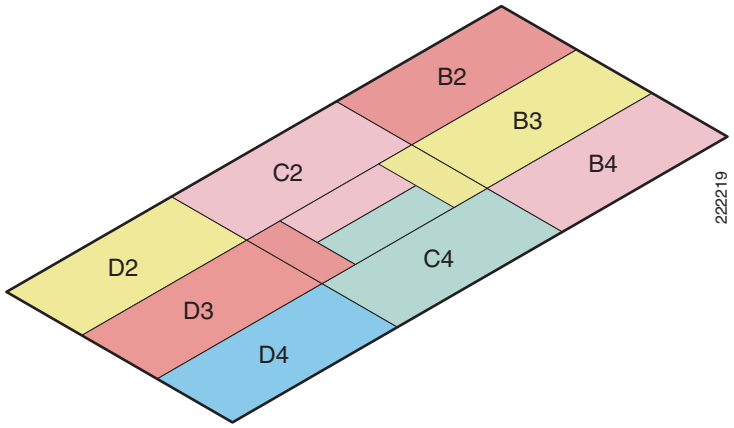


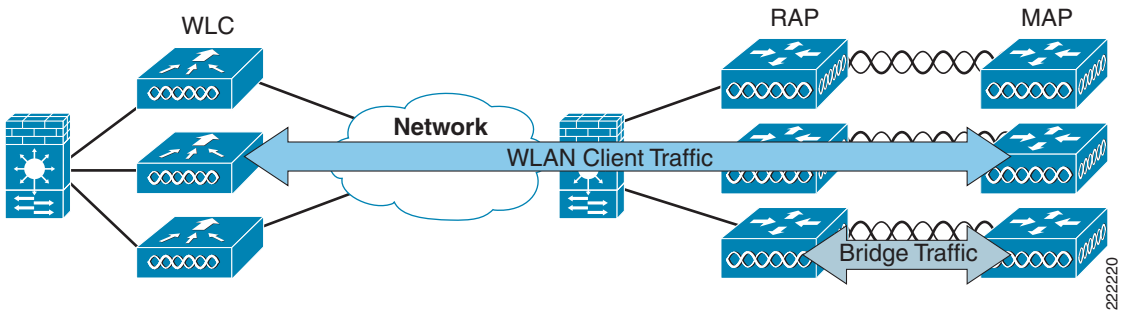
Figure 8-24 Failover Coverage



Connecting the Cisco 1500 Mesh AP to your Network

The wireless mesh has two locations where both bridged or WLAN client traffic terminate on the wired network. The first location is where the RAP attaches to the wired network, If bridging is enabled, this is where all bridged traffic connects to the wired network. The second location is where the WLC connects to the wired network; this is where WLAN client traffic from the mesh network connects to the wired network. This is shown schematically in Figure 8-25. The WLAN client traffic from the mesh is tunneled to the Wireless LAN Controller and then terminated on a VLAN to which the WLAN is assigned. The security and network configuration for each of the WLANs on the mesh depend on the security capabilities of the network to which the controller is connected.

Figure 8-25 Mesh Network Traffic Termination

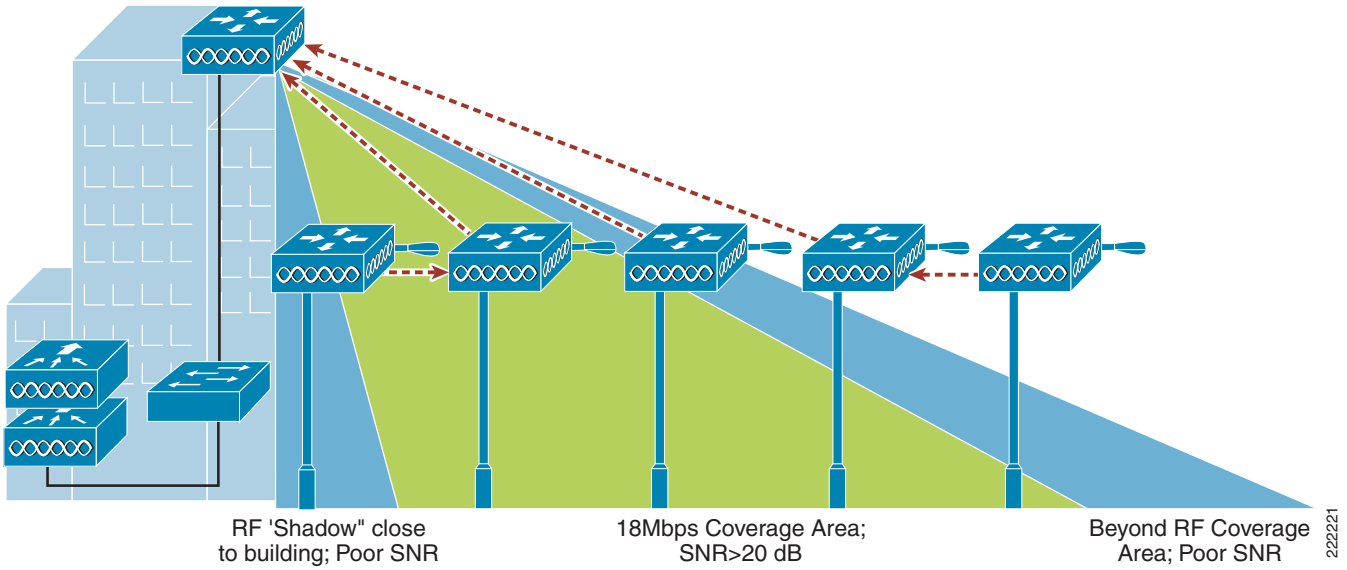


The connection to an Outdoor AP, unlike an indoor AP, may need to be firewalled from the wired network because the MAP that may be used for a bridging application and have limited security on the wired MAP ports.

Physical Placement of Mesh APs

When choosing a location for your MAPs, keep in mind issues like building height obstructions, light pole locations, and power options. In most environments there are light poles, but not all of them are equipped with an electric eye, which is a common feature used on light poles to automatically turn them on at night and off during the day. Street light power taps can be inserted between the light pole circuit and the electric eye to tap power from the street light. If a light pole does not have an electric eye, another method for powering the AP is required. Make note of what types of light poles you have and options for tapping power. When placing the roof top MAP, a directional antenna may be of use to direct coverage to a specific MAP or group of MAPs designated as the first hops into the mesh. If you plan to use omni directional antennas for the RAP, make sure to mount it towards the edge of the building so the radio coverage is not blocked. Figure 8-26 shows coverage concerns between the RAP and MAPs in the mesh.

Figure 8-26 AP Placement



AP 1500 Alternate Deployment Options

The Cisco 1500 Series Mesh AP solution supports alternate deployment modes, including the following:

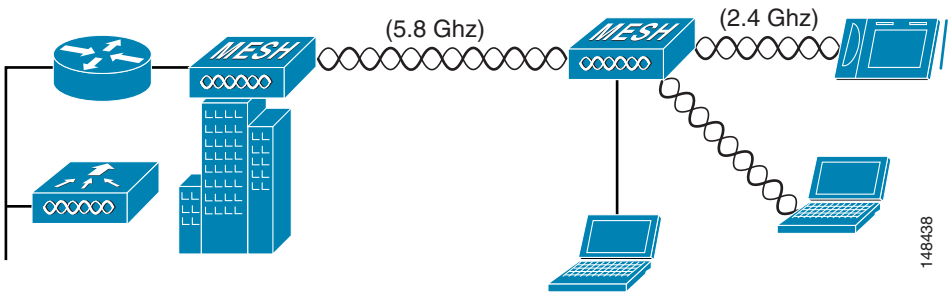
- WLAN backhaul
- Point-to-multipoint wireless bridging
- Point-to-point wireless bridging

These deployment methods can be useful for connecting LAN segments in a metropolitan environment or can be used to supplement backup connectivity for LAN segments. Client WLAN support can coexist in a bridged network configuration. Any of the following alternate deployment methods can simultaneously support mesh WLAN client traffic.

Wireless Backhaul

Cisco 1500 Mesh APs can provide a simple wireless backhaul solution where the 1500 Mesh AP is used to provide 802.11b/g services to WLAN and wired clients. This configuration is basically a wireless mesh with one MAP. Figure 8-27 shows an example of this deployment type.

Figure 8-27 Wireless Backhaul

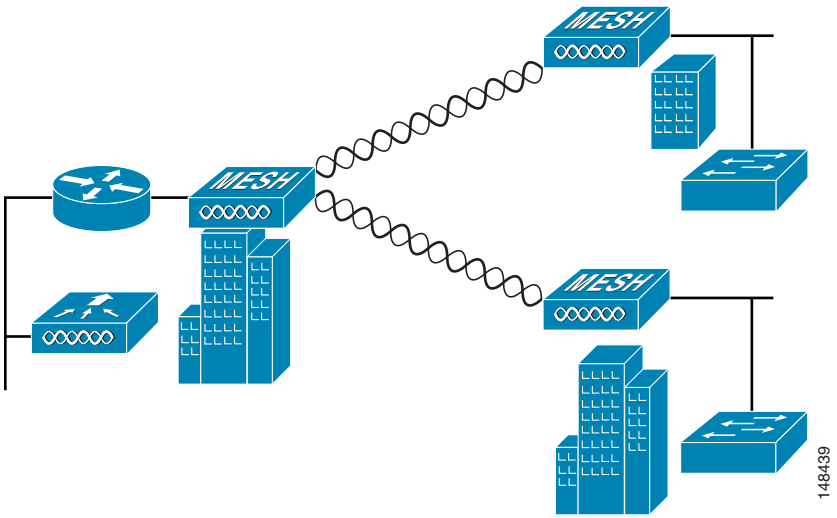


Point-to-Multipoint Wireless Bridging

In the point-to-multipoint bridging scenario, a RAP acting as a root bridge connects multiple MAPs as non-root bridges with their associated wired LANs. By default, this feature is turned off for all MAPs.

If Ethernet bridging is used, you must enable it on the controller for each MAP. Figure 8-28 shows a simple deployment with one RAP and two MAPs, but this configuration is fundamentally a wireless mesh with no WLAN clients. Client access can still be provided with Ethernet bridging enabled, although if bridging between buildings, MAP coverage from a high rooftop may not be suitable for client access.

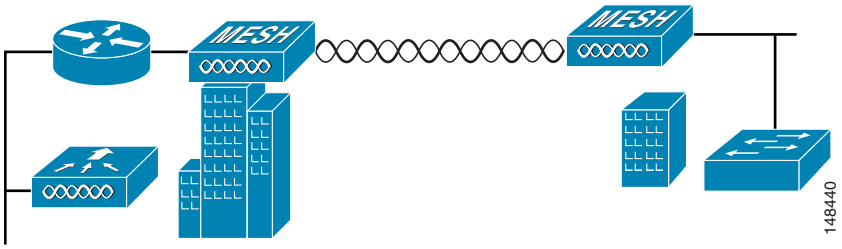
Figure 8-28 Point-to-Multipoint Wireless Bridging



10.6.3 Point-to-Point Wireless Bridging

In a point-to-point bridging scenario, a 1500 mesh AP can be used to extend a Layer 2 network by using the backhaul radio to bridge two segments of a switched network, as shown in Figure 8-29. This is fundamentally a wireless mesh with one MAP and no WLAN clients. Just as in point-to-multipoint networks, client access can still be provided with Ethernet bridging enabled, although if bridging between buildings, MAP coverage from a high rooftop may not be suitable for client access.

Figure 8-29 Point-to-Point Wireless Bridging



CHAPTER 9

VoWLAN Design Recommendations

This chapter provides additional design considerations when deploying voice over WLAN (VoWLAN) solutions. WLAN configuration specifics may vary depending on the VoWLAN devices being used and the WLAN design. This chapter provides more details about key RF and site survey considerations that are generally applicable to VoWLAN deployments, which were introduced in Chapter 3, "WLAN Radio Frequency Design Considerations."

Antenna Considerations

The more demanding network requirements of VoWLAN impacts WLAN planning at all levels, down to the choice of antenna. Key antenna considerations are as follows:

- Access point (AP) antenna selection
- Antenna placement
- Handset antenna characteristics

AP Antenna Selection

Cisco recommends a diversity ceiling-mount antenna for voice applications. Ceiling mounted antennas offer a quick and easy installation. More importantly, they place the radiating portion of the antenna in open space, which allows the most efficient signal propagation and reception. Cisco recommends that all antennas be placed 1 to 2 wavelengths from highly reflective surfaces such as metal. The 2.4 GHz wave is 4.92 inches (12.5 cm) and the 5 GHz is 2.36 inches (6 cm). The separation of one or more wavelengths between the antenna and reflective surfaces allows the AP radio a better opportunity to receive a transmission, and reduces the creation of nulls when the radio transmits. Orthogonal frequency-division multiplexing (OFDM) used by 11g and 11a helps to mitigate problems with reflections, nulls, and multipath; however, good antenna placement and the use of appropriate antenna types provide a superior solution. The ceiling tile itself is a good absorber of signals transmitted into the area above the ceiling and reflected back into the coverage area.

Antennas come in many types and form factors; no single type or module of antenna is best for all applications and locations. For additional information on the performance of various antenna types, and the part numbers of Cisco Aironet antennas, see the Cisco Aironet antenna guide at the following URL: http://www.cisco.com/en/US/products/hw/wireless/ps469/products_data_sheet09186a008008883b.html.

When attaching antennas to an AP, Cisco recommends using the Cisco AIR-ANT5959 for 2.4 GHz and ANT5145V-R for 5 GHz for indoor voice applications. These two antennas provide the following advantages:

- Low gain omni-directional coverage and antenna diversity
- Decreased upward tilt angle, which reduces the coverage that may bleed through floor above, and also reduces the reflections that may come from air ducts and other metal objects above the ceiling tile
- Easy attachment to the T-bar on most ceiling tiles

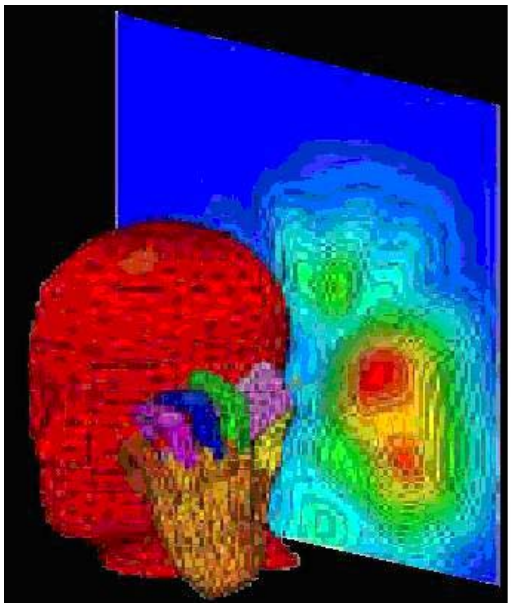
Higher gain antennas spread the signal on the horizontal plane, which creates a larger cell that also picks up more noise. This results in a lower signal-to-noise ratio (SNR), which increases the packet error ratio. SNR is defined by the following two criteria:

- Signal—The radiated energy transmitted from one radio that can be received uninterrupted by another radio. For Wi-Fi, this means that the transmitting radio is sending 802.11 protocol packets that the receiving radio is able to decode.
- Noise—Transmitted energy in the frequency range of the receiving radio that cannot be decoded by that radio.

The larger the difference in energy between the protocol packet and the background noise, the better the reception of the protocol packet and the lower the packet error rate and bit error rate. Coverage area design involves using channels to create the lowest possible packet error rate while maintaining a high call capacity.

Higher gain antennas can also reduce the number of calls on a Wi-Fi channel because of the increased coverage area. For voice, a ceiling-mounted antenna is preferred over a wall-mounted patch because the human head and body attenuate 5 dB of the signal (see Figure 9-1). Ceiling mounted antennas are better positioned to avoid more of this head and body attenuation than most wall-mounted antennas.

Figure 9-1 Head and Hand Attenuation



Antenna Positioning

Ceiling-mounted antennas typically have better signal paths to handheld phones. The recommended coverage cell size takes into consideration the signal loss because of the attenuation of the head and other obstacles. It is important to understand that the gain of antennas is reciprocal; gain applies equally to reception and transmission. Antenna gain is not an increase in transmitted power; the radio produces the transmitted power. The antenna is only a passive device. Gain is derived by focusing the signal of the radio into a direction, plane, and beam width, much in the same way a flashlight reflector focuses the light emanating from its bulb.

For a further discussion of WLAN RF planning, see Chapter 3, "WLAN Radio Frequency Design Considerations."

Handset Antennas

The Cisco Unified Wireless IP Phone 7920 and 7921G have antennas that extend from the main body of the phone. The way they are held in the hand does not significantly influence signal attenuation resulting from the hand.

For phones that integrate the antenna inside the body of the phone, the way the user holds the phone in the hand can influence signal attenuation by 4 dB. In some cases, a phone held against the head with the hand covering the antenna can result in a signal drop of 9 dB. The general rule for indoor deployments is that every 9 dB of signal loss reduces the coverage area in half. Figure 9-1 shows an example of the difference in radiating power from a handset when held to the head.

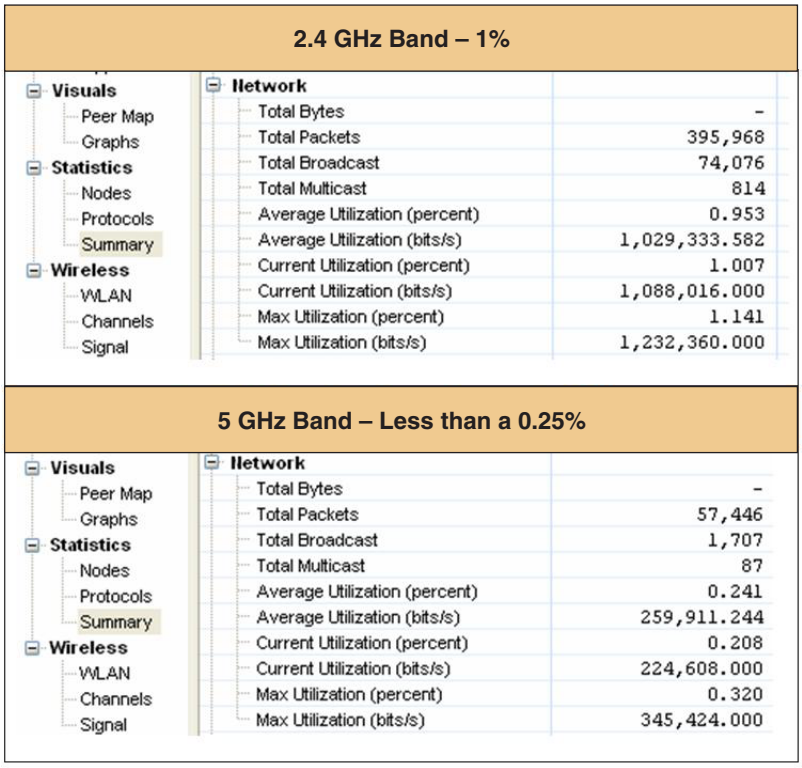
Handsets using the 2.4 GHz spectrum generally do not use diversity antennas because the 2.4 GHz wavelength is nearly five inches, so there is no practical antenna diversity option that can be implemented to improve signal reception. Therefore, the only improvement in link quality that can be achieved is at the AP. To provide optimum link quality between the phone and the AP, the AP needs to operate in its default configuration, which is with diversity enabled along with a diversity antenna.

Note that 802.11a handsets such as the Cisco 7921G do have a diversity antenna solution for the 11a radio.

Channel Utilization

The 802.11, 802.11b, and 802.11g standards use the same 2.4 GHz band. All must interoperate with each other, which introduces additional overhead reducing channel throughput. Many sites already have products using the Wi-Fi 2.4 GHz band. Additionally, there are many other products that use the same 2.4 GHz frequencies as used by Wi-Fi. Other products include Bluetooth, cordless phones, video game controllers, surveillance cameras, and microwave ovens. Because the 2.4 Ghz band is so "crowded", coupled with its channel allocation constraints, you should consider using the 5 GHz Wi-Fi band for new VoWLAN deployments. The channels available in 5 GHz are generally free of use at most sites (see Figure 9-2). Use of the UNII-2 channels for VoWLAN traffic requires the absence of radar. Cisco therefore recommends that there should be extra testing at any new site to see whether a channel in UNII-2 should be blocked out by configuration. The reason for this is that if an AP detects radar during normal use, it must leave the channel within ten seconds.

Figure 9-2 Typical Office Channel Utilization for 2.4 GHz and 5 GHz



Before the installation of the Cisco Unified Wireless Network, a site can be tested for channel interference and utilization with tools from AirMagnet, Wild Packets, Cognio, and others. The Wireless Control System (WCS) AP On-Demand Statistics Display report provides a spectrum review of the following:

- Noise by channel
- Interference by channel
- Client count versus RSSI
- Client count versus SNR
- Channel radar detection versus time

Dynamic Frequency Selection (DFS) and 802.11h Requirements of the APs

The Federal Communications Commission (FCC) of the United States, the European Telecommunications Standards Institute (ETSI), and other regulatory agencies have requirements regarding the use of radio frequencies. Portions of the 5 GHz band have been and are currently being used for radar, such as weather radar. Although most 5 GHz radar systems generally use higher frequencies with shorter wavelengths, there are still systems in place that overlap with some Wi-Fi UNII-2 bands. In 2006, the FCC opened the frequencies in the 5470–5725 MHz range to unlicensed use. With these additional frequencies came a requirement to maintaining an “interference-free” AP configuration. The AP must constantly monitor for radar pulses (typically from military, satellite, and weather stations), and must automatically switch to a “clean” channel if radar is detected.

When radar is detected, the system must do the following:

- Stop packet transmission within 200 ms
- Stop control transmissions within 10 seconds
- Avoid transmission on the channel for 30 minutes
- Scan the new channel for 60 seconds before transmission

Because of the radar requirements in the UNII-2, you should conduct a test for radar before going live with voice applications, because the required radar avoidance behavior may impact voice call quality. Cognio Spectrum Expert is also an excellent tool to test for the presence of radar. If radar is detected during such a test, the APs can then be configured to not use those channels.

Channels in the 5 GHz Band

Figure 9-3 shows the FCC 802.11a channel assignments. The DFS requirement includes the four original UNII-2 channels (52–64) and the new eight channels (100–116 and 132–140). The 5 GHz band now has 20 channels. These are non-overlapping channels, which means that they can all be co-located. 2.4 GHz has only three non-overlapping channels. A design allowing co-located channels in a coverage area aggregates the number calls obtainable in a coverage area.

Figure 9-3 802.11a Channel Allocation

Channel Identifier	36	40	44	48	52	56	60	64		149	153	157	161
Center Frequency	5180	5200	5220	5240	5260	5280	5300	5320		5745	5765	5785	5805
Band	UNII-1				UNII-2					UNII-3			

Channel Identifier	100	104	108	112	116	132	136	140
Center Frequency	5500	5520	5540	5560	5580	5660	5680	5700
Band	New UNII-2 Channels							

220339

See the Cisco website for compliance information and also check with your local regulatory authority to find out what is permitted within your country. The information provided in Table 3-2 and Table 3-3 should be used as a general guideline.

The channel-based design based on channels may be implemented to a single floor, as shown in Figure 9-4. In a multi-floor design, the channels can be separated between floors to reduce the possibility of co-channel interference.

Figure 9-4 Single Floor Channel Design

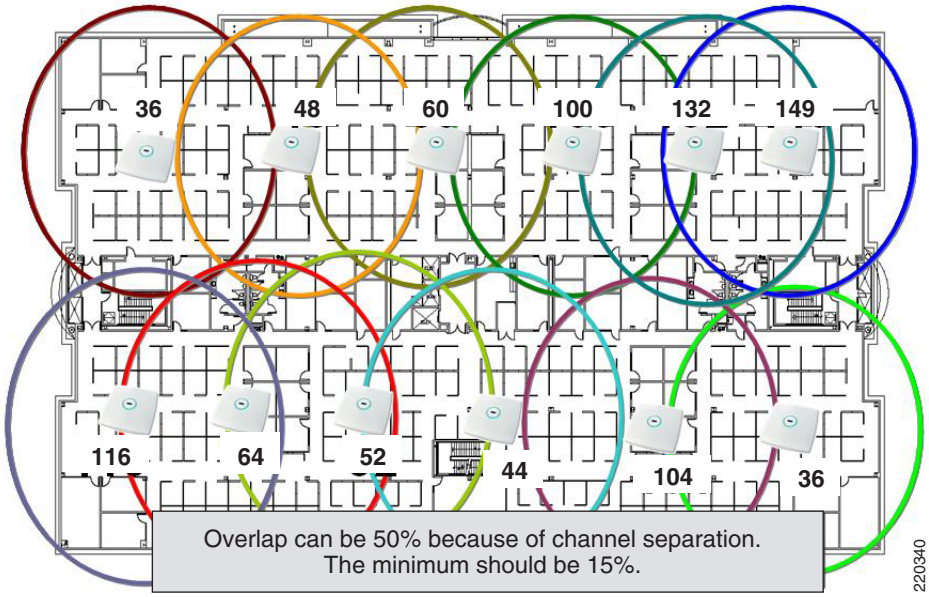
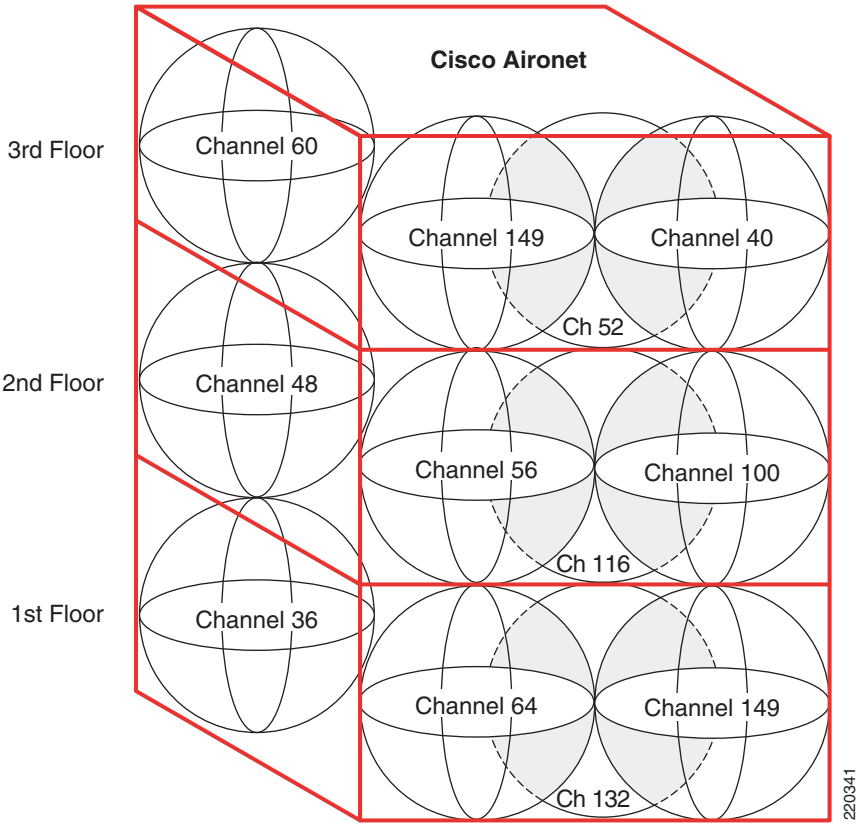


Figure 9-5 illustrates the vertical channel separation.

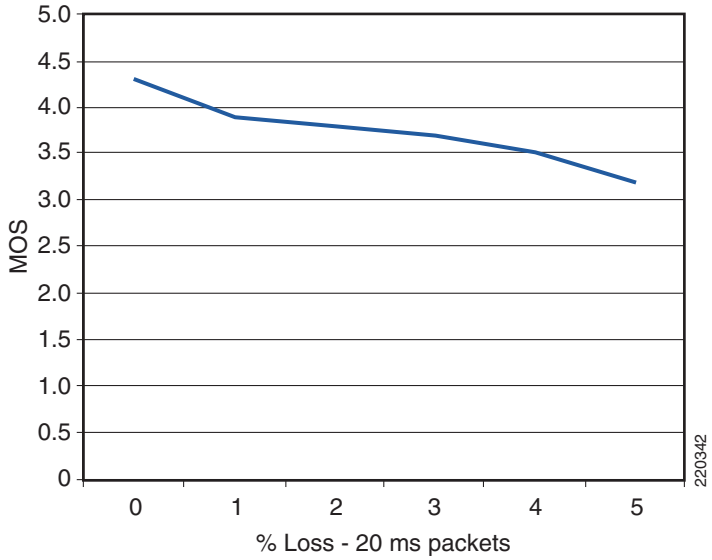
Figure 9-5 Vertical Channel Separation



Call Capacity

The number of calls on a Wi-Fi channel is limited by a number of factors. First, the media used by the AP and VoWLAN clients is the RF spectrum, which cannot be shielded from electromagnetic interference like shielded twisted-pair CAT 5 cable. The closest Wi-Fi comes to segmentation is channel separation. This open shared media of 802.11 creates the possibility for high packet loss. Most of this packet loss is addressed through retransmission of 802.11 frames, which in turn causes jitter. Figure 9-6 illustrates the packet loss relationship as a mean opinion score (MOS).

Figure 9-6 Effective Packet Loss Graphic



In 802.11a as well as 802.11g, the highest coverage range is achieved by the lowest data rate, which is 6 Mbps. The lowest packet error rate is also at 6 Mbps, for the same given power level.

An acceptable coverage area for voice is an area that maintains a packet error rate of 5 percent or less. The MOS scores are ranked as follows:

- 4.4—Top G.711 MOS score
- 4.3–4.0—“Very satisfied” to “satisfied”
- 4.0–3.6—“Some users satisfied”

Figure 9-6 shows that a packet error rate of 5 percent reduces the MOS to a level of “some users satisfied” quality of speech.

The coverage area edge for a phone is where the coverage area drops the MOS to the “very satisfied” category. This coverage area edge is referred to as a *cell edge* in this chapter. A cell edge with a 1 percent packet error rate is needed for voice because of the likelihood of multiple phone clients, data clients, co-channel interference, and other un-accounted for interferers. Cell edge and coverage design are defined in detail in other sections of this chapter.

If 802.11 and 802.11b are not required to support legacy 2.4 GHz Wi-Fi clients, Cisco recommends disabling the rates of 1, 2, 5.5, and 11. If those rates are disabled, one or more 802.11g data rates must be set to “required”. The data rate of 6 is generally the recommended data rate to be set to “required”, but this depends on the cell size design requirements, which may require using a higher bit rate. If possible, an 802.11g-only network is recommended rather than a 802.11b/g network. Most data clients and phone clients recognize the data rates advertised by the AP in its beacons and probe response.

Therefore, the clients send their management, control, multicast, and broadcast packets at the "required" data rates as advertised by the AP. The clients can send their unicast packets at any of the data rates advertised by the AP. Generally, those unicast packets are sent at a data rate that provides the highest reliable data rate for the link between the AP and client. The AP is capable of sending unicast packets at a data rate that is unique to each client link.

SNR is an important consideration for packet reception. The receiving radio is either the AP radio or the phone radio. The SNR is not likely to be the same at both radios of the link. SNR and multipath interference must be considered at the AP and at the coverage area edge. Path loss can be assumed to be the same at both ends of the link.

Cisco recommends for voice applications that the cell edge be determined by using the actual phone at the desired data rate. The voice packets sent between the AP and the phone in Wi-Fi applications are generally unicast RTP G711 packets with a typical size of 236 bytes. The Real-Time Transport Protocol (RTP) packet is based on UDP and IP protocols, and therefore RTP is connectionless. The signal strength, SNR, data rate, and error rates of the phone call can be seen from the AP statistics, either on the standalone AP or the Lightweight Access Point Protocol (LWAPP) controller. A sample of a phone client's cell edge dBm values for 802.11g and 802.11a are shown in Figure 9-7 and Figure 9-8. The call stream statistics are shown in Figure 9-9. The stream metrics can be viewed on the WCS after the voice metrics are enabled. The path to enable the metrics is Configure > Controller > ipaddress > 802.11bg > Voice Parameters > Enable Voice Metrics.

Figure 9-7 11g Client Statistics

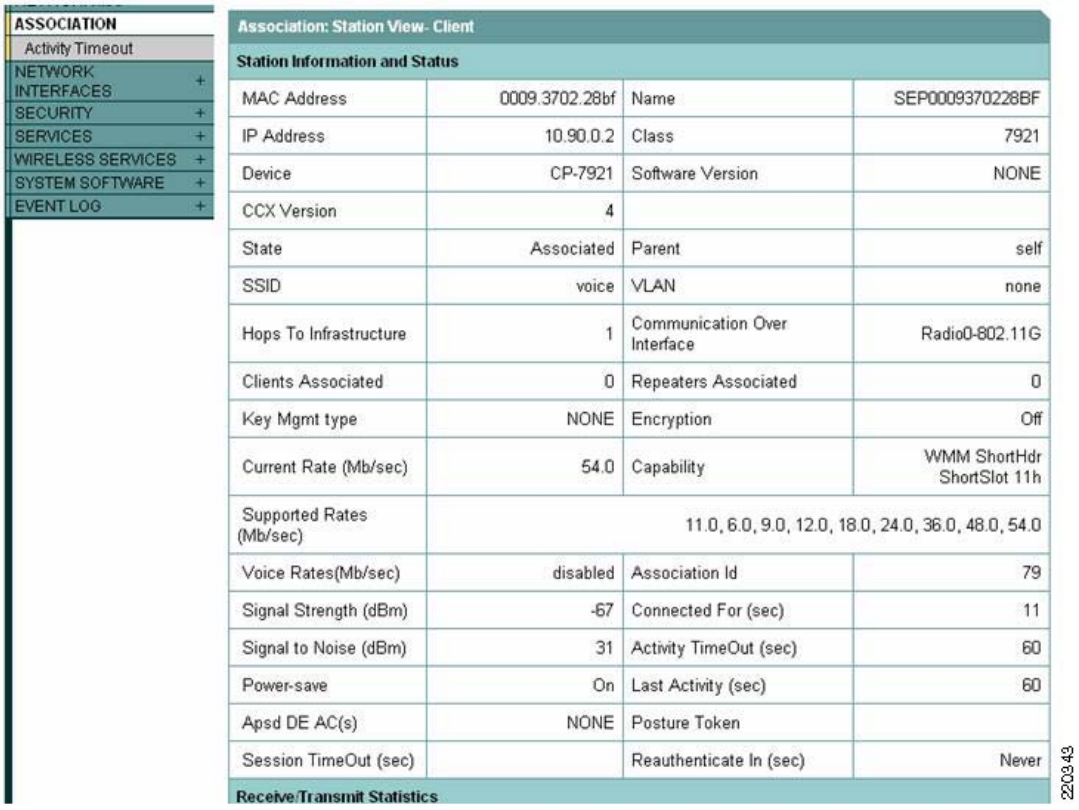


Figure 9-8 11a Client Statistics

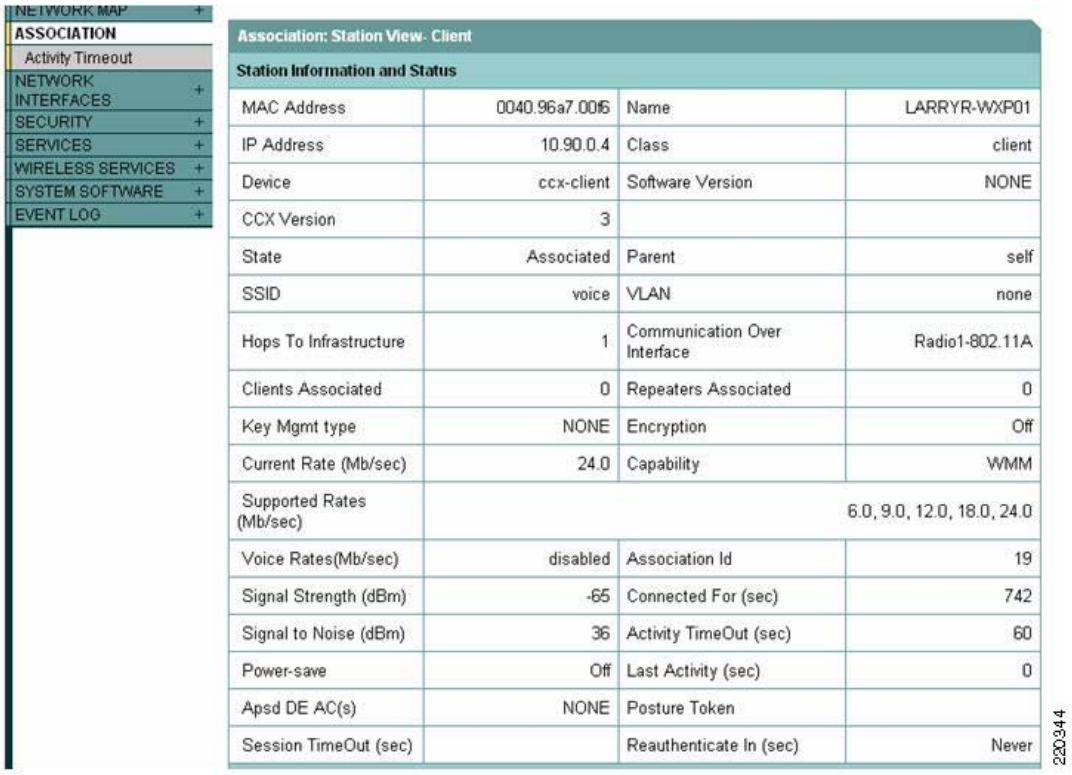
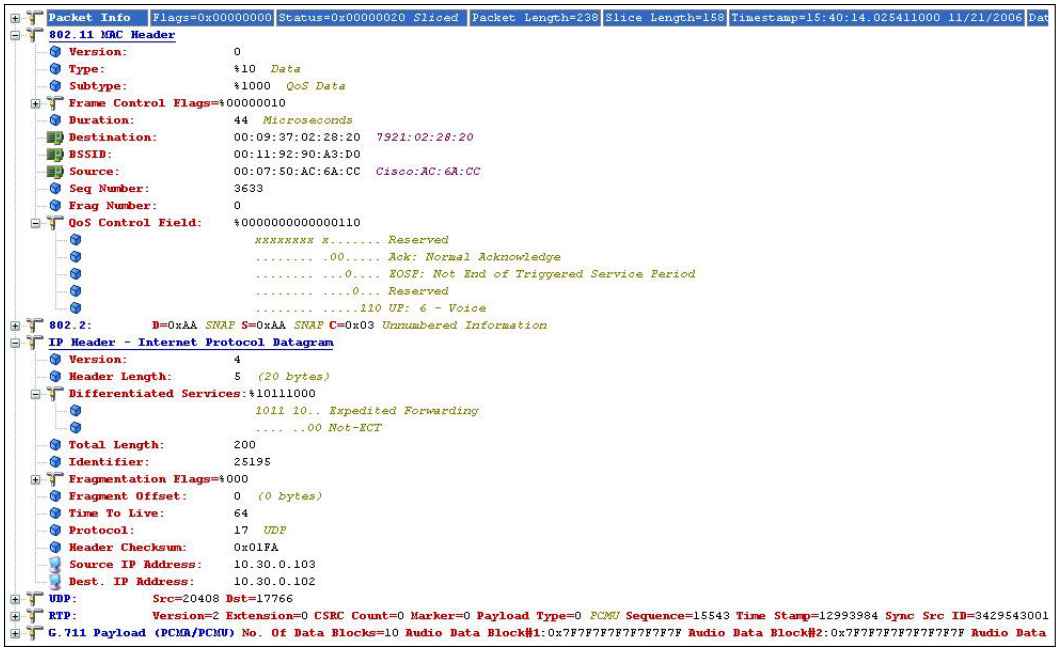


Figure 9-9 WLC Call Metrics

A decoded RTP packet is shown in Figure 9-10. The packet is originated by a 7960 phone. The over-the-air QoS marking is changed from the QoS baseline marking of 5 to a user priority of 6, which follows the 802.11e specification. Call statistics on the Cisco 7920 and 7921 phones can be viewed on the phone or by browsing into the phone using the IP address of the phone. After that cell edge is determined by testing with an actual phone, those numbers can then be adapted, using more automated tools, to complete the coverage design for the site.

Figure 9-10 Sample VoWLAN Capture



When multipath interference is present at a location where signal level measurements are being taken, it is quite likely that the reported values will fluctuate from packet to packet. A packet may be as much as 5 dB higher or lower than the previous packet. It may take several minutes to obtain an average value for a given measurement location.

AP Call Capacity

A key part of the planning process for a VoWLAN deployment is to plan the number of simultaneous voice streams per AP. When planning the voice stream capacity of the AP, consider the following points:

Note A call between two phones associated to the same AP counts as two active voice streams.

- The utilization of an unlicensed (shared) 802.11 channel is the real determinant for the number of simultaneous voice streams an AP may carry.
- Because the channel utilization and AP performance determine the number of voice streams, same channel and next channel separation are very important. Two APs in the same location, operating on the same channel do not provide double the number of voice streams. In fact, there can be fewer voice streams than one AP would provide.
- Cell capacity or bandwidth determines the number of voice streams that can be simultaneously conducted.
- The handset QoS features supported in the handsets and VoWLAN deployment should be considered.

- Various handsets have different WLAN QoS features and capabilities that impact the features that are enabled in the WLAN deployment, and ultimately determine the per-AP call capacity of the AP. Most VoWLAN handsets provide guidance on the number of calls per AP supported by that phone; this should be considered a best case figure for situations where the handset is able to use its optimal QoS features and has full access to the channel capacity.

The actual number of voice streams a channel can support is highly dependent on a number of issues, including environmental factors and client compliance to WMM and the Cisco Compatible Extension specifications. Figure 9-11 shows the Cisco Compatible Extension specifications that are most beneficial to call quality and channel capacity. Simulations indicate that a 5 GHz channel can support 14–18 calls. This means a coverage cell can include 20 APs, each operating on different channels, with each channel supporting 14 voice streams. The coverage cell can support 280 calls. The number of voice streams supported on a channel with 802.11b clients is 7; therefore, the coverage cell with three APs on the three non-overlapping channels supports 21 voice streams.

Figure 9-11 Cisco Compatible Extension VoWLAN Features

How Cisco Compatible Extensions Benefits VoWLAN Call Quality	
Feature	**Benefit**
CCKM Support for EAP-Types	Locally Cached Credentials Means Faster Roams
Unscheduled Automatic Power Save Delivery (U-APSD)	More Channel Capacity and Better Battery Life
TSPEC-Based Call Admission Control (CAC)	Managed Call Capacity for Roaming and Emergency Calls
Voice Metrics	Better and More Informed Troubleshooting
Neighbor List	Reduced Client Channel Scanning
Load Balancing	Calls Balanced Between APs
Dynamic Transmit Power Control (DTPC)	Clients Learn a Power to Transmit At
Assisted Roaming	Faster Layer 2 Roams

220352

Figure 9-11 shows the following:

- Cisco Centralized Key Management (CCKM) provides for faster client roaming for Extensible Authentication Protocol (EAP)-authenticated client, which benefits call quality.
- Call Admission Control (CAC) also benefits call quality and can create bandwidth reservation for E911 and roaming calls.
- Assisted Roaming and Neighbor List benefit call quality and battery life.
- Voice Metrics can benefit management.
- Unscheduled Automatic Power Save Delivery (U-APSD) and Dynamic Transmit Power Control (DTPC) benefit battery life.
- Load balancing and DTPC benefit call quality.

Several of the Cisco Compatible Extensions features have more than one benefit.

The amount of buffer memory, CPU speed, and radio quality are key factors of the performance of an AP radio. QoS features prioritize the voice and data traffic in the channel. For a further discussion of QoS, see Chapter 5, "Cisco Unified Wireless QoS."

The 802.11e, WMM, and Cisco Compatible Extension specifications help balance and prevent the overloading of a cell with voice streams. CAC determines whether there is enough channel capacity to start a call; if not, the phone may scan for another channel. The primary benefit of U-ASPD is the preservation of WLAN client power by allowing the transmission of frames from the WLAN client to trigger the forwarding of client data frames that are being buffered at the AP for power saving purposes. The Neighbor List option provides the phone with a list that includes channel numbers and channel capacity of neighboring APs. This is done to improve call quality, provide faster roams, and improve battery life.

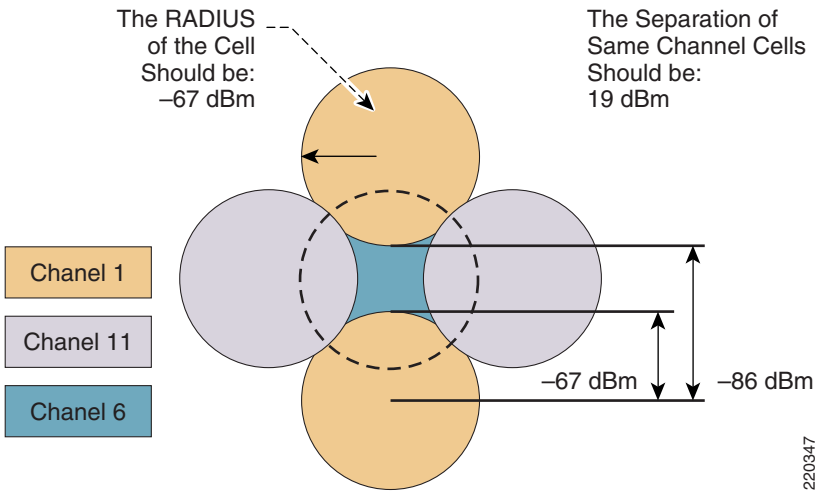
For a further discussion of U-APSD and CAC, see Chapter 3, "WLAN Radio Frequency Design Considerations."

Cell Edge Design

Guidelines for deploying 802.11b/g/a VoWLAN handsets recommend a design where a minimum power of -67 dBm is present at the cell boundary (see Figure 9-12). This practice creates cell sizes that are smaller than those used in data WLAN designs of the past. The -67 dBm threshold is a general recommendation for achieving a packet error of one percent, which requires an SNR value of 25 dB or greater (local noise conditions impact this requirement). Therefore, when determining the likely channel coverage area for a particular phone type, both signal strength and noise, measured at the phone, must be verified using the client statistics offered through the AP. See Figure 9-8 and Figure 9-11 for determining these values on the standalone and LWAPP APs.

The -67 dBm signal strength measurement has been used by 802.11b phone vendors for a number of years, and tests indicate that this same rule of thumb measurement also works well for 802.11g and 802.11a phone clients.

Figure 9-12 Cell Edge Measurements



Note The -86 dBm separations shown in Figure 9-12 is simplified and is considered ideal. It is very unlikely that this 19 dBm of separation can be achieved in most deployments. The most important RF design criteria are the -67 dBm cell radius, and the 20 percent recommended overlap between cells. Designing to these constraints optimizes channel separation.

For 5 GHz cells, there is less concern about same channel separation because of the number of available channels. There are 20 channels in 802.11a, so a two-channel separation is almost always possible, in contrast to the 2.4 GHz band where there are only three channels that do not overlap in frequency.

For both 5 GHz and 2.4 GHz, the cell edge needs to be at the floor level where a packet error rate of 1 percent is maintained at the highest data rate desired for a given channel. In the case of 802.11b, that data rate is 11 Mbps. Thus, from the center of the AP location to a point on the floor where the phone signal is seen by the AP, the cell edge is -67 dBm.

802.11g and 802.11a phone clients may be capable of rates up to 54 Mbps. Current chip sets support 54 Mbps, but transmit power capabilities do differ. Cisco highly recommends that all links between phone clients and APs be established using matching transmit power levels. (see Dynamic Transmit Power Control, page 9-14).

Coverage cells can be created for specific data rates. For a high density deployment or a deployment where a large number of calls are required within a small floor space, 802.11a is recommended because of the number of channels and the 54 Mbps data rate. The lower data rates in 802.11a can be disabled, the 24 Mbps data rate can be set to “required”, while the rates of 36 to 54 can be left enabled.

After setting the cell edge of -67 dBm, determine where the error rate of 1 percent occurs, and then examine the SNR value.

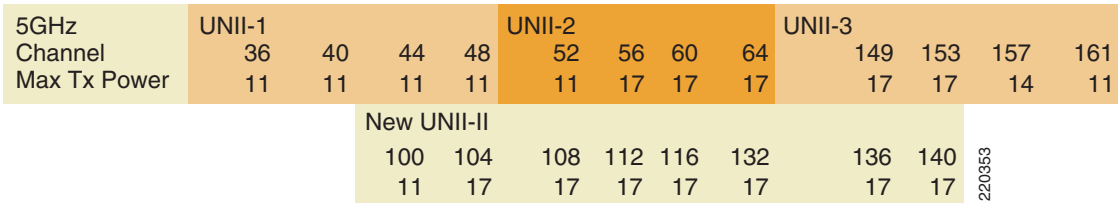
The -67 dBm cell edge may be determined as follows:

- Set the phone to its desired transmit power.
- Set the AP to a matching transmit power.
- Place the AP and the desired antenna in the location where the phone will be used.
- With an active call, or while sending and receiving packets equal in size to the G711 codec, measure the signal level out to the –67 dBm cell edge.

Carefully examine the data sheets of the particular phone device to determine the transmit power levels and data rates supported by the phone device in a particular Wi-Fi band. The data sheets for Cisco Unified Wireless IP Phones can be found at http://www.cisco.com/en/US/products/hw/phones/ps379/index.html. Consult the vendor website for phones from other vendors.

The 80211a maximum transmit power levels vary on different channels and with different AP models. The 802.11g maximum transmit power levels vary by model. Cisco Aironet AP data sheets should be carefully examined to determine which AP model supports which data rates. Figure 9-13 shows an example of the maximum 802.11a transmit power in dBm by channel.

Figure 9-13 Channel Power Assignment



The maximum permissible transmit power across the 5 GHz band varies by as much as 6 dB. This means that when using the maximum allowed transmit power throughout a site that allows all channels, there will not be equal cell coverage on all channels. It also means that if dynamic channel selection is used, the cell coverage edge may change based on the channel number. However, dynamic channel selection can be tuned (see Chapter 3, "WLAN Radio Frequency Design Considerations.") The default mode of dynamic channel selection accounts for the difference of maximum transmit power level by channel.

Cell transmit power on all APs should not exceed the maximum or desired transmit power of the phone. If the phones maximum or set transmit power is 13 dBm, Cisco recommends that all APs have a maximum transmit power of 13 dBm. Therefore, the maximum transmit power on the AP should be set to an equal level or, if not possible, the next higher transmit power level. Equal transmit power is recommended to avoid one-way audio. The AP generally has better receiver sensitivity and diversity support than the phone, so it should be able to receive the slightly lower strength phone signal. See Dynamic Transmit Power Control, page 9-14 for more information on equal transmit powers.

Dual Band Coverage Cells

Chapter 3, "WLAN Radio Frequency Design Considerations," illustrates 2.4 GHz and 5 GHz band channel coverage design. For a dual mode AP to provide equal cell coverage on both the 2.4 GHz channel and the 5 GHz channel, the 2.4 GHz channel must have an equal (or more likely lower) transmit power than the 5 GHz channel. At most sites, the noise level in the SNR formula will be lower by perhaps 10 dB. The receiver sensitivity of 802.11g radios is generally 2 dBm better than the same data rate on the 11a radio. As an example, the data sheet for the 7921G has the receive sensitivity of -78 dBm at the data rate of 36 Mbps for 802.11g, and -76 dBm for 802.11a. Therefore, given the anticipated better noise floor of 10 dB, the 802.11a cell can do better by 8 dBm. Other details such as the difference in path loss between 802.11g and 802.11a keep this from being a direct ratio. However, if the same coverage cells are desired, reducing the 802.11g network by one or two power levels from the 11a network should accomplish this goal.

Dynamic Transmit Power Control

Cisco Aironet APs by default have DTPC enabled. DTPC is automatic with Wireless LAN Controllers and is configurable on the standalone APs. Clients need to support a minimum of Cisco Compatible Extension v2 capabilities to use DTPC.

DTPC accomplishes the following:

- Sets the phones transmit power to match the transmit power of the AP
- The AP advertises its transmit power for the clients to learn
- Prevents one-way audio; that is, RF traffic is only being heard in one direction

DTPC allows the phone to automatically adjust its transmit power to that of the APs. In the example shown in Figure 9-14, this means that the phone changes its transmit from 5 mW to 100 mW.

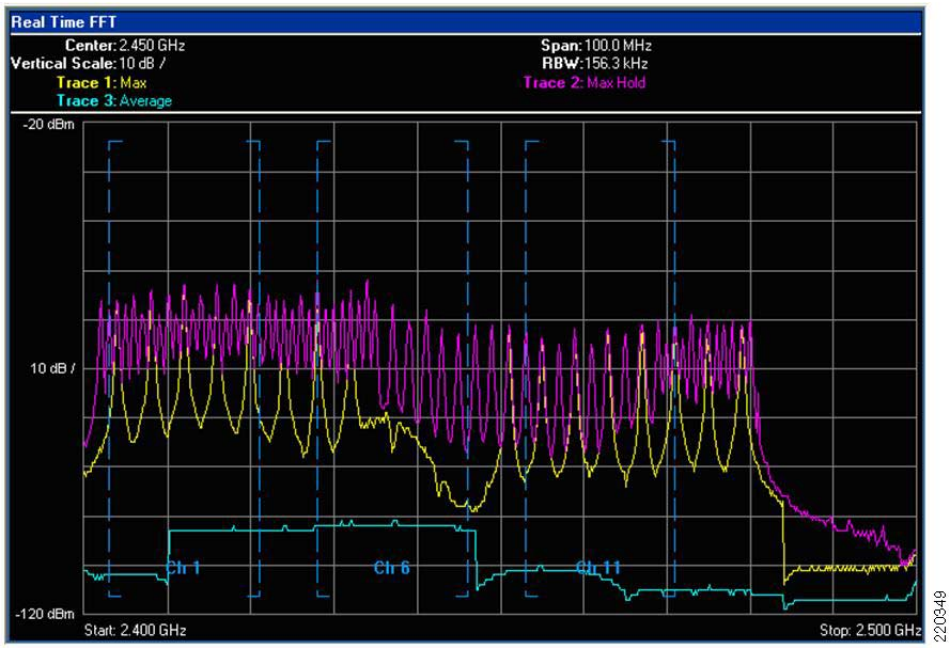
Figure 9-14 Client and AP Power Matching

The licensing requirements of 802.11g and 802.11a mean that clients do not have 100 mW transmit powers. Cisco highly recommends that the maximum configured transmit power on the access be no higher than the client phone devices hardware supports. A phone with a slightly lower transmit power than the AP is better than the AP using less power than the phone, but having matching transmit powers lessens the likelihood of one-way audio (the typical user experience of "can you hear me…. I can't hear you").

Interference Sources Local to the User

Interference can be local to the user, but is also likely to affect nearby users. Bluetooth (BT) is a popular RF protocol used in personal area networks that interferes with Wi-Fi 2.4 GHz channels. Figure 9-15 shows that the actual BT signal does span all the 2.4 GHz channels used by 802.11b/g clients. This graphic is taken from an 802.11g call with a BT headset linked to the phone. Figure 9-16 also shows the jitter caused by the BT headset.

Figure 9-15 Bluetooth (BT) Signal Pattern in the 802.11b/g 2.4 GHz Spectrum of a Typical BT Earpiece

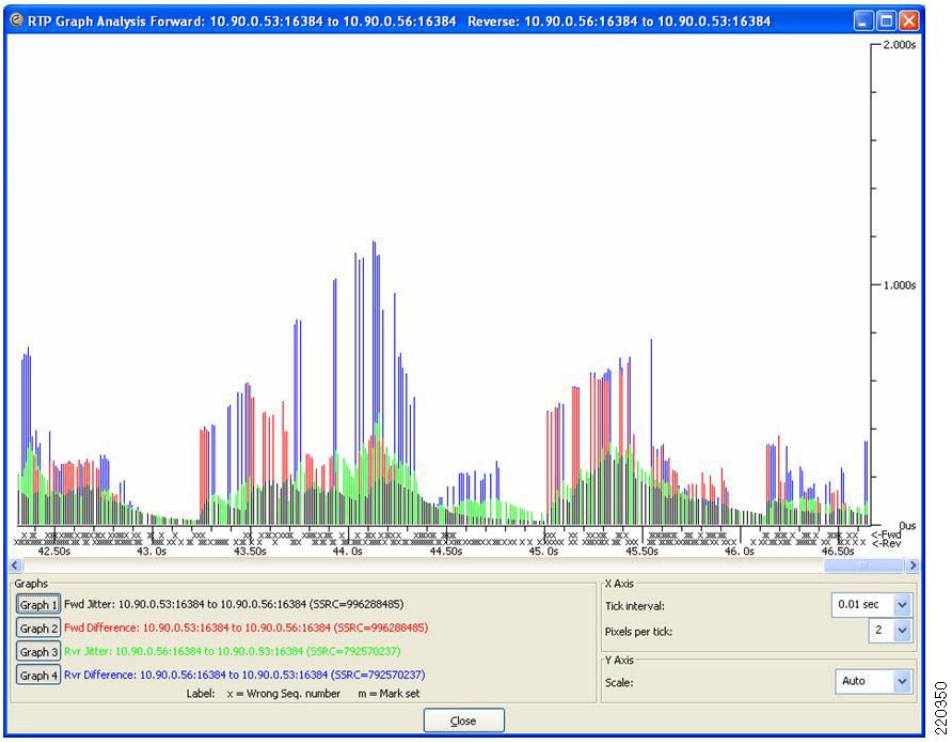


The **PINK** is the Max Hold line, or the line that shows the maximum transmit power that was reached during the test. The **YELLOW** shows the maximum transmit power in the last sample period of ten seconds. The **TURQUOISE** shows the average transmit power over the period of the test. The **vertical dashed** lines separate the three non-overlapping 802.11b/g channels **Ch1, Ch6,** and **Ch11.** The charting is from 2.400 GHz on the left to 2.500 GHz on the right. From the right edge of the Ch11 vertical blue line is the part of the 802.11 spectrum used in Europe and Japan. This capture was done with an AP and clients configured for the North American regulatory domain. This graph shows that the BT earpiece was easily transmitting outside of FCC regulations.

Notice that the BT signal is very narrow. BT transmits data on a single MHz of frequency, stops the transmission, moves to another frequency in the 802.11 2.4 GHz band, and then transmits data. This is repeated continually. The 802.11b and 802.11g signals are sent with a combined 22 MHz of frequency. The radio remains on that 22 MHz of frequency. This grouping of 22 MHz is referred to as the channel. The Max Hold line shows how strong the BT is while in search mode. The signal level is above that of a 50 mW (17 dBm) OFDM 802.11g radio. A signal of this strength and duration causes 802.11b/g phones to drop the VoWLAN call. Lesser strength BT signals cause jitter, resulting in a lower MOS value.

Figure 9-16 shows an example of an Ethereal jitter analysis of three simultaneous phone calls, each using a BT earpiece.

Figure 9-16 Jitter Analysis Example



All three calls were on the same AP, and were calls to other phones on this AP.

CHAPTER 10

Cisco Unified Wireless Guest Access Services

The introduction of Wireless LAN (WLAN) technologies in the enterprise has changed the way corporations and small-to-medium businesses function by freeing staff and network resources from the constraints of fixed network connectivity.

WLAN has also changed how individuals access the Internet and their corporate networks from public locations. The advent of public WLAN (hotspots) has caused mobile workers to become accustomed to being able to access their corporate network from practically anywhere.

Introduction

The paradigm of public access has extended to the enterprise itself. Long gone is the scenario where it was sufficient for a company to provide its partners, visitors, and guests with a place to sit along with an outside line with which to make phone calls. Our highly mobile, information-on-demand culture requires on-demand network connectivity. A half-day spent at a partner or customer venue without access to one's own network resources can impact the productivity of a meeting, service or sales call, and reduce the overall personal productivity of an individual who is away from their office. For this reason, enterprise guest access services are becoming increasingly important and a necessity in the corporate environment.

While there is broad recognition that guest networking is becoming increasingly important, there is also well-founded apprehension over how one safeguards their internal company information and infrastructure assets. Ironically, unbeknownst to many enterprises, their network might already play host to guests who, in an uncontrolled manner, find ways to access the Internet via improperly implemented wired or wireless networks. These guests are not hackers in the true sense, but otherwise well-intentioned individuals trying to get their jobs done. So, on the surface, while it might sound risky to implement a guest access solution, when implemented correctly, an enterprise that implements a guest access solution will most likely improve their overall security posture as a result of the network audits associated with the implementation process.

In addition to overall improved security, implementing a guest access network offers these additional general benefits:

- Authentication and authorization control of guests based on variables including date, duration, and bandwidth
- An audit mechanism to track who is currently using, or has used, the network

Additional benefits of a wireless-based guest access include the following:

- It provides wider coverage by including areas such as lobbies and other common areas that otherwise might not have been wired for network connectivity.
- It removes the need for designated guest access areas or rooms.

Scope

Several architectures can be implemented to offer guest access in the enterprise. It is not the goal of this chapter to cover all possible solutions. Instead, this chapter focuses on the implementation of wireless guest networking using the Cisco Unified Wireless solution. For more information on deploying wired and wireless Guest Access services in other topology scenarios, see the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Network_Virtualization/GuestAcc.html.

Wireless Guest Access Overview

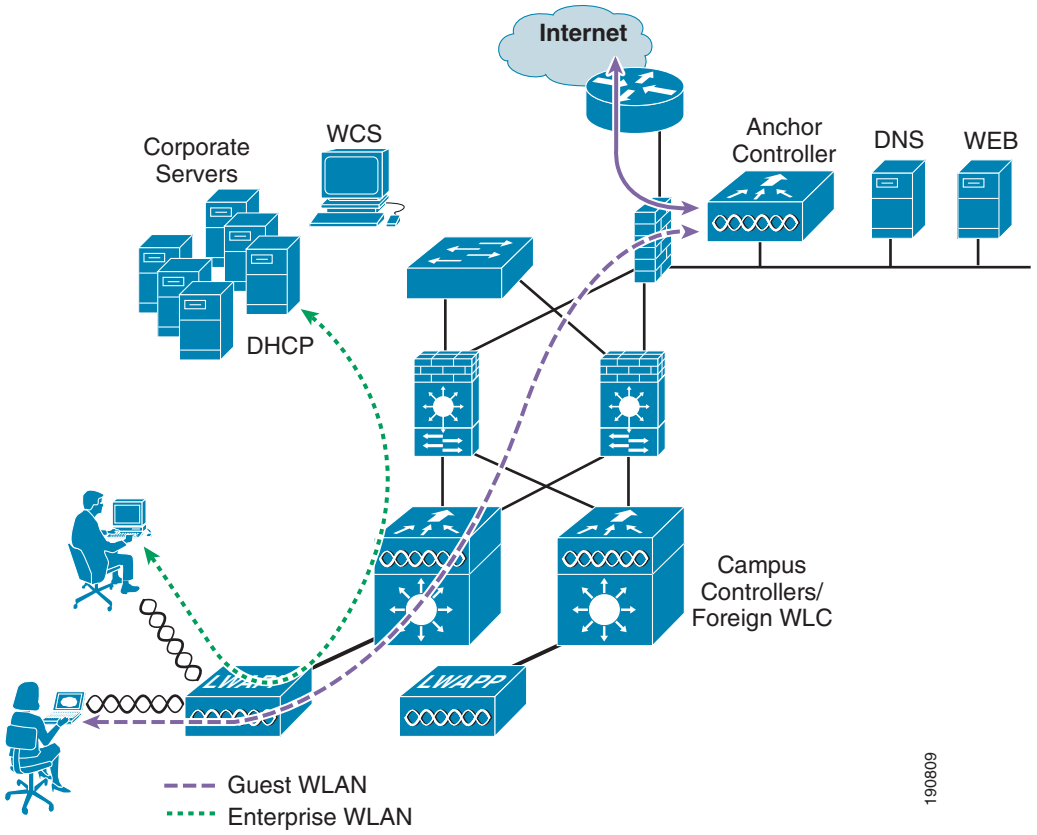
Ideally, the implementation of a wireless guest network uses as much of an enterprise's existing wireless and wired infrastructure as possible to avoid the cost and complexity of building a physical overlay network. Assuming this is the case, the following additional elements and functions are needed:

- A dedicated guest WLAN/SSID—Implemented throughout the campus wireless network wherever guest access is required.
- Guest traffic segregation—Requires implementing Layer 2 or Layer 3 techniques across the campus network to restrict where guests are allowed to go.
- Access control—Involves using imbedded access control functionality within the campus network or implementing an external platform to control guest access to the Internet from the enterprise network.
- Guest user credential management—A process by which a sponsor or lobby administrator can create temporary credentials in behalf of a guest. This function might be resident within an access control platform or it might be a component of AAA or some other management system.

Guest Access using the Cisco Unified Wireless Solution

The Cisco Unified WLAN solution offers a flexible, easy-to-implement method for deploying wireless guest access by using Ethernet in IP (RFC3378) within the centralized architecture. Ethernet in IP is used to create a tunnel across a Layer 3 topology between two WLC endpoints. The benefit of this approach is that there are no additional protocols or segmentation techniques that must be implemented to isolate guest traffic from the enterprise. See Figure 10-1 for an example of guest access topology using a centralized WLAN architecture.

Figure 10-1 Centralized Controller Guest Access



As shown in Figure 10-1, a WLC is located in the enterprise DMZ where it performs an "anchor" function. This anchor controller is responsible for terminating EoIP tunnels that originate from other campus WLCs throughout the network. These "foreign" controllers are responsible for termination, management, and standard operation of the various WLANs provisioned throughout the enterprise, including one or more guest WLANs. Guest WLANs, instead of being switched locally to a corresponding VLAN, are instead transported via an EoIP tunnel to the anchor controller. Specifically, guest WLAN data frames are encapsulated using LWAPP from the AP to the foreign controller and then encapsulated in EoIP from the foreign WLC to a guest VLAN defined on the anchor WLC. In this way, guest user traffic is forwarded to the Internet transparently, with no visibility by, or interaction with, other traffic in the enterprise.

WLAN Controller Guest Access

The WLC Guest Access solution is self-contained and does not require any external platforms to perform access control, web portal, or AAA services. All these functions are configured and run within the anchor controller. However, the option exists to implement one or all of these functions externally and will be discussed later in the chapter.

Supported Platforms

The anchor function, which includes tunnel termination, web authentication, and access control is supported on the following WLC platforms (using version 4.0 and later software images):

- Cisco 4400 Series
- Cisco 6500 Series (WISM)
- Cisco 3750 with integrated WLC

The following WLC platforms cannot be used for anchor functions, but can be used for standard controller deployments and guest mobility tunnel origination (foreign WLC) to a designated anchor controller(s):

- Cisco WLAN Controller Module for Integrated Service Routers (ISR)
- Cisco 2100 Series

Auto Anchor Mobility to Support Wireless Guest Access

Auto anchor mobility, or guest WLAN mobility, is a key feature of the Cisco Unified Wireless solution. It offers the ability to map a provisioned guest WLAN to one or more (anchor) WLCs by using an EoIP tunnel. Auto anchor mobility allows a guest WLAN and all associated guest traffic to be transported transparently across an enterprise network to an anchor controller that resides in the Internet DMZ (see Figure 10-2).

Figure 10-2 Auto Anchor EoIP Tunnels

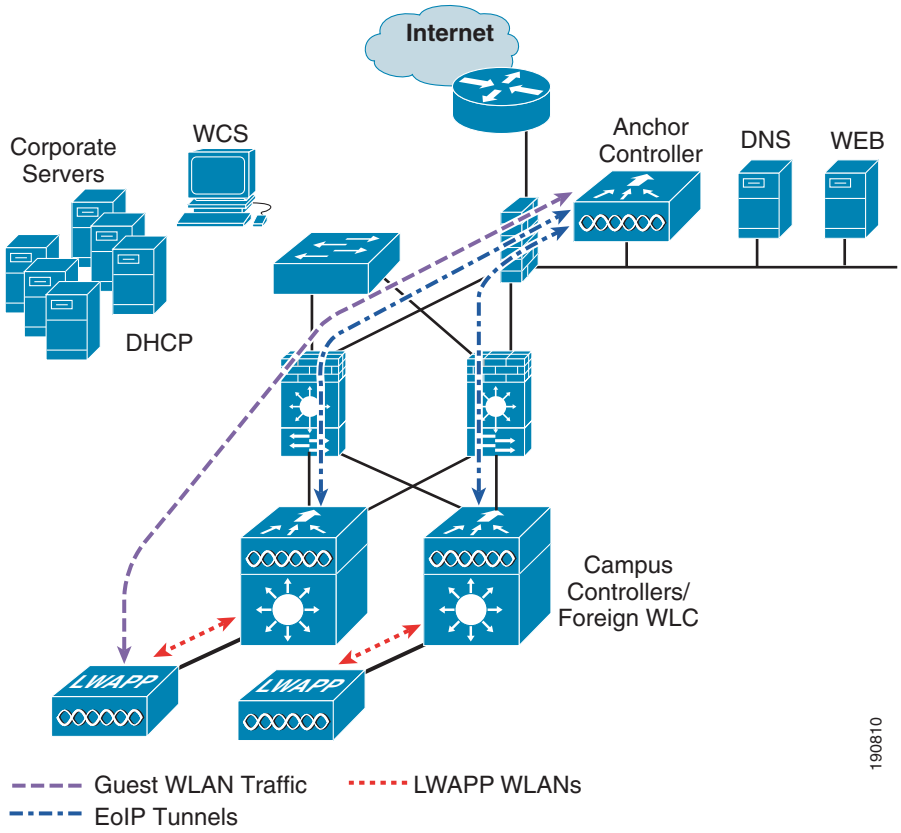
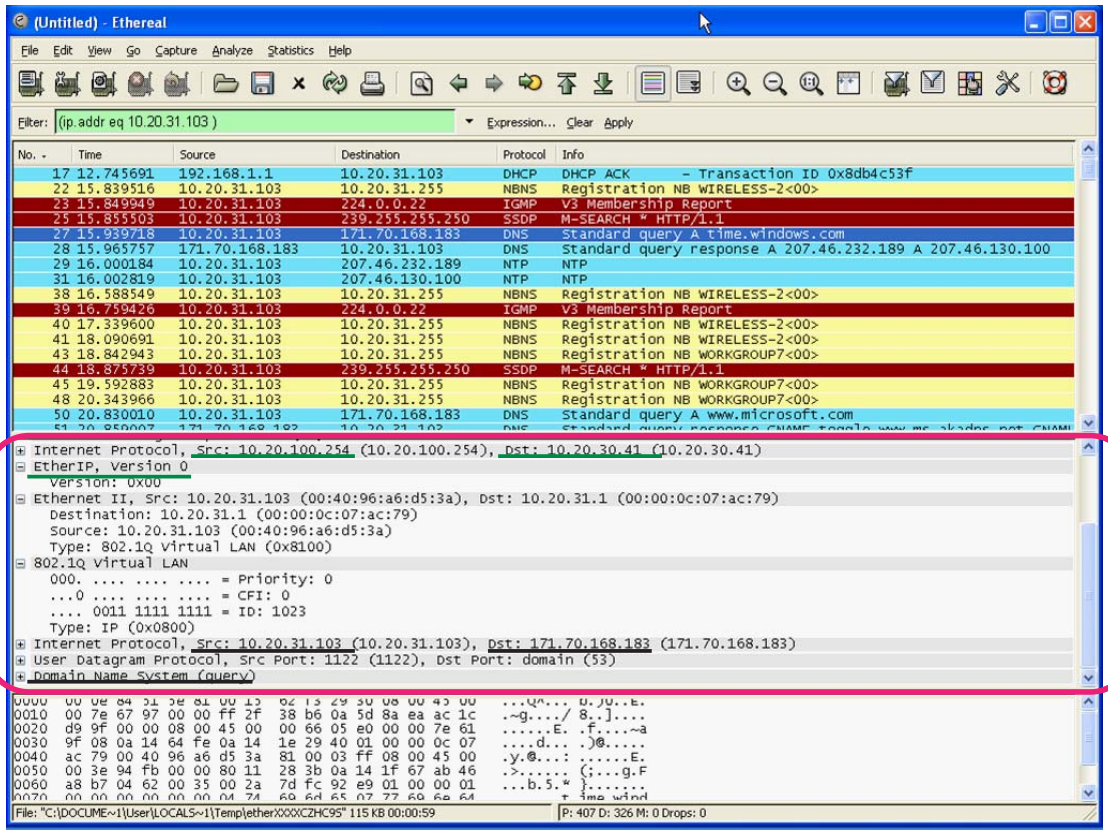


Figure 10-3 shows a sniffer trace of an Ethernet in IP tunnel (highlighted) between a foreign controller with a guest WLAN provisioned and an anchor controller that is performing local web authentication. The first IP detail shown represents the Ethernet in IP tunnel between the foreign and anchor controllers. The second IP detail is that of guest traffic (in this case, a DNS query).

Figure 10-3 Sample Ethernet in IP Sniffer Trace



Anchor Controller Deployment Guidelines

This section provides guidelines for deploying an anchor controller to support wireless guest access.

Anchor Controller Positioning

Because the anchor controller is responsible for termination of guest WLAN traffic and subsequent access to the Internet, it is typically positioned in the enterprise Internet DMZ. In doing so, rules can be established within the firewall to precisely manage communications between authorized controllers throughout the enterprise and the anchor controller. Such rules might including filtering on source or destination controller addresses, UDP port 16666 for inter-WLC communication, and IP protocol ID 97 Ethernet in IP for client traffic. Other rules that might be needed include the following:

- TCP 161 and 162 for SNMP
- UDP 69 for TFTP
- TCP 80 or 443 for HTTP, or HTTPS for GUI access
- TCP 23 or 22 for Telnet, or SSH for CLI access

Depending on the topology, the firewall can be used to protect the anchor controller from outside threats.

For the best possible performance and because of its suggested positioning in the network, it is strongly recommended that the guest anchor controller be dedicated to supporting guest access functions only. In other words, the anchor controller should not be used to support guest access in addition to controlling and managing other LWAPP APs (LAPs) in the enterprise.

DHCP Services

As previously described, guest traffic is transported at Layer 2 via EoIP. Therefore, the first point at which DHCP services can be implemented is either locally on the anchor controller or the controller can relay client DHCP requests to an external server. See Guest Access Configuration, page 10-14 for configuration examples.

Routing

Guest traffic egress occurs at the anchor controller. Guest WLANs are mapped to a dynamic interface/VLAN on the anchor. Depending on the topology, this interface might connect to an interface on a firewall, or directly to an Internet border router. Therefore, a client's default gateway IP is either that of the firewall or the address of a VLAN/interface on the first hop router. For ingress routing, it is assumed the guest VLAN is directly connected to a DMZ interface on a firewall or to an interface on a border router. In either case, the guest (VLAN) subnet is known as a directly connected network and advertised accordingly.

Anchor Controller Sizing and Scaling

The most cost-effective platform to support guest networking in most enterprise deployments is the Cisco 4400 Series controller. Assuming the controller is being deployed to support guest access with EoIP tunnel termination only, the 4402 with support for 12 APs is sufficient because it is assumed the controller is not going to be used to manage LAPs in the network.

A single 4400 Series controller can support EoIP tunnels from up to 40 foreign controllers within the enterprise. Additionally, the 4400 supports up to 2500 simultaneous users and has a forwarding capacity of 2 Gbps.

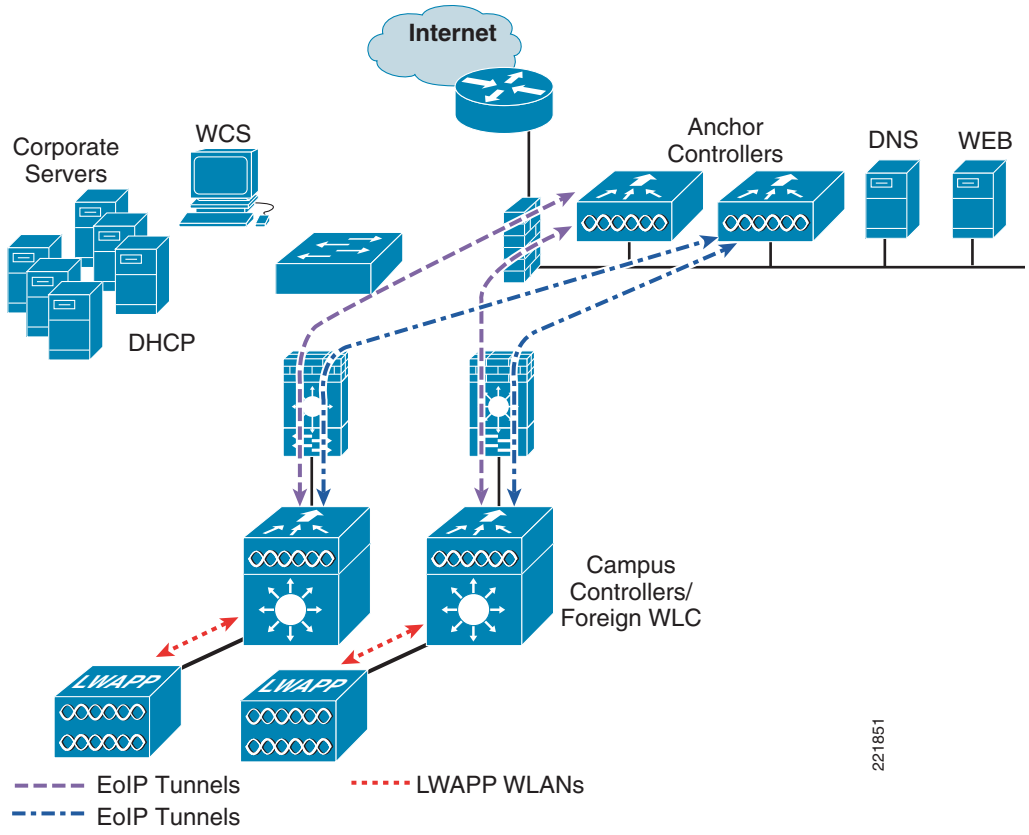
Anchor Controller Redundancy

Beginning with Release 4.1 of Unified Wireless solution software, a "guest N+1" redundancy capability was added to the auto anchor/mobility functionality. This new feature introduces an automatic ping function that enables a foreign controller to proactively ping anchor controllers to verity control and data path connectivity. In the event of failure or an active anchor becomes unreachable, the foreign controller does the following:

- Automatically detects that the anchor has become unreachable
- Automatically disassociates any wireless clients that were previously associated with the unreachable anchor
- Automatically re-associates wireless client(s) to an alternate anchor WLC

With guest N+1 redundancy, two or more anchor WLCs can be defined for a given guest WLAN. Figure 10-4 shows a generic guest access topology with anchor controller redundancy.

Figure 10-4 Guest Access Topology with Guest Anchor N+1 Redundancy



Keep in mind the following with regard to guest N+1 redundancy:

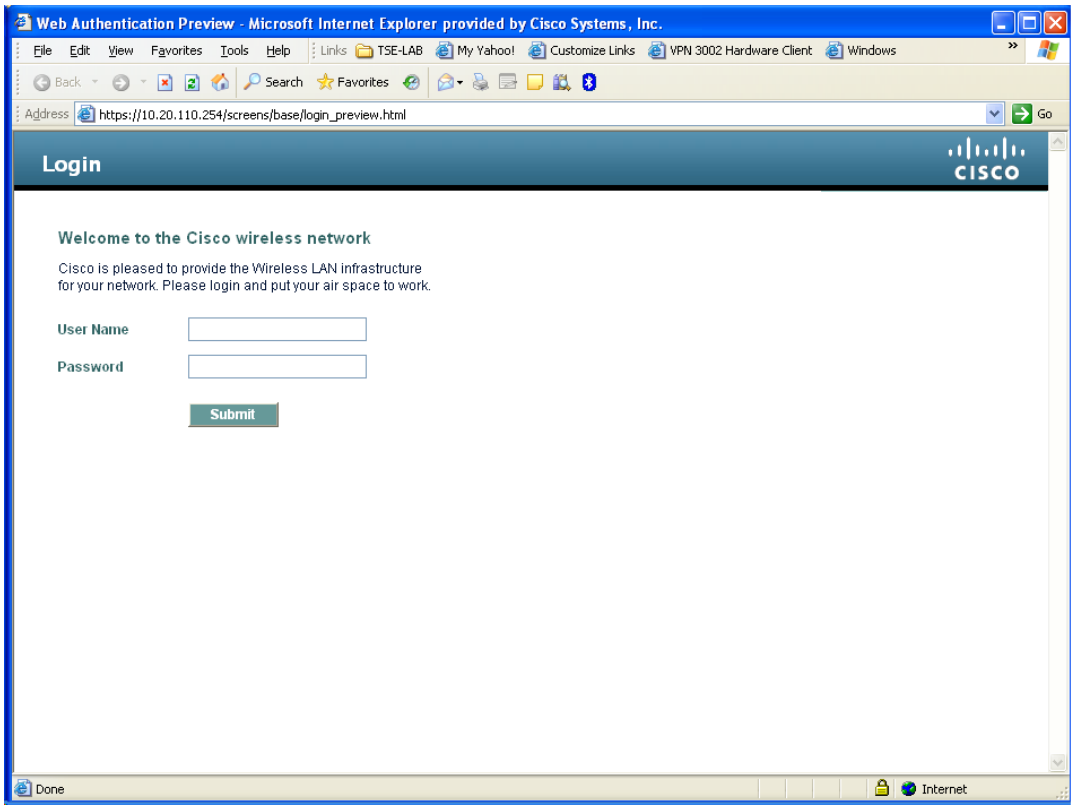
- A given foreign controller load balances wireless client connections across the list of anchor controllers configured for the guest WLAN. There is currently no method to designate one anchor as primary with one or more secondary anchors.
- Wireless clients that are associated with an anchor WLC that becomes unreachable are re-associated with another anchor defined for the WLAN. When this happens, assuming web authentication is being used, the client is redirected to the web portal authentication page and required to re-submit their credentials.

Note Multicast traffic is not supported over guest tunnels, even if multicast is enabled on the Cisco Unified Wireless Network.

Web Portal Authentication

The Cisco Centralized Guest Access solution offers a built-in web portal that is used to solicit guest credentials for authentication and offers simple branding capabilities, along with the ability to display disclaimer or acceptable use policy information (see Figure 10-5).

Figure 10-5 Controller Web Authentication Page



The web portal page is available on all Cisco WLAN controller platforms and is invoked by default when a WLAN is configured for Layer 3 web policy-based authentication.

If a more customized page is required, administrators have the option of importing and locally storing a customized page. Additionally, if an enterprise wants to use an external web server, the controller can be configured to redirect to it in place of using the internal server. See Guest Access Configuration, page 10-14 for web page configuration guidelines.

User Redirection

As is typical for most web-based authentication systems, in order for guest clients to be redirected to the WLC web authentication page, they must launch a web browser session and attempt to open a destination URL. For redirection to work correctly, the following conditions must be met:

- DNS resolution—The guest access topology must ensure that valid DNS servers are assigned via DHCP and those DNS servers are reachable to users prior to authentication. When a client associates to a web policy WLAN for authentication, all traffic is blocked except DHCP and DNS. Therefore, the DNS servers must be reachable from the anchor controller. Depending on the topology, this might require opening up conduits through a firewall to permit DNS or modifying ACLs on an Internet border router.

Note Clients with static DNS configurations might not work depending on whether their configured DNS servers are reachable from the guest network.

- Resolvable Home Page URL—The home page URL of a guest user must be globally resolvable by DNS. If a user home page is, for example, an internal company home page that cannot be resolved outside of their company intranet, that user is not redirected. In this case, the user must open a URL to a public site such as www.yahoo.com or www.google.com.
- HTTP Port 80—If the home page of a user is resolvable, but connects to a web server on a port other than port 80, they are not redirected. Again, the user is required to open a URL that uses port 80 to be redirected to the WLC web authentication page.

Note In addition to port 80, there is an option to configure one additional port number that the controller can monitor for redirection.The setting is available only through the CLI of the controller: <*controller_name*> config> **network web-auth-port** <*port*>.

Guest Credentials Management

Guest credentials can be created and managed centrally using WCS beginning with release 4.0 and later. A network administrator can create a limited privilege account within WCS that permits lobby ambassador access for the purpose of creating guest credentials. With such an account, the only function a lobby ambassador is permitted to do is create and assign guest credentials to controllers that have web-policy configured WLANs. For configuration guidelines, see Guest Access Configuration, page 10-14.

As with many configuration tasks within WCS, guest credentials are created using templates. Beginning with release 4.1, the following new guest user template options and capabilities were introduced:

- There are two types of guest templates: one for scheduling immediate guest access with limited or unlimited lifetime, and the other permits administrators to schedule “future” guest access and offers time of day as well as day of week access restrictions.
- The solution now offers administrators the ability to e-mail credentials to guest users. Additionally, when the “schedule” guest template is used, the system automatically e-mails credentials for each new day (interval) that access is offered.
- Guest credentials can be applied to the WLC(s) based on a (guest) WLAN SSID and WCS mapping information; campus/building/floor location or based on a WLAN SSID and a specific controller or list of controllers. The latter method is used when deploying guest access using the guest mobility anchor method as discussed in this chapter.

For further information, see Guest Management Using WCS, page 10-30.

After a lobby ambassador has created a guest template, it is applied to one or more controllers depending on the guest access topology. Only controllers with a “*web” policy-configured WLAN* are listed as a candidate controller to which the template can be applied. This is also true when applying guest templates to controllers based on WCS map location criteria.

Guest credentials, once applied, are stored locally on the (anchor) WLC (under Security > Local Net Users) and remain there until expiration of the “Lifetime” variable as defined in the guest template. If a wireless guest is associated and active when their credentials expire, the WLC stops forwarding traffic and returns to the WEBAUTH_REQD policy state for that user. Unless the guest credentials are re-applied (to the controller), the user is no longer able to access the network.

Note The Lifetime variable associated with guest credentials is independent of the WLAN session timeout variable. If a user remains connected beyond the WLAN session timeout interval, they are de-authenticated. The user is then redirected to the web portal and, assuming their credentials have not expired, must log back in to regain access. To avoid annoying redirects for authentication, the guest WLAN session timeout variable should be set appropriately.

Local Controller Lobby Admin Access

In the event that a centralized WCS management system is not deployed or unavailable, a network administrator can establish a local admin account on the anchor controller, which has only lobby admin privileges. A person who logs in to the controller using the lobby admin account has access to guest user management functions. Configuration options available for local guest management are limited in contrast to the capabilities available through WCS, and include the following:

- User name
- Generate password (check box)
- Administrator-assigned password
- Confirm the password
- Lifetime—days:hours:minutes:seconds
- SSID (check box)
- Only WLANs configured for Layer 3 web policy authentication are displayed
- Description

Any credentials that may have been applied to the controller by WCS are shown when an admin logs into the controller. A local lobby admin account has privileges to modify or delete any guest credentials that were previously created by WCS. Guest credentials that are created locally on the WLC do not automatically appear in WCS unless the controller's configuration is updated/refreshed in WCS. Locally created guest credentials that are imported into WCS as a result of a WLC configuration refresh appear as a new guest template that can be edited and re-applied to the WLC.

Guest User Authentication

As previously discussed in Guest Credentials Management, page 10-10, when an administrator uses WCS or a local account on a controller to create guest user credentials, those credentials are stored locally on the controller, which in the case of a centralized guest access topology, would be the anchor controller.

When a wireless guest logs in through the web portal, the controller handles the authentication in the following order:

1. The controller checks its local database for username and password and, if present, grants access.

If no user credentials are found, then:

2. The controller checks to see if an external RADIUS server has been configured for the guest WLAN (under WLAN configuration settings). See External Radius Authentication, page 12-38 for a configuration example. If so, then the controller creates a RADIUS access-request packet with the user name and password and forwards it to the selected RADIUS server for authentication.

If no specific RADIUS servers have been configured for the guest WLAN:

3. The controller checks its global RADIUS server configuration settings. Any external RADIUS servers configured with the option to authenticate "network" users are queried with the guest user credentials. See External Radius Authentication, page 12-38 for a configuration example. Otherwise, if no RADIUS servers have "network user" checked, and the user has not authenticated as a result of 1 or 2 above, authentication fails.

Note A RADIUS server can still be used to support network user authentication even if the network user check box is cleared under the WLC Security > AAA > RADIUS settings. However, to do so, a server must then be explicitly selected under the Security > AAA Servers settings of a given WLAN. See External Radius Authentication, page 12-38 for a configuration example.

External Authentication

WLC and WCS guest account management (lobby ambassador) capabilities can be used only to create and apply guest user credentials for local authentication on the WLC. However, there may be cases where an enterprise already has an existing guest management /authentication solution deployed as part of a wired guest access or NAC solution. If this is the case, the anchor controller/guest WLAN can be configured to forward web portal authentication to an external RADIUS server, as described in Guest User Authentication, page 10-11.

The default protocol used by the controller to authenticate web users is Password Authentication Protocol (PAP). In the event you are authenticating web users to an external AAA server, be sure to verify the protocols supported by that server. The anchor controller can also be configured to use CHAP or MD5-CHAP for web authentication. The web auth protocol type is configured under the Controller configuration settings of the WLC.

External Authentication using Cisco Secure ACS and Microsoft User Databases

If a guest access deployment is planning to use a Microsoft user database in conjunction with Cisco ACS to authenticate guest users, see the following additional Cisco ACS configuration caveats: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/installation/guide/windows/postin.html.

See specifically the following URL: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/installation/guide/windows/postin.html#wp1041223

Guest Pass-through

Another variation of wireless guest access is to bypass user authentication altogether and allow open access. However, an enterprise may still need to present an acceptable use policy or disclaimer page to users before granting access. If this is the case, then a guest WLAN can be configured for web policy pass through. In this scenario, a guest user is redirected to a portal page containing disclaimer information. Pass through mode also has an option for a user to enter an e-mail address before connecting (see Figure 10-6 and Figure 10-7 for sample pages). See Guest Access Configuration, page 10-14 for configuration examples.

Figure 10-6 Pass-through Welcome AUP Page

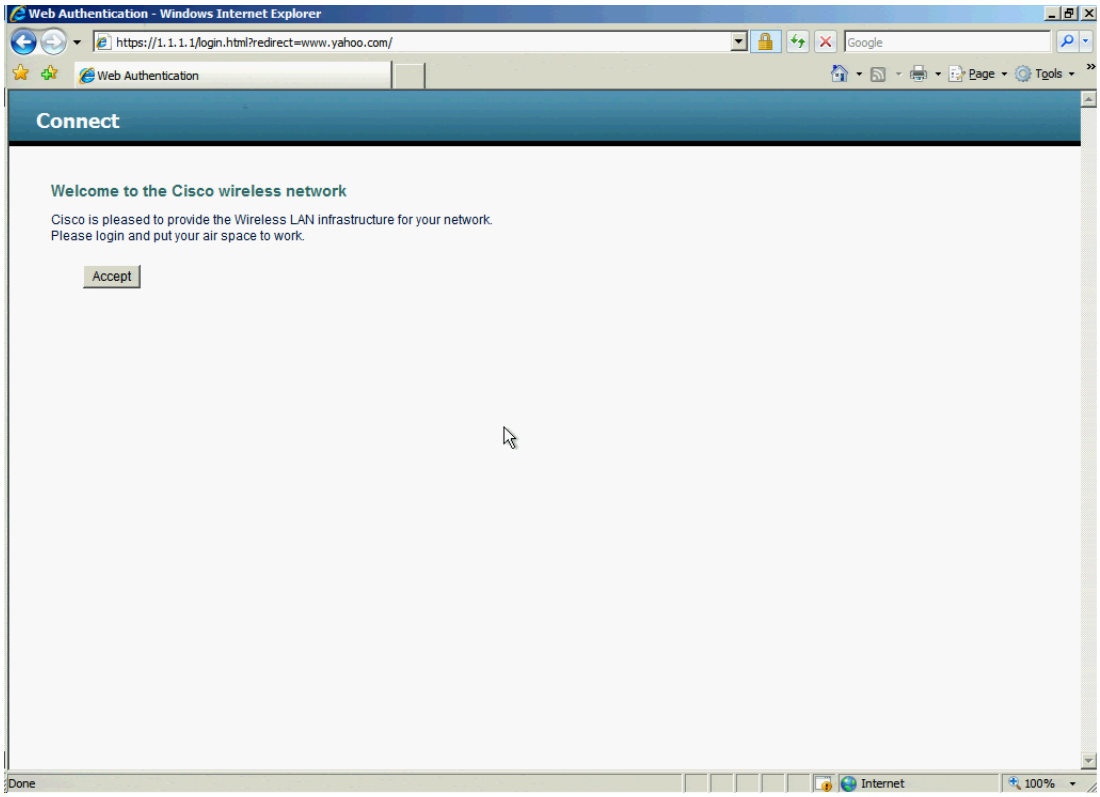
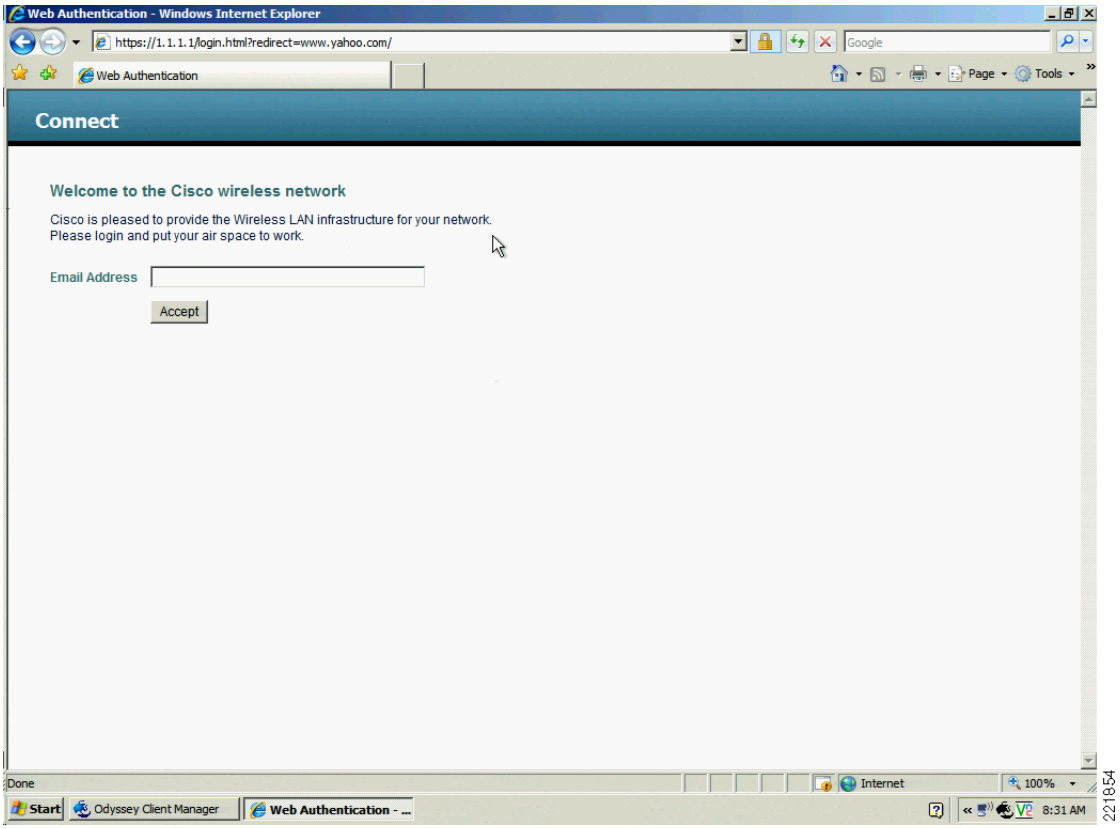


Figure 10-7 Pass-through Page with E-mail



Guest Access Configuration

This section describes how to enable a wireless guest access service within the Cisco Unified Wireless solution. The configuration tasks require the use of a web browser, Windows IE6 (only). A web session is established with the controller by opening an HTTPS session to the controller management IP address: **https://***management_IP* or optionally to a controller service port IP address.

The following procedures assume there is already a deployed infrastructure of controllers and LAPs with the possible exception of the anchor WLC(s). See Anchor Controller Deployment Guidelines, page 10-6 for more information.

Note Cisco recommends that the configuration steps outlined in this section be followed in the order in which they are presented.

The following references are used throughout the configuration sections:

- Foreign WLC—Refers to the one or more WLCs deployed throughout an enterprise campus or at branch location that are used for managing and controlling a group of LAPs. Foreign controllers map a guest WLAN into a guest mobility EoIP tunnel.
- Anchor WLC—Refers to one or more WLCs deployed in the enterprise DMZ that are used to perform guest mobility EoIP tunnel termination, web redirection, and user authentication.

Note Only the relevant portion of a given configuration screen capture is shown in this section.

The implementation of the Cisco Unified Wireless Guest Access solution can be broken into the following configuration categories:

1. Anchor WLC Installation and Interface configuration—This section briefly discusses installation requirements, steps and caveats associated with implementing one or more anchor WLCs. When implementing guest access for the first time in an existing Unified Wireless deployment, the anchor WLC is usually a new platform that is installed at the Internet edge of an Enterprise network.
2. Mobility Group Configuration—This section outlines the parameters that must be configured in order for the foreign WLCs to be able to initiate EoIP tunnels to one or more guest anchor WLCs. The mobility group configuration does not itself create the EoIP tunnels, but rather establishes peer relationships between the foreign and anchor WLCs in order to support a guest access WLAN service.
3. Guest WLAN Configuration—Highlights WLAN specific configuration parameters that are required to map the guest WLAN (originating from a foreign WLC) to the anchor WLC. It is during this portion of the guest access solution configuration that EoIP tunnels are created between the foreign and anchor WLCs. This section also covers the settings required to invoke Layer 3 redirection for web-based authentication.
4. Guest Account Management—This section outlines how to configure and apply guest user credentials locally on the anchor WLC using WCS' or the anchor WLC's lobby admin interface.
5. Other Features and Solution Options—Discusses other features that may be configured including, but not limited to:
   a. Web-portal page configuration and management
   b. Support for external web redirection
   c. Pre-authentication ACLs
   d. Anchor WLC DHCP configuration
   e. External radius authentication
   f. External access control

Anchor WLC Installation and Interface Configuration

As described in Anchor Controller Positioning, page 10-6, Cisco recommends that the anchor WLC be dedicated solely to guest access functions and not be used to control and manage LAPs in the enterprise.

This section does not address all aspects of interface configuration on the anchor WLC. It is assumed the reader is familiar with the WLC initialization and configuration process required upon initial bootup using the serial console interface. If not, see the following URL: http://www.cisco.com/en/US/docs/wireless/controller/4400/quick/guide/ctrlv32.html.

This section offers specific information and caveats as they pertain to configuring interfaces on a WLC being deployed as an anchor in a guest access topology.

As part of the initial configuration (using the serial console interface), you are required to define the following three static interfaces:

- Controller management—This interface/IP is used for communications with other controllers in the network. It is also the interface used to terminate EoIP tunnels that originate from the foreign controllers.

- AP manager interface—Even though the controller is not used to manage APs, you are still required to configure this interface. Cisco recommends the AP manager interface be configured on the same VLAN and subnet as the management interface.
- Virtual interface—The controller quickstart installation documentation recommends defining the virtual IP with an address, such as 1.1.1.1. This address needs to be the same for all controllers that are members of the same mobility group name. The virtual interface is also used as the source IP address when the controller redirects clients for web authentication.

Guest VLAN Interface Configuration

The interfaces previously described are for operations and administrative functions associated with the controller. To implement a guest access service, another interface must be defined. This is the interface through which guest traffic is forwarded for routing to the Internet. As previously described in Anchor Controller Positioning, page 10-6, the guest interface will likely connect to a port on a firewall or be switched to an interface on an Internet border router.

Defining a New Interface

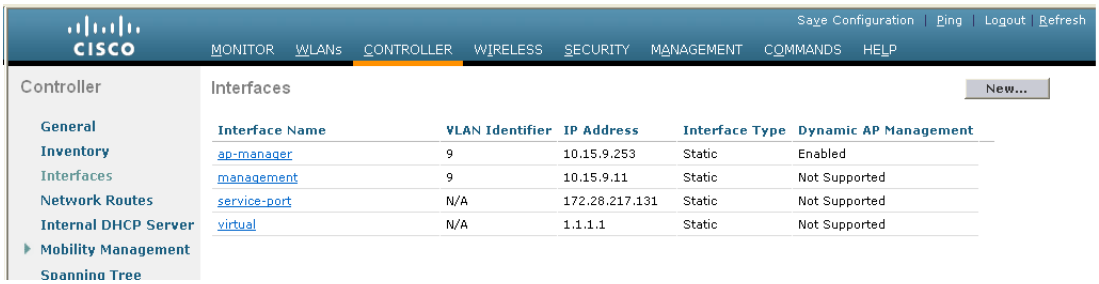
Perform the following to define and configure an interface to support guest traffic:

Step 1 Click the **Controller** tab.

Step 2 In the left pane, click **Interfaces**.

Step 3 Click **New**. (See Figure 10-8.)

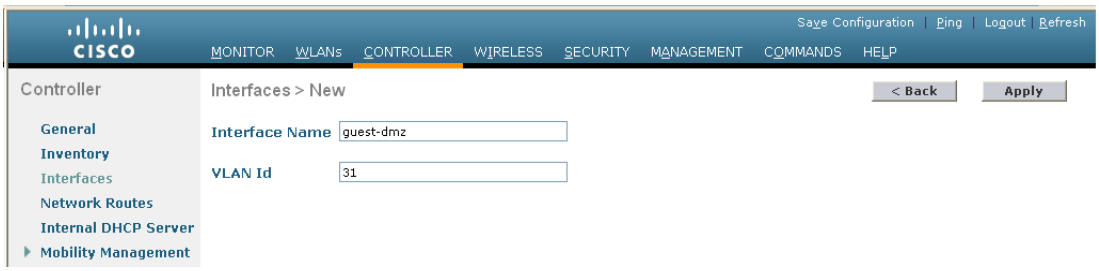
Figure 10-8 Controller Interfaces



Defining an Interface Name and VLAN ID

Step 4 Enter an interface name and VLAN ID. (See Figure 10-9.)

Figure 10-9 Interface Name and VLAN ID



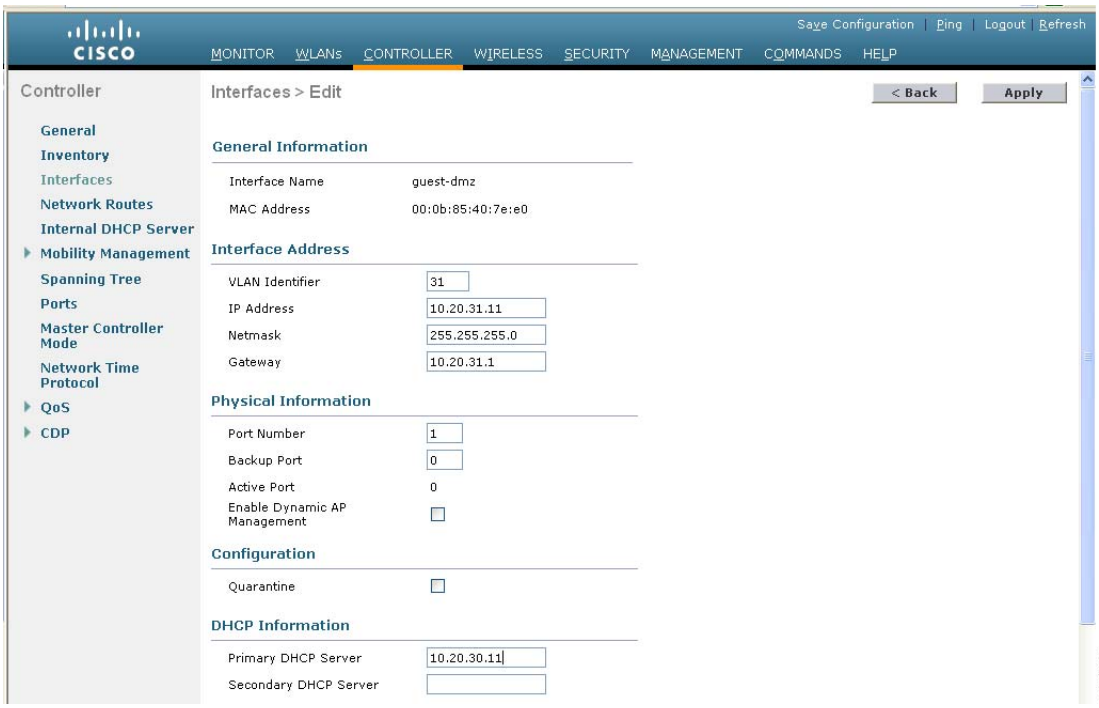
Defining Interface Properties

Step 5 Define the following properties:

- Interface IP
- Mask
- Gateway (for the firewall or next hop router connected to the anchor controller)
- DHCP Server IP (If using an external DHCP server, use the IP address of that server in the Primary DHCP Server field.)

  See Figure 10-10.

Figure 10-10 Defining Interface Properties



Note If DHCP services are to be implemented locally on the anchor controller, populate the primary DHCP server field with the management IP address of the controller. See Anchor WLC Installation and Interface Configuration, page 10-15.
If guest N+1 redundancy is being implemented in the DMZ, repeat the above interface configuration for each additional anchor WLC being deployed.

Mobility Group Configuration

The following default mobility group parameters should already be defined on the foreign WLC(s) as part of a standard centralized WLAN deployment. To support auto-anchor mobility for guest access, the anchor WLC(s) must also be configured with a mobility group domain name.

Defining the Default Mobility Domain Name for the Anchor WLC

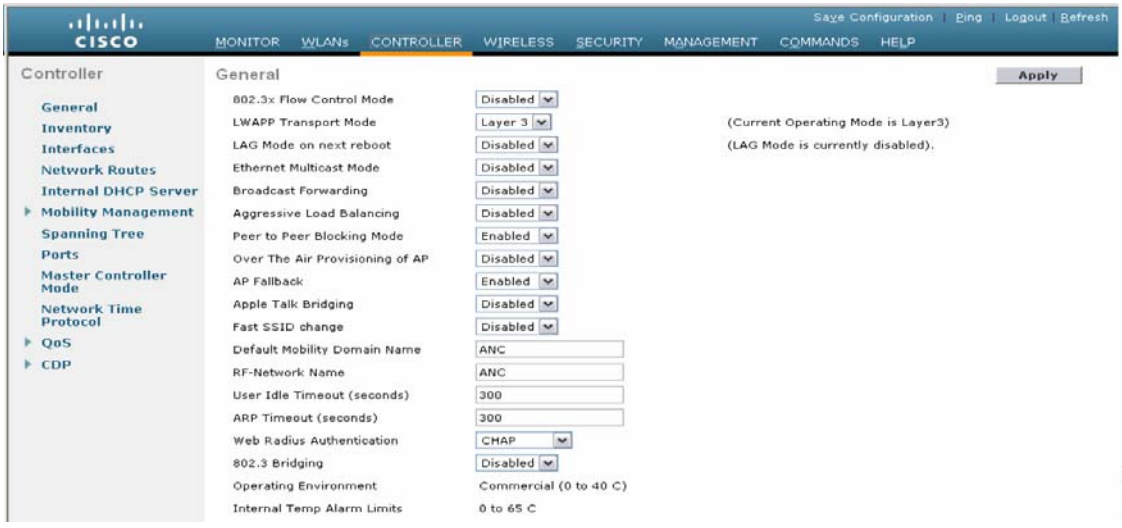
Configure a default mobility domain name for the anchor WLC. The anchor's mobility domain name should be different than what is configured for the foreign WLCs. In the examples below, the WLCs (foreign controllers) associated with the enterprise wireless deployment are all members of mobility group 'SRND'. The guest anchor WLC on the other hand, is configured with a different mobility group name: “ANC”. This is done to keep the anchor WLC logically separate from the primary mobility domain associated with the enterprise wireless deployment.

Step 1 Click the Controller tab.

Step 2 Enter a name in the Default Mobility Domain Name field.

Step 3 Click **Apply**. (See Figure 10-11.)

Figure 10-11 Defining a Default Mobility Domain Name on the Anchor WLC



Defining Mobility Group Members of the Anchor WLC

Every foreign WLC within the enterprise deployment that is going to support the guest WLAN must be defined as a mobility group member in the guest anchor WLC(s).

Step 1 Click the **Controller** tab.

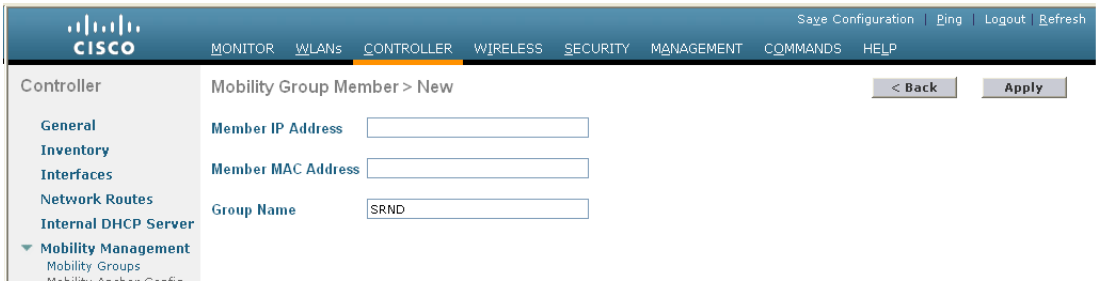
Step 2 In the left pane, click **Mobility Management** and then **Mobility Groups**. (See Figure 10-12.)

Figure 10-12 Defining Mobility Group Members

Adding Foreign Controllers as Mobility Group Members

Step 3 Click **New** to define a MAC and IP address for each foreign controller that will support the guest access WLAN. (See Figure 10-13.)

Figure 10-13 Adding Foreign Controllers to Anchor WLC



Note The 'Group Name' in Figure 10-13 above is the name configured under the foreign WLC's 'Default Mobility Domain Name', which should be different than the name used by the anchor WLC.The member IP and MAC address are those addresses associated with the management interface of the foreign WLCs. Repeat the above steps for each additional foreign WLC that will support the guest WLAN. If more than one anchor is being deployed (guest N+1 redundancy), then repeat the steps in Defining the Default Mobility Domain Name for the Anchor WLC, page 10-18 and Defining Mobility Group Members of the Anchor WLC, page 10-19.

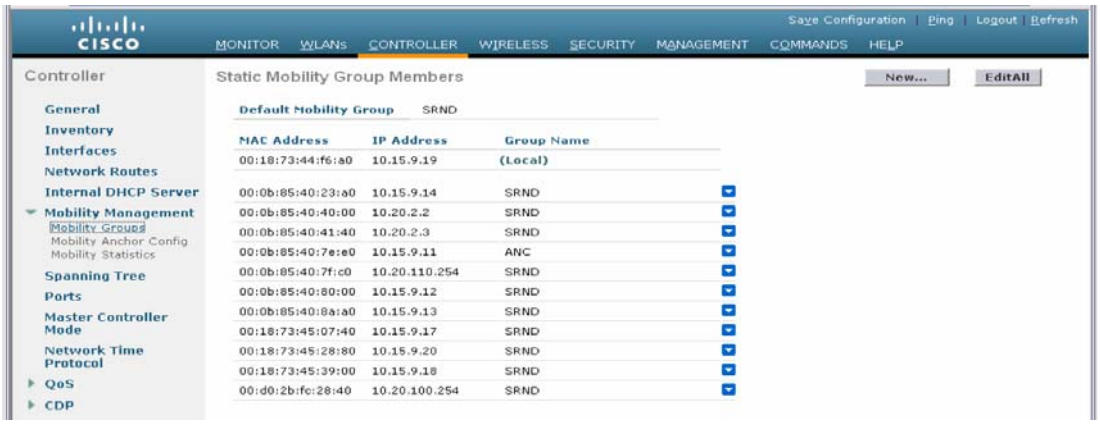
Adding the Anchor WLC as a Mobility Group Member of a Foreign WLC

As described in Auto Anchor Mobility to Support Wireless Guest Access, page 10-4, each foreign WLC maps the guest WLAN into an EoIP tunnel that terminates on the anchor WLC. Therefore, the anchor WLC(s) must be defined as a mobility group member in each foreign controller. In the example below, note that the group name entry for the anchor WLC is 'ANC' (see Defining Mobility Group Members of the Anchor WLC, page 10-19) whereas the other WLCs that comprise the enterprise wireless deployment are members of the mobility group: 'SRND'.

Step 1 Click **New** to add the anchor WLC's IP, MAC address, and Group Name to the mobility members table.

Step 2 Repeat these steps for each additional foreign controller. (See Figure 10-14.)

Figure 10-14 Adding Anchor Controller(s) to Foreign WLC



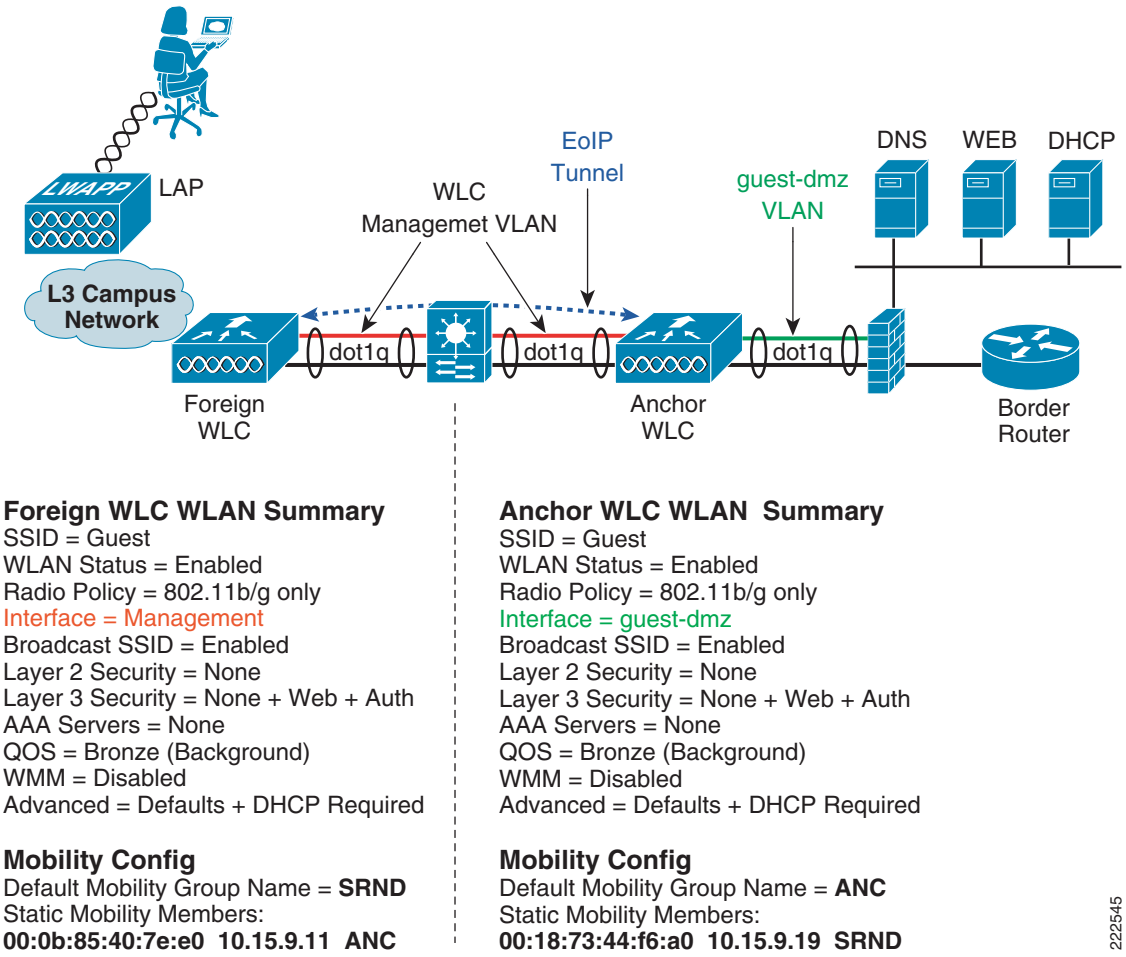
Note If guest N+1 anchor redundancy capability is being deployed, two or more anchor WLC entries are added to each foreign WLC's Mobility Group Members list.

Guest WLAN Configuration

The following section describes how to configure a single guest WLAN. The guest WLAN is configured on every foreign WLC that manages APs where guest access is required. Even though the anchor WLC(s) is not specifically used to manage LAPs associated with a guest WLAN, it must also be configured with the guest WLAN because the anchor WLC is a logical extension of the WLAN where user traffic is ultimately bridged (using LWAPP between the AP and the foreign controller, and EoIP between the foreign controller and the anchor controller) to an interface/VLAN on the anchor WLC.

Note It is extremely important to note that *all* parameters defined in the WLAN Security, QoS, and Advanced settings tabs, *must be configured identically* in both the anchor and foreign WLC(s). Figure 10-15 shows a high level diagram illustrating the WLAN configuration discussed below.

Figure 10-15 WLAN Configuration

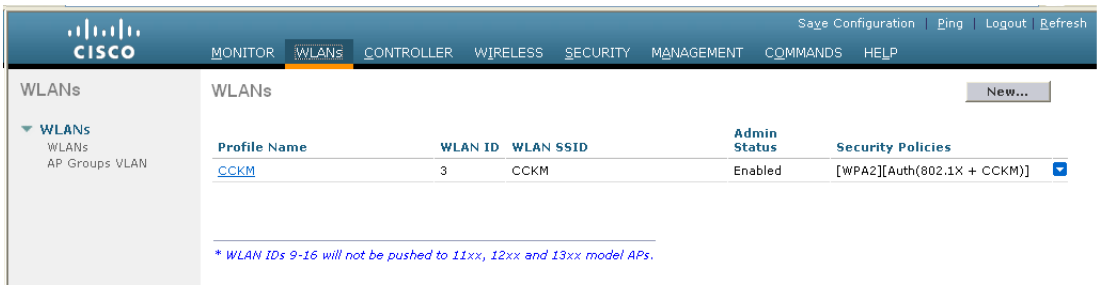


Note The parameters defined in the WLAN Security, QoS, and Advanced settings tabs, *must be configured identically* in both the anchor and foreign controller(s).

Foreign WLC—Guest WLAN Configuration

Step 1 Click the **WLANs** tab and then click **New**. (See Figure 10-16.)

Figure 10-16 Guest WLAN Configuration



Defining a Guest WLAN SSID

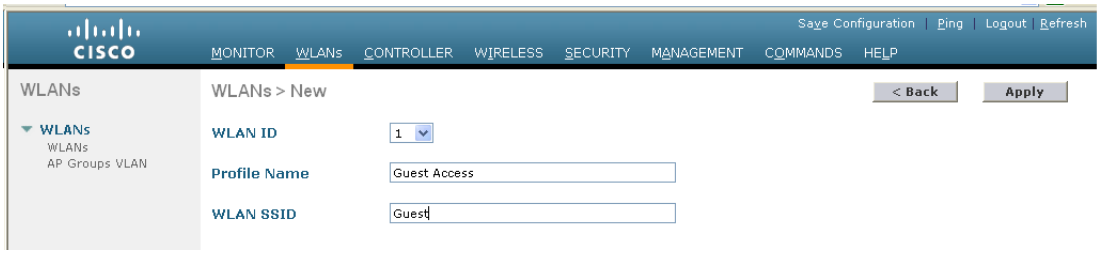
Step 2 Define an SSID that is intuitive or easily recognized by potential guest users.

The controller automatically assigns a VLAN ID. Administrators have the option selecting 1 – 16, as long as the ID is not already in use by another SSID/ WLAN.

Step 3 Define a Profile Name.

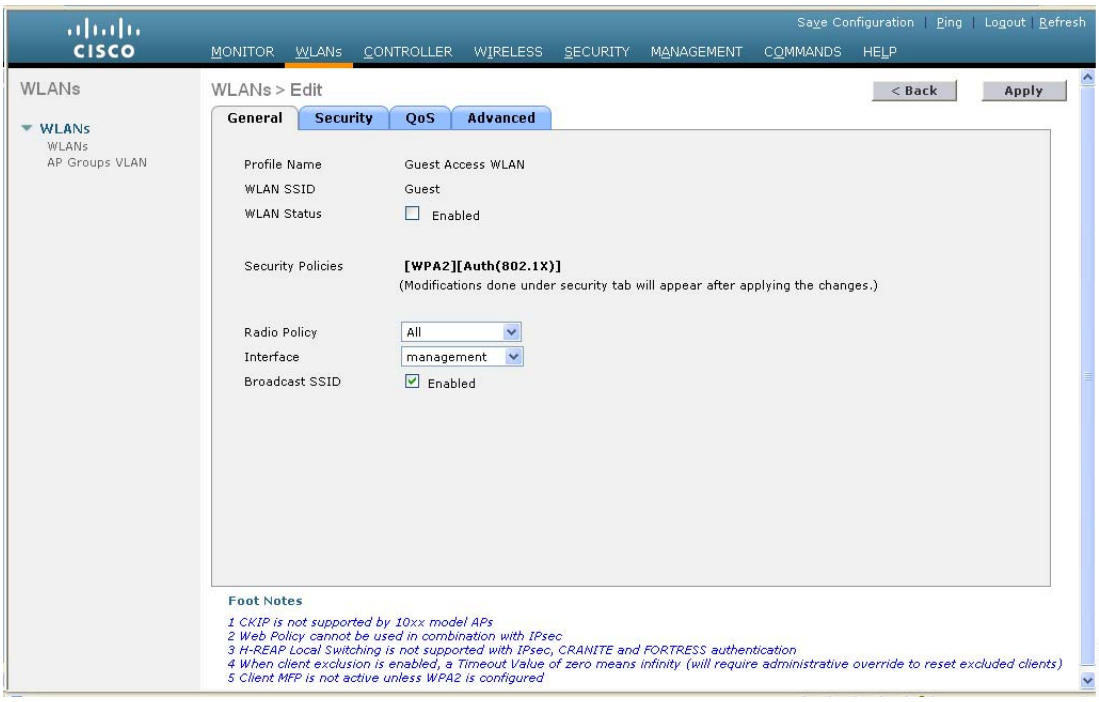
Step 4 Click **Apply**. (See Figure 10-17.)

Figure 10-17 Defining a Guest WLAN SSID



After creation of the new WLAN, the configuration page appears, as shown in Figure 10-18.

Figure 10-18 WLAN Configuration Page



Note The default interface used by the foreign WLC for the guest WLAN is the management interface. If the EoIP tunnel cannot be established with the anchor, the foreign controller will disassociate any wireless clients that were previously associated with the unreachable anchor and then assign new clients and reassociated clients to the interface configured under the guest WLAN of the foreign itself. Therefore, it is recommended to link the guest WLAN on the foreign to a non-routable network, or alternatively configure the DHCP server of the management interface with an unreachable IP address. If the anchor becomes unreachable, this prevents the guest clients to gain access to the management network.

Defining Guest WLAN Parameters and Policies

Under the General Configuration tab, perform the following steps.

Step 1 Enable the WLAN by clicking the box next to WLAN Status.

Step 2 Optionally, set the radio policy if you wish to restrict which bands support the guest access.

a. Broadcast SSID is enabled by default; leave enabled.

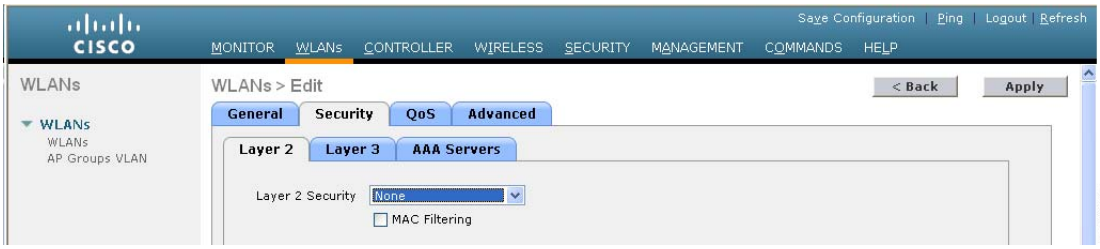
b. By default, the WLAN is assigned to the “management” interface of the WLC. Do not change this.

Step 3 Click the **Security** tab. (See Figure 10-19.)

Figure 10-19 Defining Guest WLAN General Policies

Step 4 Set the Layer 2 Security to **none** from its default setting (802.1x WPA/WPA2). (See Figure 10-20.)

Figure 10-20 WLAN Layer 2 Security Configuration



Step 5 Click the **Layer 3** tab. (See Figure 10-21.)

Figure 10-21 Guest WLAN Layer 3 Security Configuration

Step 6 Click the **Web Policy** checkbox (a list of additional options will be presented).

A dialog warning box appears, indicating that the WLC will pass DNS traffic to and from clients prior to authentication.

Step 7 Select **Authentication** or **Pass-through** for the web policy. (See Guest User Authentication, page 10-11.)

Note A pre-authentication ACL can be used to apply an ACL that allows un-authenticated clients to connect to specific hosts or URL destinations before authentication. The ACL is configured under Security > Access Control Lists. If a pre-authentication ACL is used in conjunction with the web auth policy, it must include a rule to permit DNS requests; otherwise, the client will be unable to resolve and connect to a destination host/URL that would otherwise be allowed by the ACL.

Step 8 Select the **QoS** tab, as shown in Figure 10-22.

Figure 10-22 Guest WLAN QoS Configuration

Step 9 Optionally, set the upstream QoS profile for the guest WLAN. The default is 'Silver (Best Effort)'. In this example, the guest WLAN has been re-assigned to the lowest QoS class.

Step 10 Click the **Advanced** tab. (See Figure 10-23.)

Figure 10-23 Guest WLAN Advanced Configuration

Step 11 Set Session Timeout (this is optional).

Note Any session timeout greater than 0 (default) forces de-authentication after expiration, and requires the user to re-authenticate through the web portal.

Step 12 Set DHCP Addr. Assignment to “Required”.

Note Setting DHCP Addr. Assignment to “Required” is recommended to prevent guest users from attempting to use the guest network using a static IP configurations.

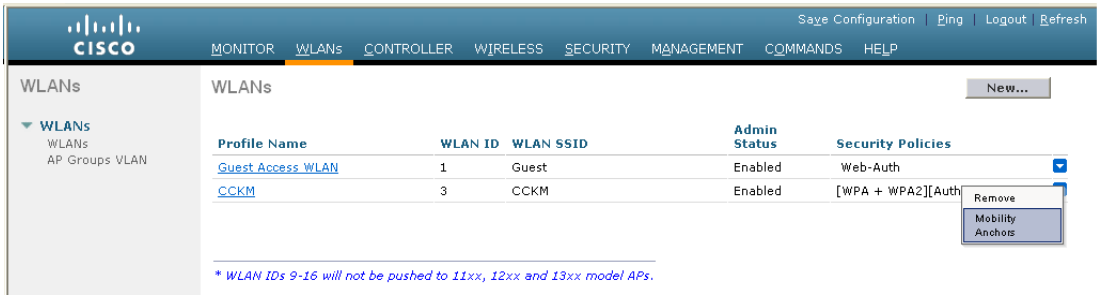
Step 13 Click **Apply** when finished.

Establishing the Guest WLAN Mobility Anchor(s)

Step 1 From the WLAN menu on the foreign WLC find the newly created guest WLAN.

Step 2 Highlight and click **Mobility Anchors** from the right-hand pull-down selection list. (See Figure 10-24.)

Figure 10-24 WLAN Mobility Anchor



Step 3 In the Switch IP Address (Anchor) pull-down selection list, select the IP address corresponding to the management interface of the anchor WLC deployed in the network DMZ. This is the same IP address configured in Adding the Anchor WLC as a Mobility Group Member of a Foreign WLC, page 10-20.

Step 4 Click **Mobility Anchor Create**. (See Figure 10-26.)

Figure 10-25 Selecting Management Interface from Switch IP Address (Anchor)

Figure 10-26 Selecting WLAN Mobility Anchor

Verifying the Guest WLAN Mobility Anchor

Once configured, the screen shown in Figure 10-27 shows the mobility anchor (selected from above), assigned to the Guest WLAN.

Figure 10-27 Verifying the Guest WLAN Mobility Anchor

For ease of verification, the page displays whether or not the mobility tunnel data path and LWAPP control path have been established with the anchor. If either or both show “down”, see Troubleshooting Guest Access, page 10-54 for troubleshooting tips. The pull-down selection list to the right offers the option to send a ping to the destination anchor WLC.

Step 5 When finished, click **Back**.

Step 6 Repeat the steps above for each additional anchor WLC being deployed (guest N+1 redundancy).

This completes the guest WLAN configuration. Repeat all steps from Foreign WLC—Guest WLAN Configuration, page 10-21 through Verifying the Guest WLAN Mobility Anchor, page 10-27 for each additional foreign WLC that will support the guest WLAN.

Guest WLAN Configuration on the Anchor WLC

Guest WLAN configuration on the anchor controller(s) is identical to that of the foreign controller except for minor differences in the WLAN interface and mobility anchor configuration, which are detailed below.

Note The SSID defined for the guest WLAN must be exactly the same as what is defined on the foreign WLCs.

Anchor WLC—Guest WLAN Interface

As indicated above, the parameters configured for the guest WLAN on the anchor WLC are the same except the interface to which the WLAN is mapped. In this case, the guest WLAN is assigned to an interface/VLAN on the anchor WLC, which connects to an interface on a firewall or Internet border router.

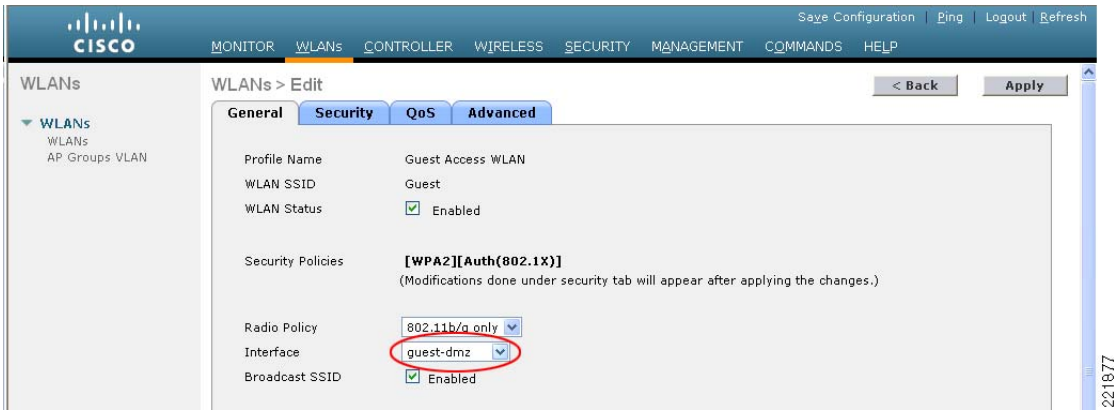
Step 1 Click the **WLANs** tab.

Step 2 Create, configure, and enable the guest WLAN the same way it was configured on the foreign WLC(s) except for the following:

In the WLANs general configuration, under **Interface,** choose the interface name created in Guest VLAN Interface Configuration, page 10-16. (See Figure 10-28.)

Step 3 Click **Apply**.

Figure 10-28 Anchor WLC Guest WLAN Interface Configuration



Anchor WLC—Defining the Guest WLAN Mobility Anchor

The second parameter that differs in configuration from the foreign WLC is the WLAN mobility anchor configuration. The guest WLAN mobility anchor is the anchor WLC itself.

Step 1 Click the **WLANs** tab.

Step 2 Find the Guest WLAN and click **Mobility Anchors**.

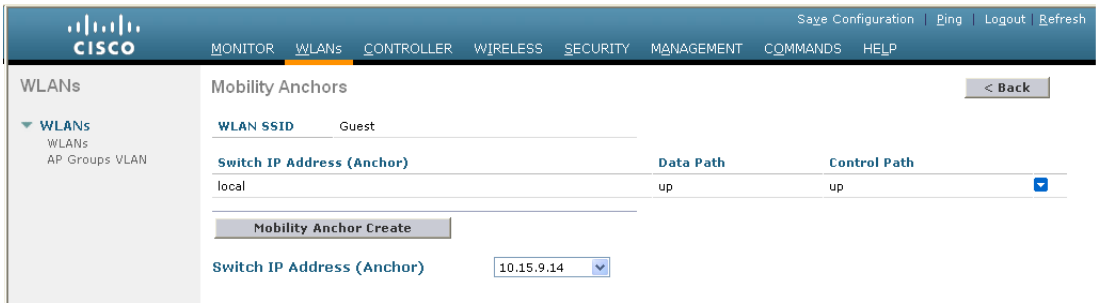
Step 3 From the pull-down selection list, choose the IP address representing the anchor controller. The IP address has (Local) next to it.

Step 4 Click **Mobility Anchor Create**. (See Figure 10-29.)

Figure 10-29 Defining the Guest WLAN Mobility Anchor

Note that the guest WLAN mobility anchor is *local*. (See Figure 10-30.)

Figure 10-30 Verifying Guest Mobility Anchor



Because the mobility anchor for the guest WLAN is the anchor WLC itself, the Data and Control Path status will always show “up”. If not, check to ensure that you have selected the local WLC as the anchor from the 'Switch IP Address (Anchor) drop down menu.

Step 5 If guest N+1 redundancy is being implemented, repeat the WLAN configuration for each additional anchor WLC being deployed. Otherwise, this completes the configuration steps required to create the guest WLAN on the anchor WLC.

Guest Account Management

- If guest credentials are going to be managed locally on the anchor controller, there are two methods by which they can be created and applied:
- Through a WCS lobby ambassador admin or super user/root admin account
- Directly on the controller via a local lobby admin account or other management account with read/write access

Guest Management Using WCS

The following configuration examples assume WCS version 4.1.83 or later has been installed and configured, and a lobby ambassador account has been created. For more information on installing and configuring WCS, see the following URL: http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html.

Regarding the creation of guest accounts, see the following URL: http://www.cisco.com/en/US/products/ps6305/products_configuration_guide_chapter09186a008083184 1.html#wp1075155.

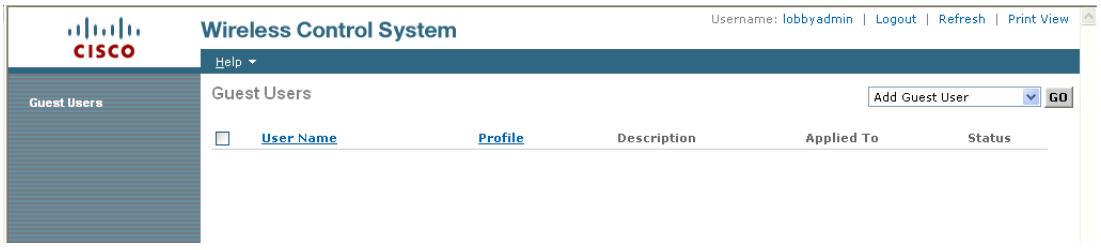
Note Ensure that the individual WLC configurations are synchronized with WCS before creating guest templates.

Log in to WCS using the Lobby Ambassador credentials assigned by the system administrator. (See Figure 10-31.)

Figure 10-31 WCS Login

After logging in, the screen shown in Figure 10-32 appears.

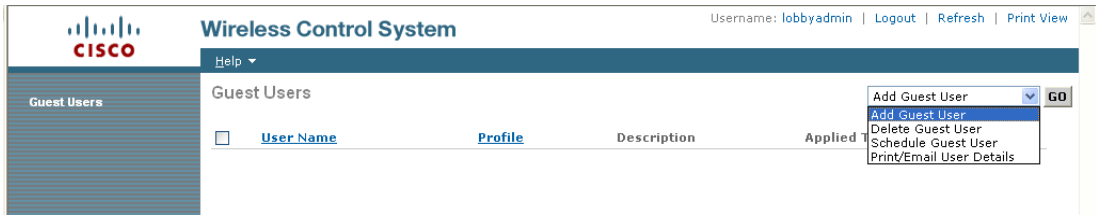
Figure 10-32 WCS Lobby Admin Interface



There are two types of guest templates:

- The **Add Guest User** template allows administrators to create and immediately apply guest credentials to one or more anchor WLCs.
- The **Schedule Guest User** template allows administrators to create guest credentials that are applied to one or more anchor WLCs at some future month, day, and time. (See Figure 10-33.)

Figure 10-33 Guest User Template Option



Using the Add Guest User Template

Step 1 From the pull-down selection list, select **Add Guest User** and click **Go.**

Step 2 The template shown in Figure 10-34 appears.

Figure 10-34 Add Guest User Template

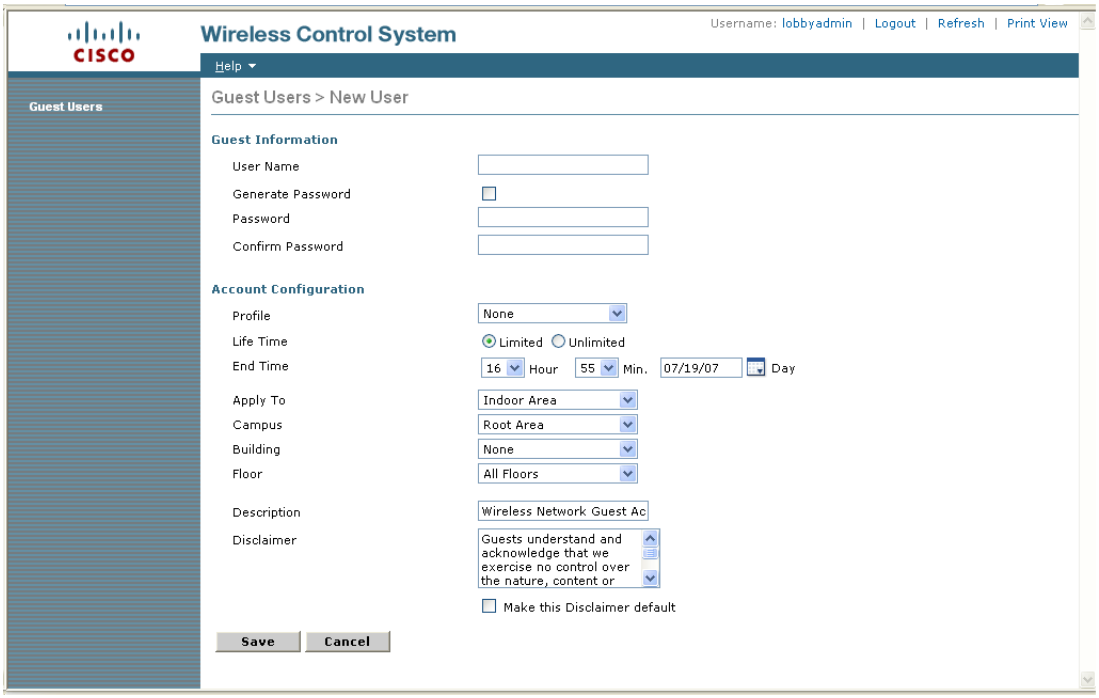
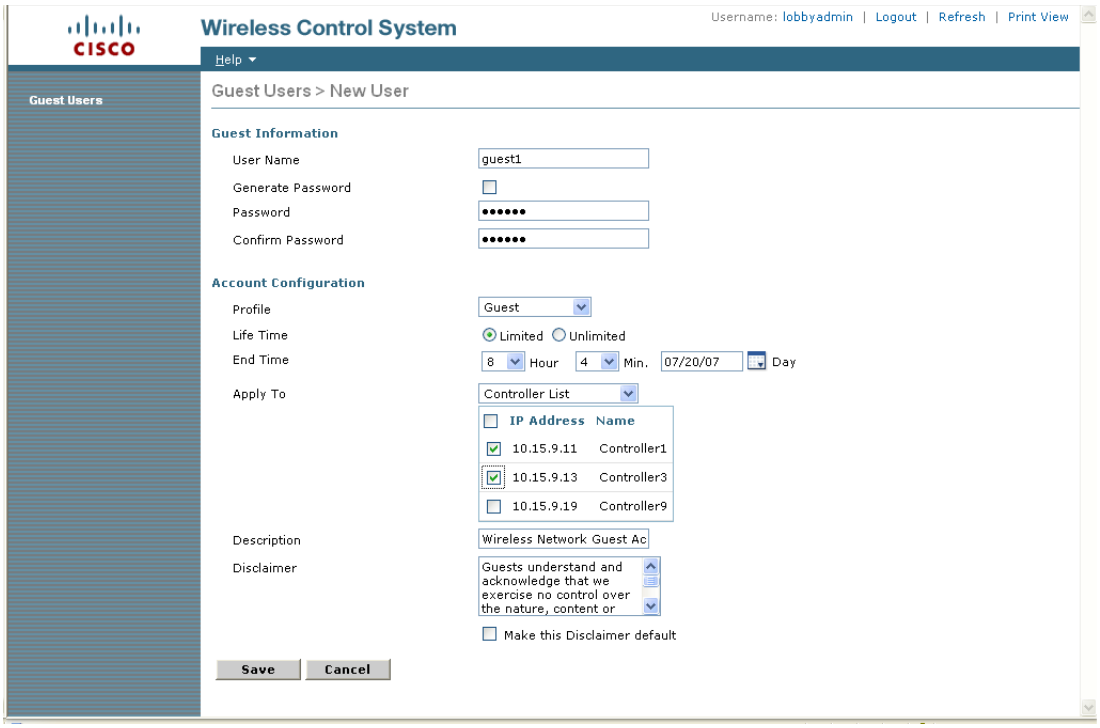


Figure 10-35 shows an example of guest user account creation.

Figure 10-35 Guest User Account Creation



Step 3 Under Guest Information, enter a User Name and Password.

Passwords are case sensitive. User names are restricted to 24 characters or less. Administrators also have an option to allow the system to automatically generate a password by clicking on the **Generate Password** check box.

Step 4 Under **Account Configuration,** select the following:

- Profile—The pull-down selection list displays a list of WLANs (SSIDs) configured with a L3 Web Policy.
- Life Time—Select “limited” or “unlimited”
- End Time—If the guest account is “limited”, select the month, day, and time the credentials are to expire.
- Apply To—From the pull-down selection list, select **Controller List** and click the check box next to the controller(s) representing anchor WLCs. Note that there will be other controllers listed; however, these represent the foreign WLCs. There is no need to apply user credentials on the foreign WLCs because the authentication enforcement point is the anchor WLC.

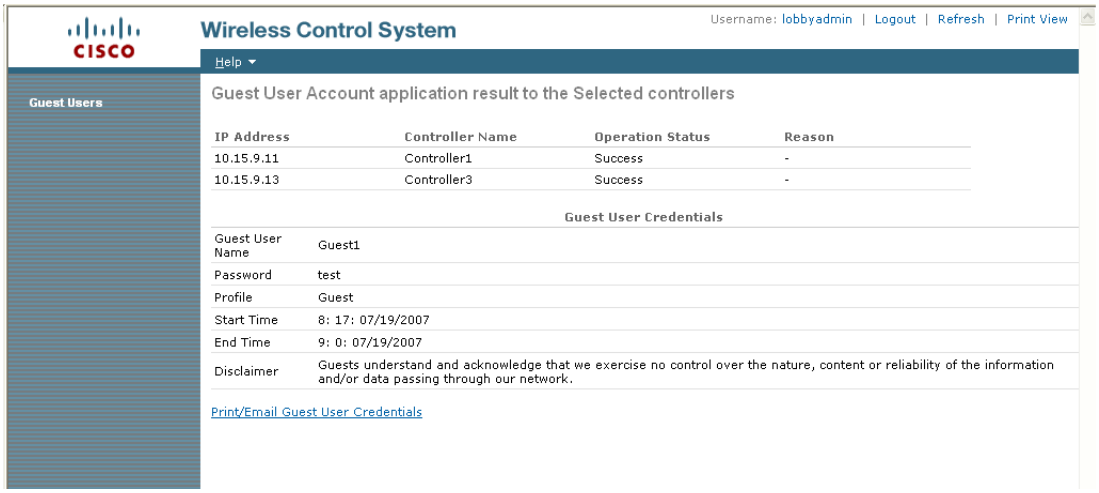
Note As seen in Figure 10-35, there are various options for where the credentials can be applied, including being able to control the physical/geographic location where a user can access the guest WLAN. These include outdoor areas, indoor areas, building, floor, and so on. This location-based access method can only be used if: 1) the WLAN deployment has been integrated into the WCS mapping database, and 2) the guest WLAN (a WLAN with web policy) does not use mobility anchors.

- Description—Enter a description. The description is displayed on the WLC to which the credentials are applied under Security > Local Net Users. It is also included in the e-mail that can be sent to a guest informing them of what credentials to use to access the network.

- Disclaimer—Used in the e-mail that can be sent to a guest user informing them of what credentials to use to access the network

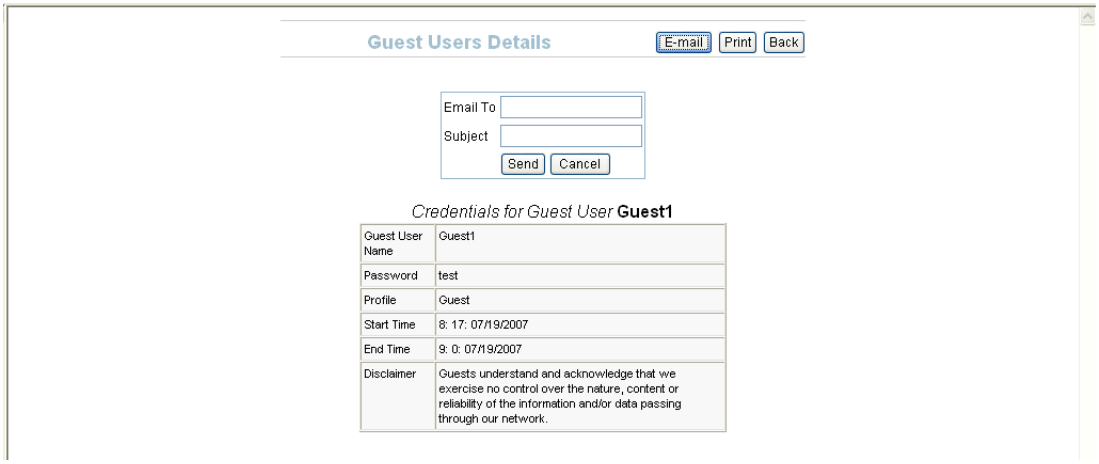
Step 5 Click **Save** when finished. The summary screen shown in Figure 10-36 appears, acknowledging that credentials have been applied to the anchor controller(s). The admin is also presented with an option to print or e-mail the credentials to the guest user.

Figure 10-36 Successful Guest Account Creation



Step 6 Click **Print/Email Guest User Credentials**. The screen shown in Figure 10-37 appears.

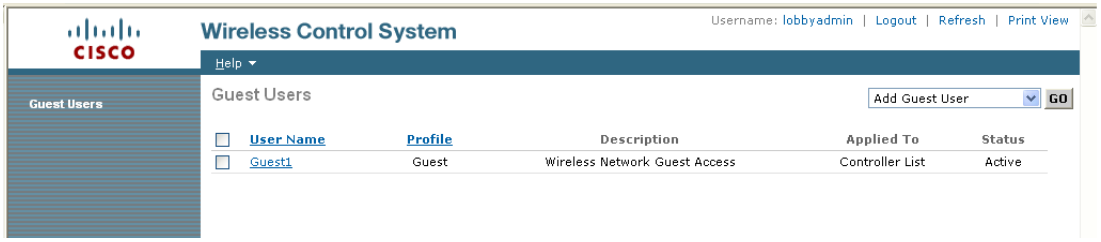
Figure 10-37 Print/Email Guest User Details



Note For details on setting up an SMTP mail server to support e-mailing guest account information to users, see the WCS Configuration guide at the following URL: http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcsadmin.html.

After printing and or e-mailing the account details, the screen shown in Figure 10-38 appears. By clicking the **User Name,** an admin can go back and edit the guest account or remove it by checking the box next to the User Name and selecting **Delete Guest User** from the pull-down selection list.

Figure 10-38 WCS Guest Users Summary



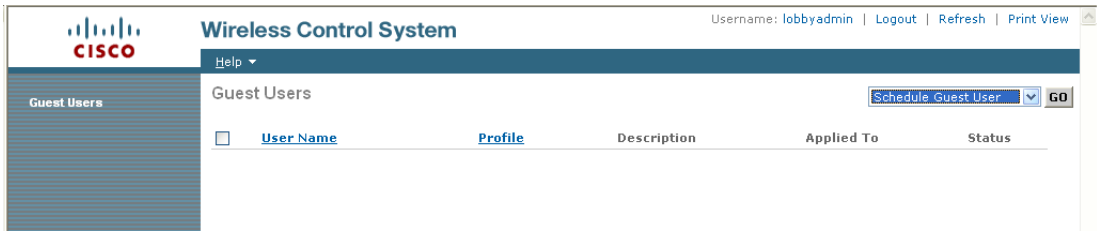
Note If a user template is deleted from WCS while a user is active, they are de-authenticated.

Using the Schedule Guest User Template

For details about configuring guest accounts, see the WCS Configuration guide at the following URL: http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcsadmin.html.

Figure 10-39 shows the guest user template option.

Figure 10-39 Guest User Template Option



Step 1 From the pull-down selection list, select **Schedule Guest User** and click **Go.**

The template shown in Figure 10-40 appears.

Figure 10-40 Schedule Guest User Template

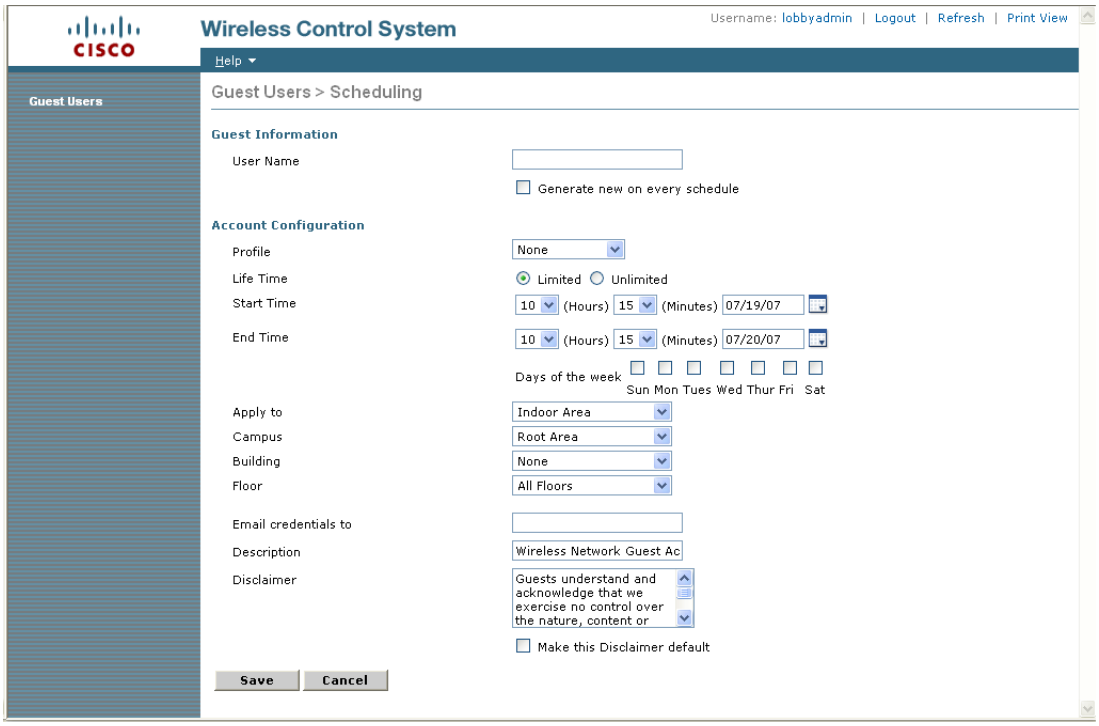
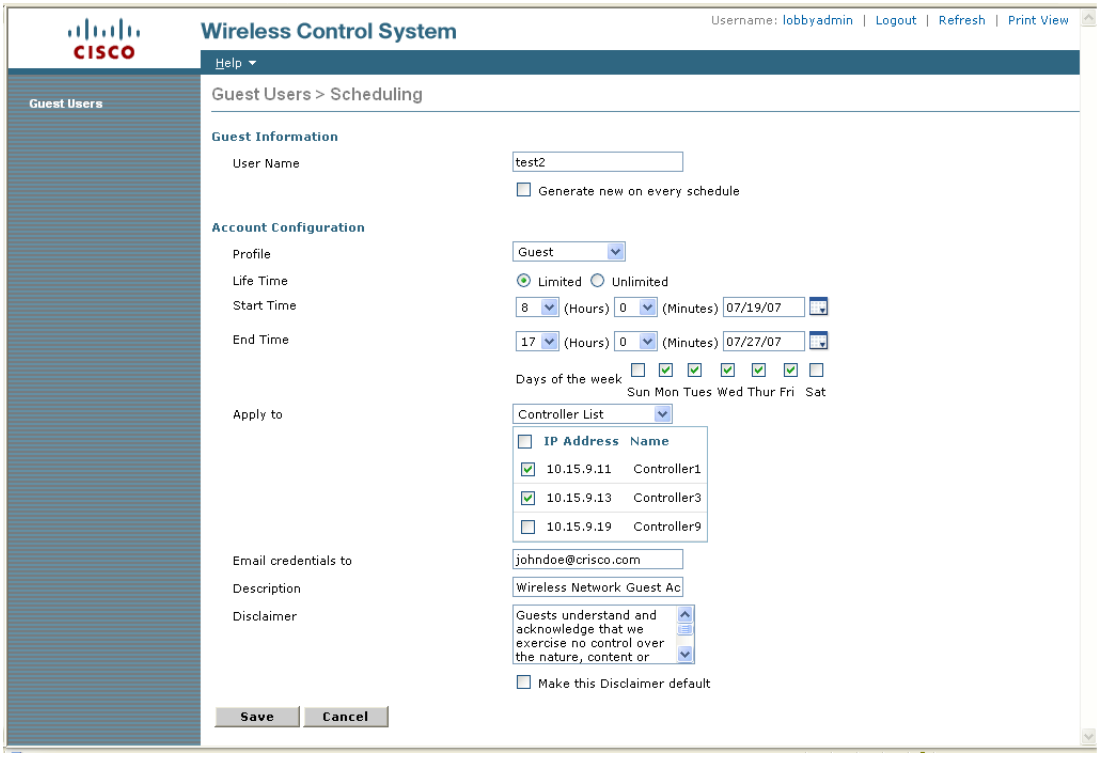


Figure 10-41 shows an example of a schedule guest user account creation.

Figure 10-41 Schedule Guest User Account Creation



Step 2 Under Guest Information, enter a User Name. User names can be up to 24 characters long. When using the schedule-based template, administrators have the option to allow the system to automatically generate the user name for each new day that access is being offered. Also, when using this template, the system automatically generates the user password. There is no option to manually assign a password.

Step 3 Under Account Configuration, select the following:

- Profile—The pull-down selection list displays a list of WLANs (SSIDs) configured with an L3 Web Policy.
- Life Time—Select “limited” or “unlimited”.
- Start Time—Select the time, month, and day when the account is to become active.

Note The start time cannot begin within the current day that the account is being created. The start day must be one or more days beyond the day the account is being created.

- End Time—If the account is limited, select the stop time, month, and day.

Note The stop day can be a period no longer than 30 days from the start day.

- Days of Week—Depending on the lifetime of the account, administrators have the ability to control for which days of the week access is available. Click the check boxes next to those days of the week access is permitted.

Note If "Days of the Week" is selected, the start and stop times represent the period within each day that access is available. Upon expiry within a given day, WCS removes the credentials from the applicable controllers. For each new day/interval that access is permitted, WCS automatically generates a new password (and optionally a username), e-mails it to the guest user, and re-applies the new credentials to the applicable WLCs. If "Days of the Week" is not defined, access begins based on the start day and time and is continuously active until the end day and time.

- Apply To—From the pull-down selection list, select **Controller List** and click the check box next to the controller(s) representing anchor WLCs. Note that there will be other controllers listed; however, these represent the foreign WLCs. There is no need to apply user credentials on the foreign WLCs because the authentication enforcement point is the anchor WLC.

Note As seen in Figure 10-41, there are various options for where the credentials can be applied, including being able to control the physical/geographic location where a user can access a guest WLAN. These include outdoor areas, indoor areas, building, floor, and so on. This location-based access method can only be used if: 1) the WLAN deployment has been integrated into the WCS mapping database, and 2) the guest WLAN (a WLAN with web policy) does not use mobility anchors.

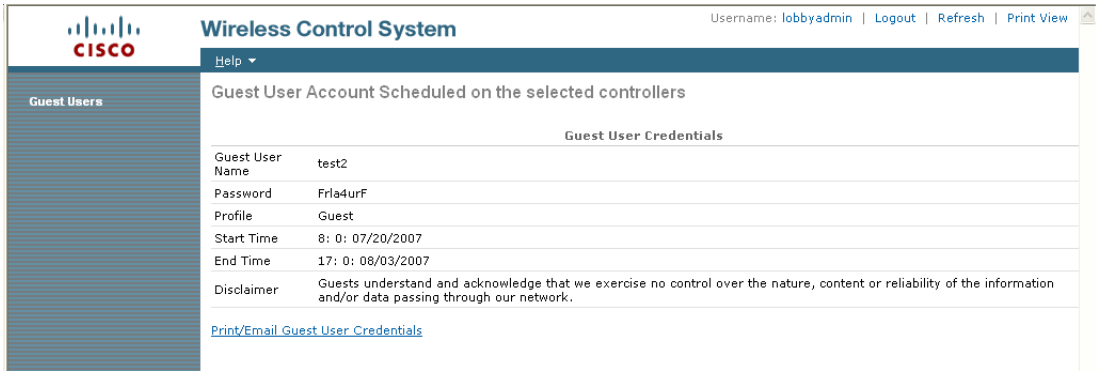
- E-mail Credentials to—Enter the e-mail address for whom an account is being established. This is a mandatory field.

Note An SMTP mail server must be configured in WCS so that it can use to send guest account information. For details, see the following URL: http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcsadmin.html.

- Description—Provide a description. The description is displayed on the WLC to which the credentials are applied under Security > Local Net Users. The description is also included in an e-mail that can be sent to the guest, informing them of what credentials to use to access the network.
- Disclaimer—Used in the e-mail that is sent to a guest user, informing them of what credentials to use to access the network.

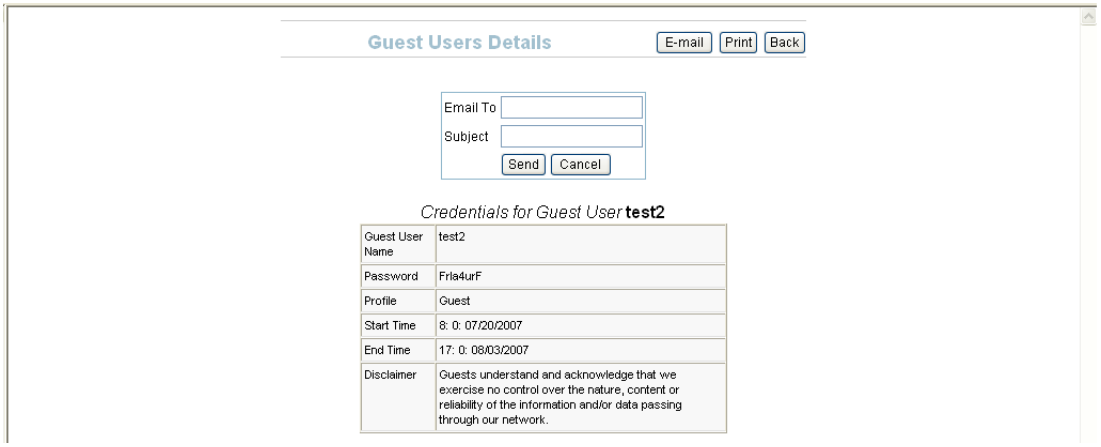
Step 4 Click **Save** when finished. The screen shown in Figure 10-42 appears, acknowledging that the scheduled account has been created. The admin is also presented with an option to print or e-mail the credentials to the guest user.

Figure 10-42 Successful Scheduled Account Creation



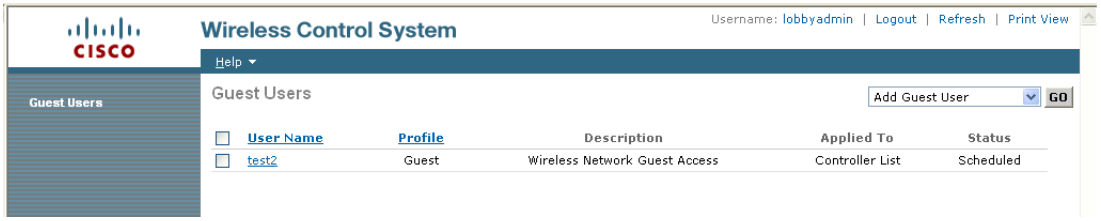
Step 5 Optionally, click **Print/Email Guest User Credentials**. The screen shown in Figure 10-43 appears.

Figure 10-43 Print/E-mail Guest User Details



After printing and/or e-mailing the account details, the summary screen shown in Figure 10-44 appears. By clicking the **User Name,** an admin can go back and edit the guest account or remove it by checking the box next to the User Name and selecting **Delete Guest User** from the pull-down selection list.

Figure 10-44 WCS Guest Users Summary



Note If a user template is deleted from WCS while a user is active, they are de-authenticated**.**

This completes the steps required to create a guest account using the lobby ambassador interface in WCS.

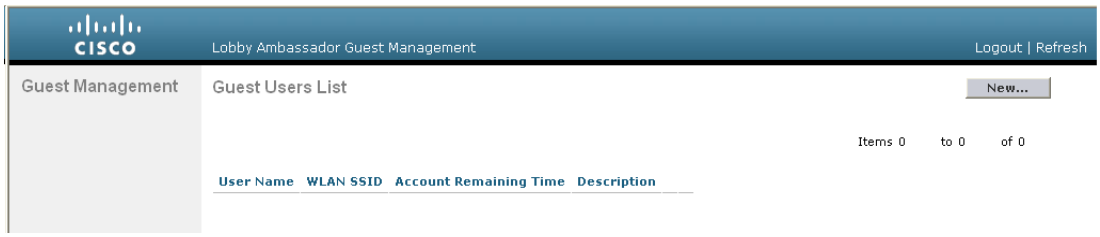
Managing Guest Credentials Directly on the Anchor Controller

The following procedure assumes that a network administrator has established a local management account with lobby admin privileges on one or more anchor controllers.

Step 1 Login to the anchor controller using the lobby admin credentials assigned by the system administrator. Remember that conduits might need to be opened through a firewall to permit HTTP/HTTPS for web administration of the controller. See Anchor Controller Positioning, page 10-6.

After login, the screen shown in Figure 10-53 appears.

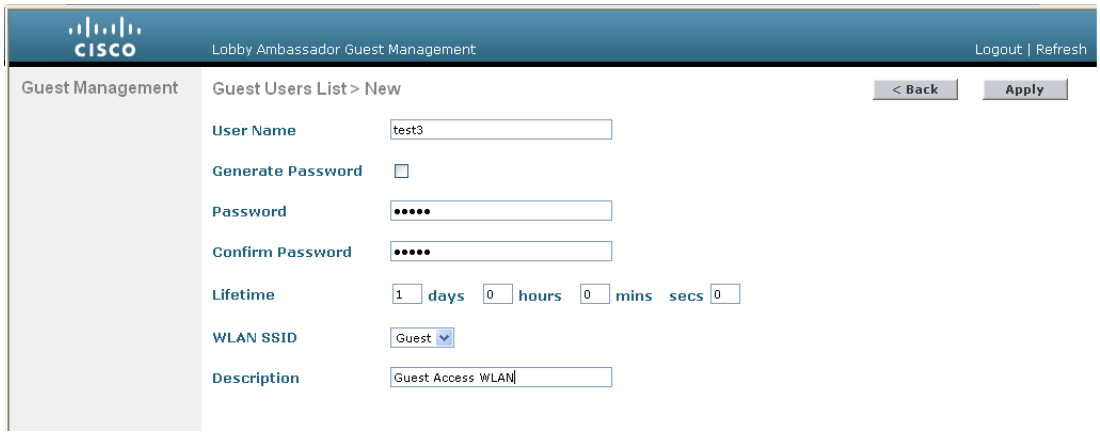
Figure 10-45 Anchor Controller Login



Step 2 Click **New**.

The screen shown in Figure 10-46 appears.

Figure 10-46 Creating Local WLC Guest Credentials



Step 3 To create user credentials, perform the following steps:

a. Enter a username and password (manual or auto).

b. Select the WLAN/SSID to which the guest account applies (only WLANs configured with an L3 web policy are displayed).

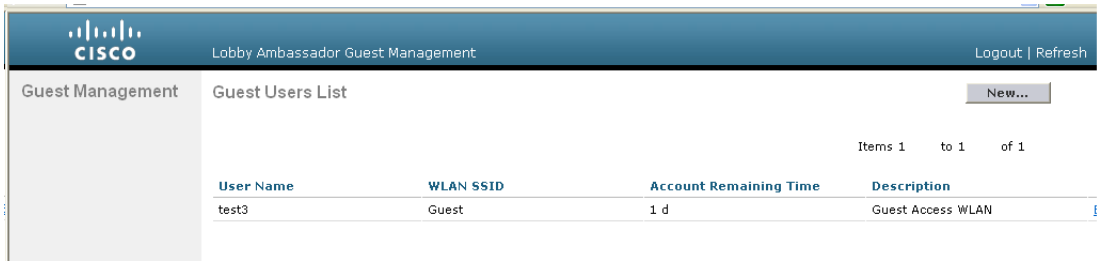
c. Enter a lifetime for the credentials.

d. Enter a description for the user.

Step 4 Click **Apply**.

The screen shown in Figure 10-47 appears and shows the newly-added guest user.

Figure 10-47 Anchor WLC Guest Users List



From this screen you have the option to do the following:

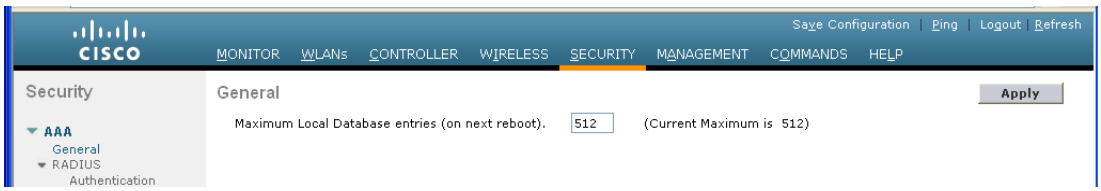
- Edit the existing user (link at far right; not visible)
- Delete the existing user (link at far right; not visible)
- Add a new user

Configuring the Maximum Number of User Accounts

The default number of guest user accounts that can be defined on the controller is 512. This value can be changed by completing the following steps.

Step 1 Click the **Security** tab. (See Figure 10-48.)

Figure 10-48 Configuring the Maximum Number of User Accounts



Step 2 In the left pane, click **General** under AAA properties.

Step 3 Configure the maximum number of user database entries (between 512 and 2048).

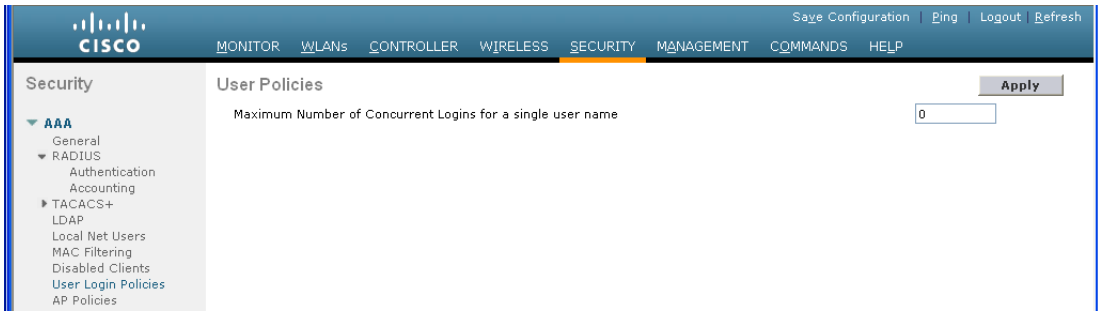
Step 4 Click **Apply**.

Maximum Concurrent User Logins

The maximum number of concurrent logins for a local user account on the WLC can be configured. Values include 0 for unlimited concurrent logins or can be limited from 1 to 8. The maximum user logins is configured by completing the following steps:

Step 1 Click the **Security** tab. (See Figure 10-49.)

Figure 10-49 User Login Policies



Step 2 In the left pane, click **User Login Policies** under AAA.

Step 3 Configure the maximum number of concurrent user logins (between 0–8).

Step 4 Click **Apply**.

Guest User Management Caveats

Note the following caveats:

- Guest accounts can be added using either method above or both methods together.
- When using WCS, the lobby admin may not have visibility of user accounts that might have been created locally on the anchor controller if the controller configuration has not been recently synchronized with WCS. If this is the case and a WCS lobby admin attempts to add an account with a user name that is already configured on the WLC, the WCS configuration overrides the local configuration.
- When adding user accounts locally on the controller, the local admin will have visibility of all accounts that have been created, including those that were created via WCS.
- If a guest user is currently authenticated to a WLAN and their credentials are deleted from WCS or locally on the controller, the user traffic stops flowing, and the user is de-authenticated.

Other Features and Solution Options

Web Portal Page Configuration and Management

The internal web server and associated functionality is hosted locally on the anchor controller. When a WLAN is configured to use the web policy, either for authentication or pass-through, the internal web server is invoked by default. No further configuration is required. The internal portal includes a few optional configuration parameters.

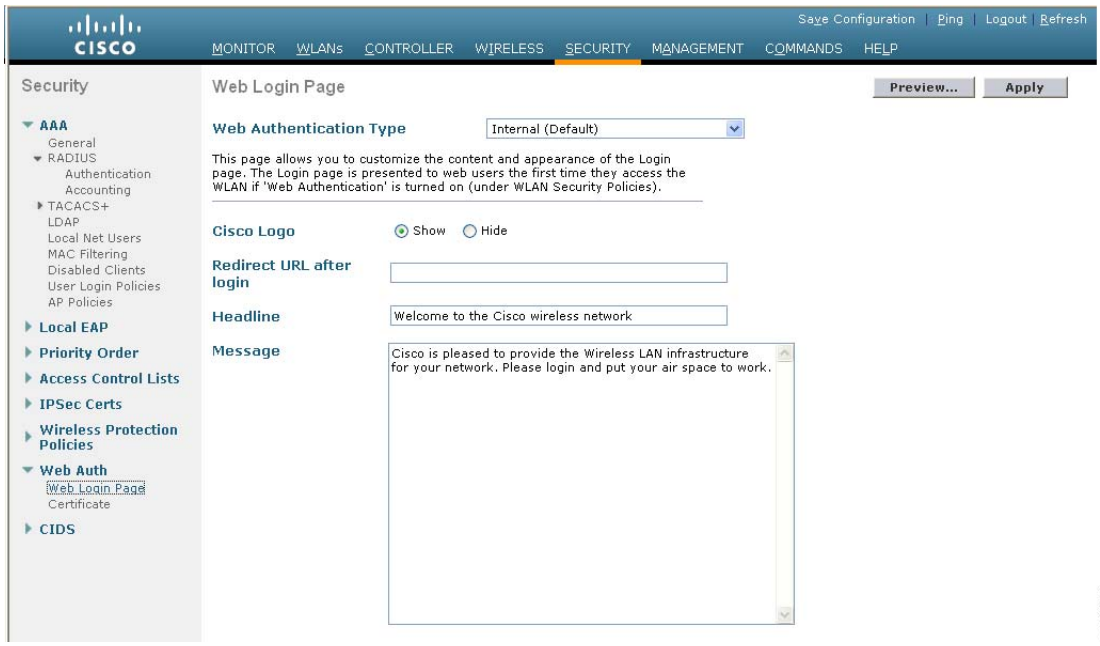
Internal Web Page Management

Step 1 Click the **Security** tab.

Step 2 In the left pane, click **Web Auth** and then **Web Login Page**.

The configuration screen shown Figure 10-50 is displayed. You can change the heading and message information that appears on the portal page. You can also choose a post-authentication redirect URL.

Figure 10-50 Web Login Page Configuration Screen



Step 3 Click **Apply**.

Step 4 Optionally, click **Preview** to view what the user sees when redirected.

Importing A Web Page

You can download a customized web page and store it locally on the anchor controller. To import a customized web page, perform the following steps.

Step 1 Click the **Commands** tab. (See Figure 10-51.)

Figure 10-51 Importing a Web Page

Step 2 Under File Type, select **Web Auth Bundle**.

Step 3 Define the IP address and file path on the TFTP server where the files reside.

Step 4 Click **Download** to begin.

Be aware of these caveats when downloading a web auth bundle:

- Select **Web Auth Bundle** from the pull-down selection list to ensure that the files are stored in the correct directory on the controller.
- The **Web Auth Bundle** must be a **.tar** file of the HTML and image files associated with the custom web login page. When downloaded, the WLC un-tars the files and places them in the appropriate directory.
- The **Web Auth Bundle** (**.tar** file) cannot be larger than 1 MB.
- The file name for the HTML login page must be **login.html**.

See the following URL for more information about downloading and using customized web pages: http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcssol.html#wp1065703.

Selecting an Imported Web Auth Page

To use a customized web-auth page that has been downloaded to the controller, perform the following steps:

Step 1 Click the **Security** tab.

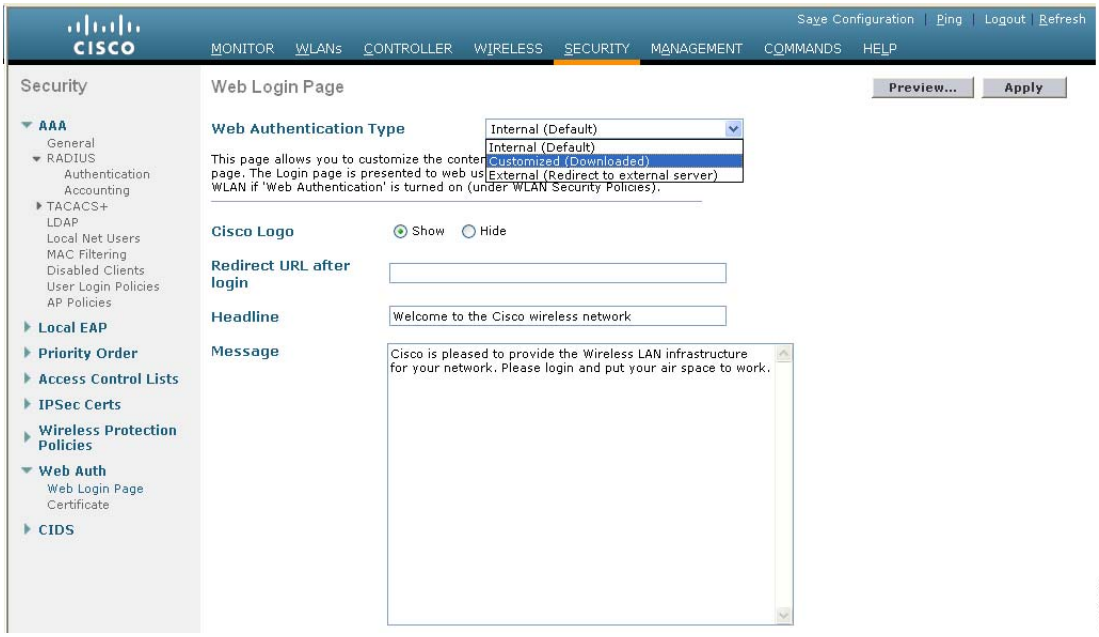
Step 2 In the left pane, click **Web auth** and then **Web Login Page**.

Step 3 From the Web Authentication Type pull-down selection list, select **Customized** (Downloaded).

Step 4 Click **Preview** to view the downloaded page.

Step 5 Click **Apply** when finished. (See Figure 10-52.)

Figure 10-52 Selecting an Imported Web Auth Page



Internal Web Certificate Management

The web auth login page uses SSL for safeguarding user credentials. For simplicity, the controller uses a self-signed certificate. Because the certificate is self-signed, guest users can expect to see a pop-up alert similar to the following when they are redirected to the authentication page shown in Figure 10-53.

Figure 10-53 Web Certificate Security Alert (IE6)

At this point, you can proceed by either clicking **Yes** or you can select **View Certificate** and manually install it as a trusted site.The web server uses the virtual interface IP address configured in Anchor WLC Installation and Interface Configuration, page 10-15, as its source address. If a hostname is defined along with the IP address, that host name must be resolvable by DNS so that:

- The client is redirected to the web auth page.
- The user does not encounter a web certificate error because of conflicts between hostname and host IP address.

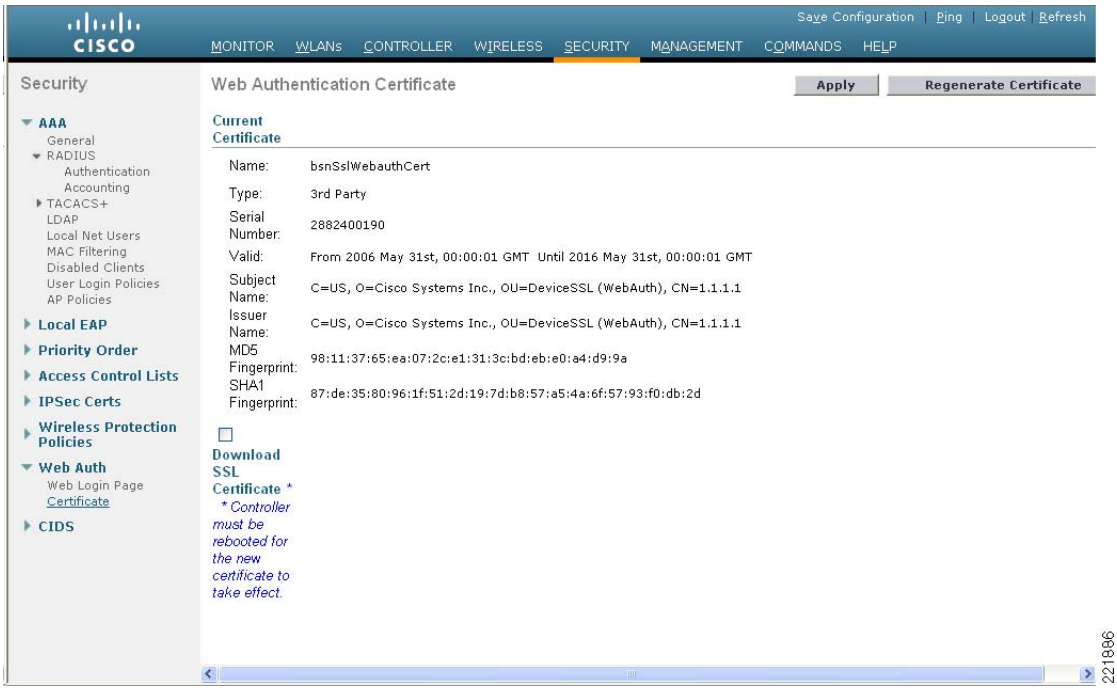
Importing an External Web Certificate

For cases where a legitimate web certificate issued by a trusted root CA is required, one can be downloaded to the controller by performing the following steps:

Step 1 Click the **Security** tab.

In the left pane, click **Web Auth** and then **Certificate**. (See Figure 10-54.)

Figure 10-54 Importing an External Web Certificate



Step 2 Place a check mark in the **Download SSL Certificate** checkbox.

Step 3 Complete the required fields for downloading the certificate.

Step 4 Click **Apply**.

Step 5 After the certificate has been downloaded, reboot the server.

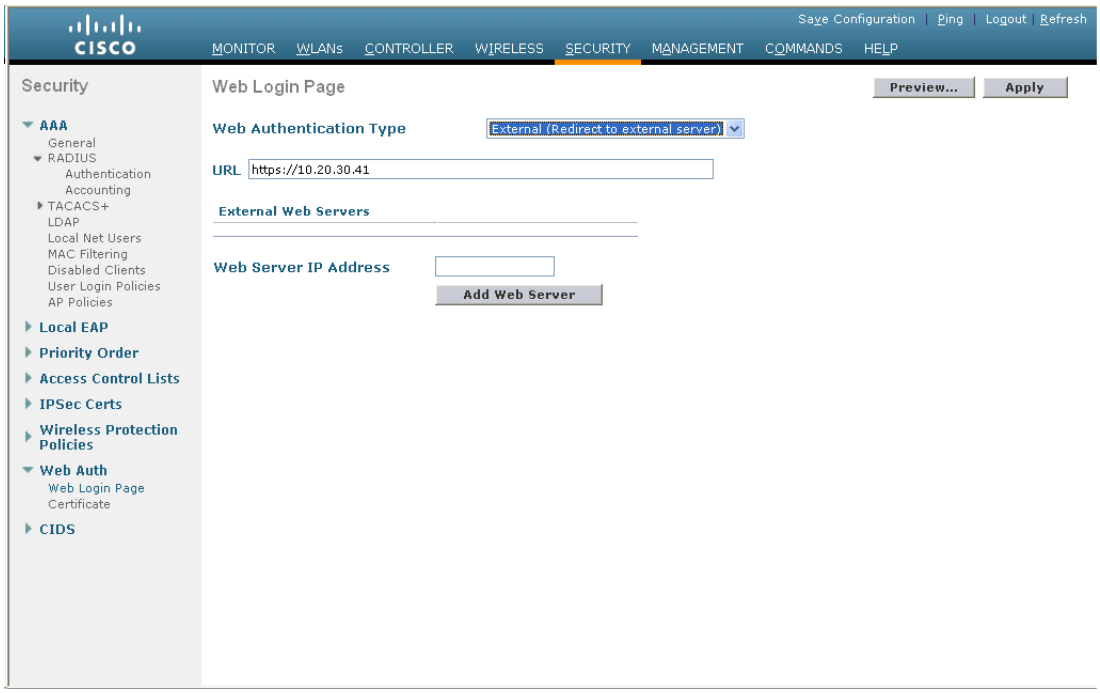
Support for External Web Redirection

In some cases, an enterprise might already have deployed a web-portal system to support wired guest access or NAC functionality. If this is the case, the anchor controller can be configured to redirect wireless guest users to an external web portal using the following steps:

Step 1 Click the **Security** tab.

Step 2 In the left pane, click **Web auth** and then **Web Login Page**. (See Figure 10-55.)

Figure 10-55 Supporting External Web Redirection



Step 3 Fill in the Web Server IP and URL fields.

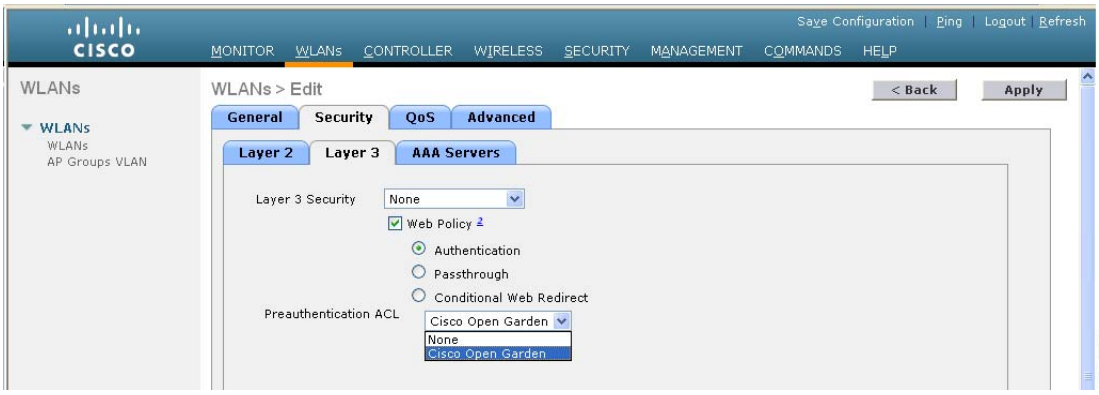
Step 4 Click **Apply**.

See the following URL for more information on the use of external web servers with controller web authentication:
http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008076f974.shtml

Anchor WLC-Pre-Authentication ACL

A pre-authentication ACL (pre-auth ACL) can be applied to the guest WLAN, which allows unauthenticated clients to connect to specific hosts or URL destinations prior to authenticating. The pre-auth ACL is applied under the guest WLAN Layer 3 Security settings and, if enabled, is performed only on the anchor WLC(s). (See Figure 10-56.)

Figure 10-56 WLAN Pre-authentication ACL



The specific ACL is configured under Security > Access Control Lists. (See Figure 10-57 and Figure 10-58.)

Figure 10-57 WLC Access Control Lists

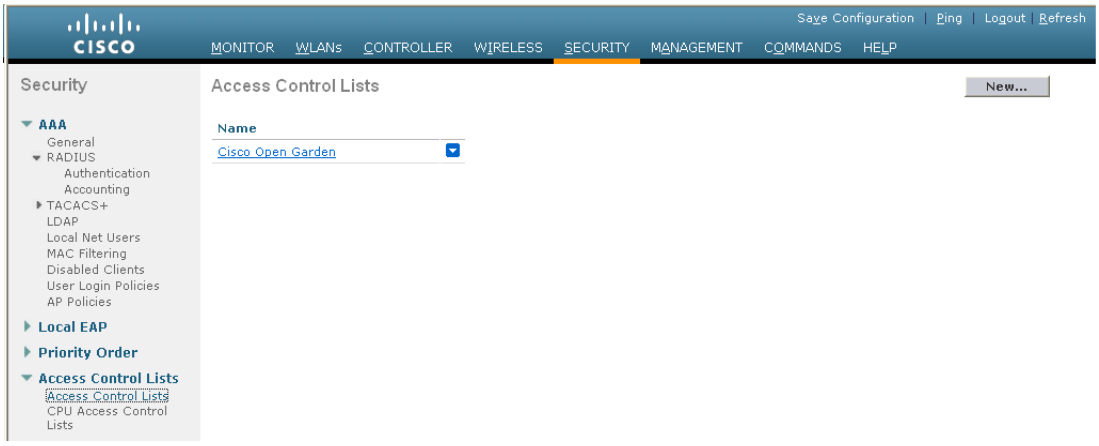
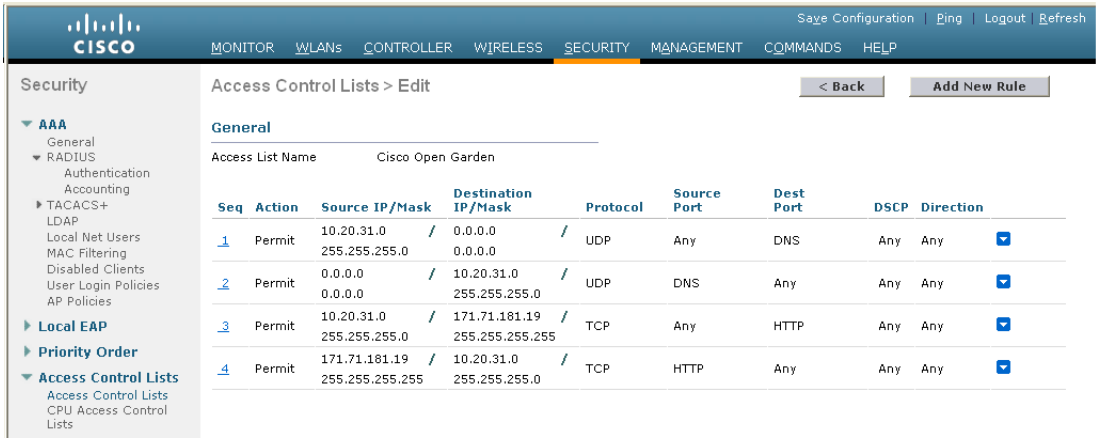


Figure 10-58 Pre-Auth ACL Example



Note If a pre-authentication ACL is used in conjunction with the web auth policy, it must include a rule to permit DNS requests; otherwise, the client is unable to resolve and connect to a destination host/URL that is otherwise allowed by the ACL.

Anchor Controller DHCP Configuration

If the anchor controller is going to manage DHCP services for the guest access WLAN, proceed with the steps below.

Note The anchor controller cannot be used to manage DHCP services if guest N+1 redundancy is being implemented, because there is no mechanism to synchronize address leases for a single guest VLAN/subnet across two or more WLCs.

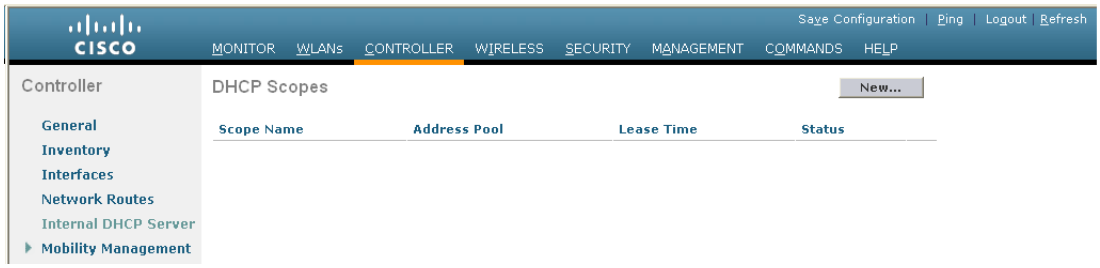
Adding a New DHCP Scope to the Anchor Controller

Step 1 Click the **Controller** tab.

Step 2 In the left pane, click **Internal DHCP Server**.

Step 3 Click **New**. (See Figure 10-59.)

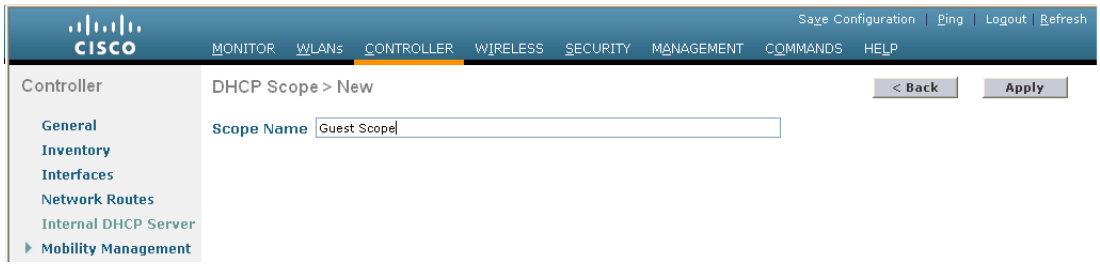
Figure 10-59 Adding a New DHCP Scope



Defining a Scope Name

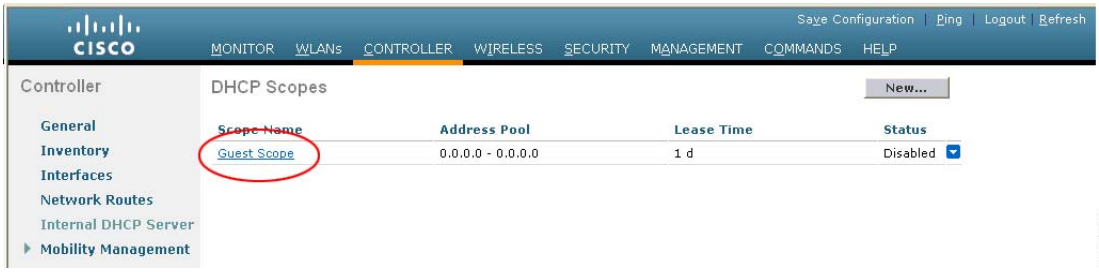
Step 4 Define a name for the scope and click **Apply**. (See Figure 10-60.)

Figure 10-60 Defining a Scope Name



Step 5 Click **Scope Name** to edit. (See Figure 10-61.)

Figure 10-61 Editing DHCP Scope



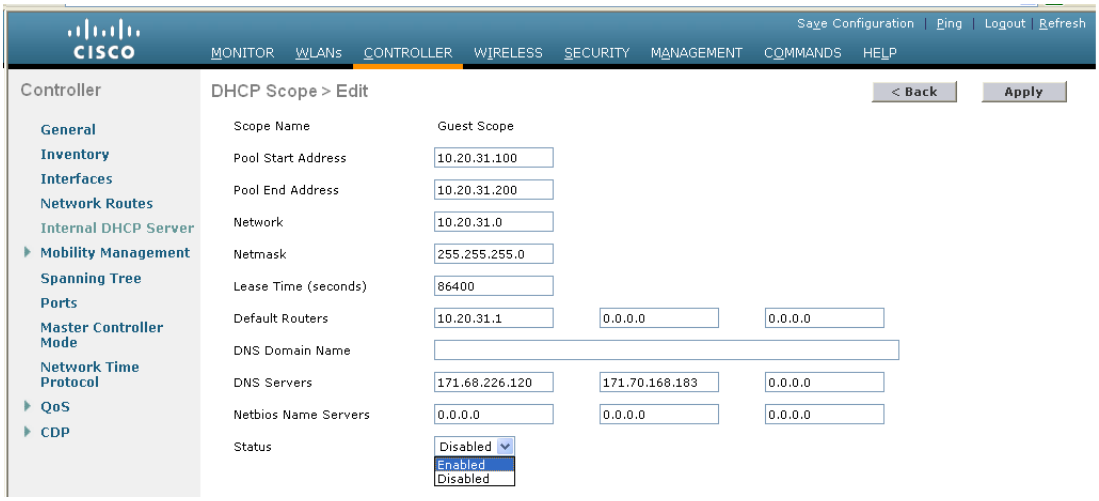
Defining Scope Properties

Step 6 Define the following minimum information:

- Pool start and stop
- Network
- Mask
- Default routers
- DNS servers

Step 7 For Status, select **Enabled** and click **Apply**. (See Figure 10-62.)

Figure 10-62 Configuring and Enabling Scope Properties



External Radius Authentication

As described in Guest User Authentication, page 10-11, an external RADIUS server can be used to authenticate guest users in place of creating and storing guest credentials locally on the anchor controller. If this method is used, the lobby admin features described in Guest Account Management, page 10-29 cannot be used. It is assumed that some other guest management system will be used in conjunction with the external RADIUS server.

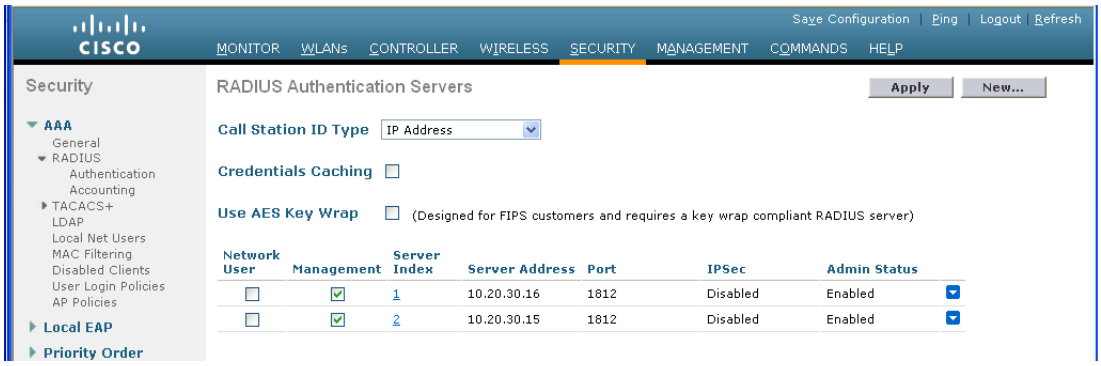
To configure a guest WLAN to use an external RADIUS server, perform the following configuration steps on the anchor controller.

Adding a RADIUS Server

Step 1 Click the **Security** tab.

A summary screen is displayed. (See Figure 10-63.)

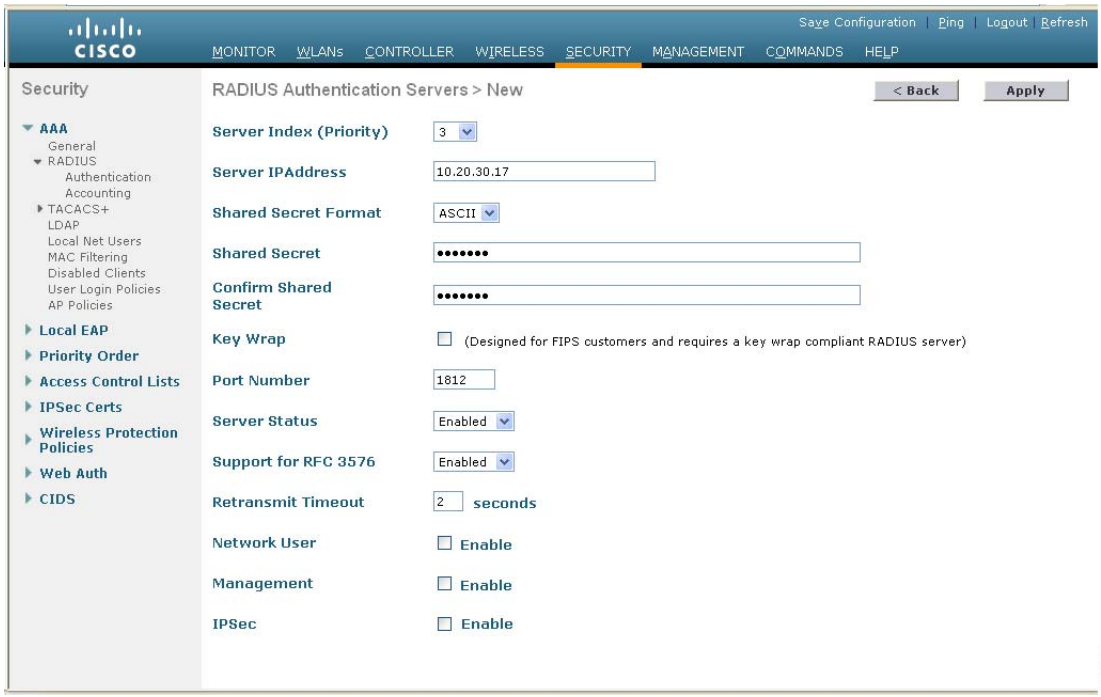
Figure 10-63 Summary Screen



Step 2 Click **New**.

The screen shown in Figure 10-64 appears.

Figure 10-64 Defining RADIUS Server Settings



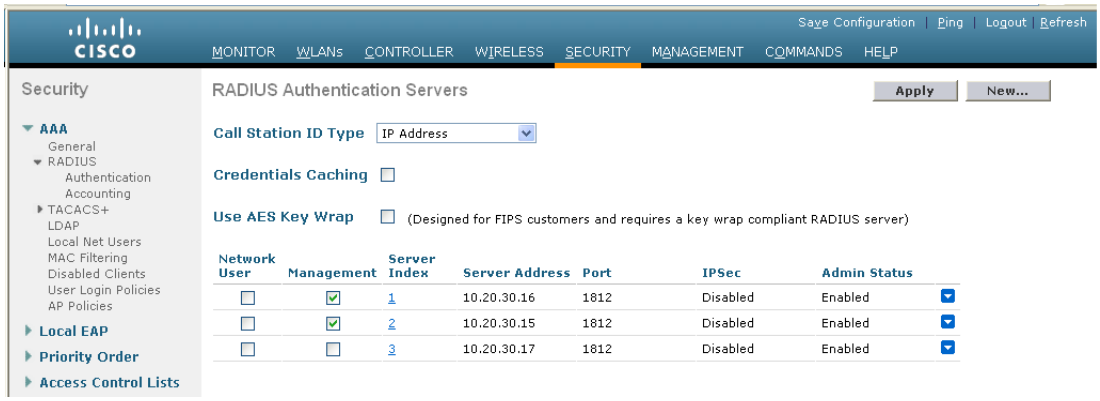
Step 3 To define RADIUS server settings, configure the IP address, shared secret, and authentication port number as defined on the RADIUS server.

If the Network User check box is cleared, the RADIUS server is used only for user authentication when it is specifically selected under the RADIUS setting of a given WLAN. Otherwise, if the Network User check box is checked, the server is used globally for all user authentications based on its server priority.

Step 4 Click **Apply**.

The summary screen shown in Figure 10-65 shows the newly-added server.

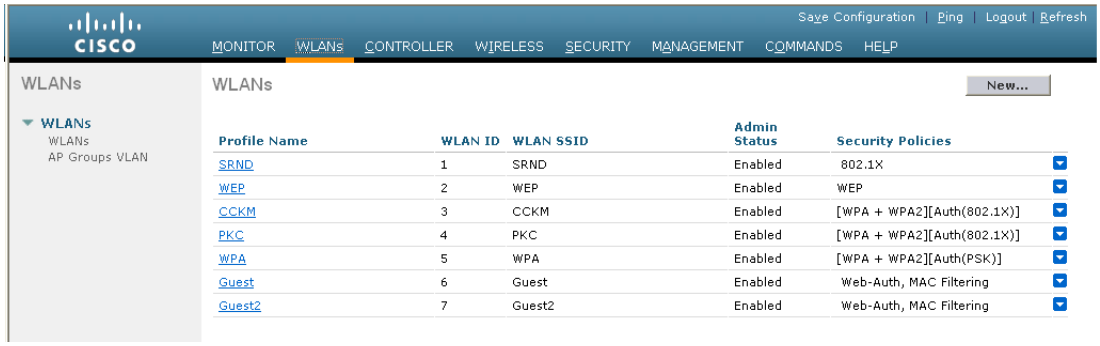
Figure 10-65 Summary Screen



Step 5 To select a RADIUS server, click the **WLANs** tab.

The screen shown in Figure 10-66 appears.

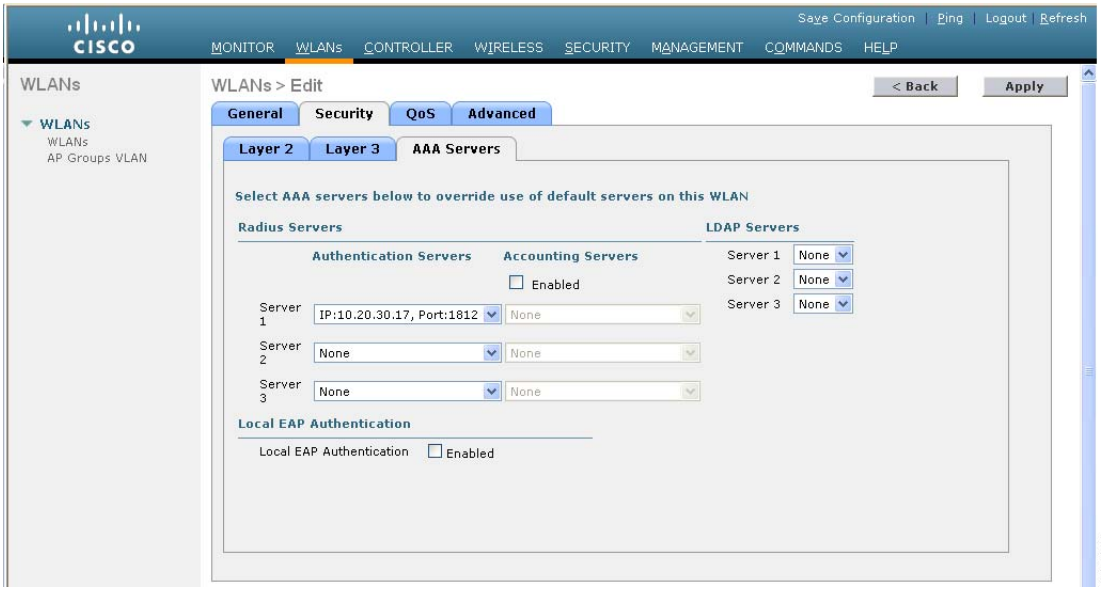
Figure 10-66 WLANs Tab



Step 6 Find the guest WLAN and click on its **Profile Name**.

The guest WLAN configuration screen is displayed, as shown in Figure 10-67.

Figure 10-67 Guest WLAN Configuration Screen



Step 7 Select **AAA Servers** under the WLAN Security tab

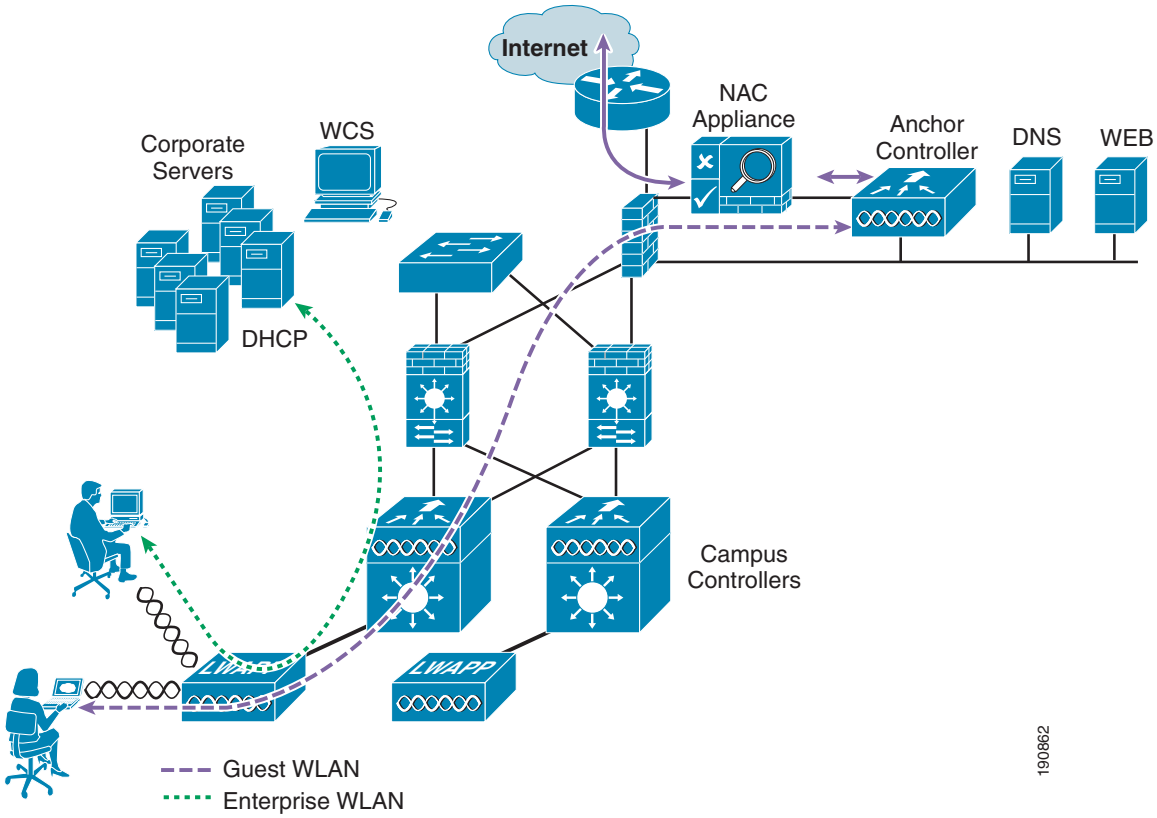
Step 8 Select the RADIUS server to be used for web authentication from the pull-down selection list under Authentication Servers.

External Access Control

The centralized guest access topology described in this chapter can be integrated with an external access control platform such the Cisco NAC Appliance.

In this scenario, an enterprise might have already deployed an access control platform in their Internet DMZ to support wired guest access services (see Figure 10-68).

Figure 10-68 Wireless Guest Access with External Access Control



As shown in Figure 10-68, the wireless guest access topology remains the same except that the guest VLAN interface on the anchor controller, instead of connecting to a firewall or border router, connects to an inside interface on an access control platform such as the Cisco NAC Appliance.

In this scenario, the NAC Appliance is responsible for redirection, web authentication, and subsequent access to the Internet. The campus and anchor controllers are used only to tunnel guest WLAN traffic across the enterprise into the DMZ, where the NAC appliance or some other platform is used to control guest access.

Configuration of the guest WLAN, campus, and anchor controllers is the same as described in the previous examples. The only exception is that Layer 3 web policy is not enabled under the guest WLAN security settings (see Figure 10-69 and Figure 10-70).

Figure 10-69 Guest WLAN Layer 3 Security Policy

Figure 10-70 Guest WLAN L2 Security Settings

The configurations above establishes a WLAN with no security policies. Guest traffic passes through the anchor controller to the inside or untrusted interface of the Cisco NAC Appliance, where it is blocked until the user has authenticated.

DHCP can be hosted locally on the controller or externally via the NAC Appliance or dedicated server.

Its beyond the scope of this chapter to address Cisco NAC Appliance or other external access control platform specific configurations. See the specific platform documentation for additional configuration guidelines.

Verifying Guest Access Functionality

The guest access service is working correctly if a user:

- Can associate to the guest WLAN
- Receives an IP address via DHCP
- Opens their browser and is redirected to the web authentication page
- Enters their credentials and connects to the Internet (or other authorized upstream services)

Troubleshooting Guest Access

The following verifications and troubleshooting tasks assume the following:

- The solution is using the web authentication functionality resident in the anchor controller(s).
- User credentials are created and stored locally on the anchor controller(s).

Before attempting to troubleshoot the various symptoms below, at the very least you should be able to ping from the campus (foreign) controller to the anchor controller(s). If not, verify routing.

Next, you should be able to perform the following advanced pings. These can only be performed via the serial console interfaces of the controllers:

- **mping** *neighbor WLC ip*

  This pings the neighbor controller through the LWAPP control channel.

- **eping** *neighbor WLC ip*

  This pings the neighbor controller through the LWAPP data channel.

If a standard ICMP ping goes through, but mpings do not, ensure that the default mobility group name of each WLC is the same, and ensure that the IP, MAC, and mobility group name of each WLC is entered in the mobility members list of every WLC.

If pings and mpings are successful, but epings are not, check the network to make sure that IP protocol 97 (Ethernet-over-IP) is not being blocked.

User Cannot Associate to the Guest WLAN

- Verify that the guest WLAN is enabled on the anchor controller and all foreign controllers that support the guest WLAN
- Verify that the guest WLAN SSID is being broadcast.
- Verify client adapter/software configuration.

User Does Not Obtain an IP Address via DHCP

- Verify that WLAN configuration settings are identical on the anchor and foreign controllers (except for WLAN interface and mobility anchors; see Guest WLAN Configuration on the Anchor WLC, page 10-27)
- Verify that the guest WLAN is enabled on the anchor WLC(s)
- Check for a proper DHCP server address under the guest VLAN interface settings on the anchor controller(s)
  - If using an external DHCP server, the IP address should be that of the external server.
  - Verify reachability to the external DHCP server from the anchor controller.
  - If using the anchor controller for DHCP services, the DHCP server IP address should be the management IP address of the controller.
  - Verify that a DHCP scope has been configured and enabled on the controller.
  - Verify that the network mask of the DHCP scope is consistent with the mask on the guest VLAN interface.
  - Verify that the DHCP scope does not overlap with any addresses assigned to the network infrastructure.

User is Not Redirected to Web Auth Page

The following assumes the user is able to associate to the guest WLAN and obtain an IP address:

- Verify that valid DNS servers are being assigned to the client via DHCP.
- Ensure that the DNS servers are reachable from the anchor controller.
- Verify that the URL being opened in the web browser is resolvable.
- Verify that the URL being opened in the web browser is connecting to HTTP port 80.

Note The internal web auth server does not redirect incoming requests on ports other than 80 and one other user defined port number (see User Redirection, page 10-9).

User Cannot Authenticate

- Verify that user credentials are active on the anchor controller(s).

  Guest credentials typically have a lifetime associated with them. If the credentials have expired, they do not appear under the Security > Local Net Users list on the anchor controller. Use WCS to re-apply the user template or re-create user credentials locally on the controller. See Guest Management Using WCS, page 10-30 and Guest Credentials Management, page 10-10.

- Verify user password.

User Cannot Connect to Internet or Upstream Service

- Verify routing to and from the anchor controller from the firewall or border router connecting to the anchor controller(s)
- Verify NAT configuration on firewall or Internet border router (if applicable)

System Monitoring

Following are some monitoring commands that might be helpful in troubleshooting.

Anchor Controller

From the serial console port:

```
Cisco Controller) >show client summary

Number of Clients................................ 1

MAC Address        AP Name            Status         WLAN  Auth  Protocol  Port

-----------------  -----------------  -------------  ----  ----  --------  ----

00:40:96:ac:5f:f8  10.15.9.19         Associated     3     Yes   Mobile    1
```

Note that the protocol is mobile. The Auth field reflects the actual status of the user. If the user has passed web auth, the field displays YES. If not, the field shows NO.

Also notice the AP name. This is the management IP address of the foreign controller (originating controller).

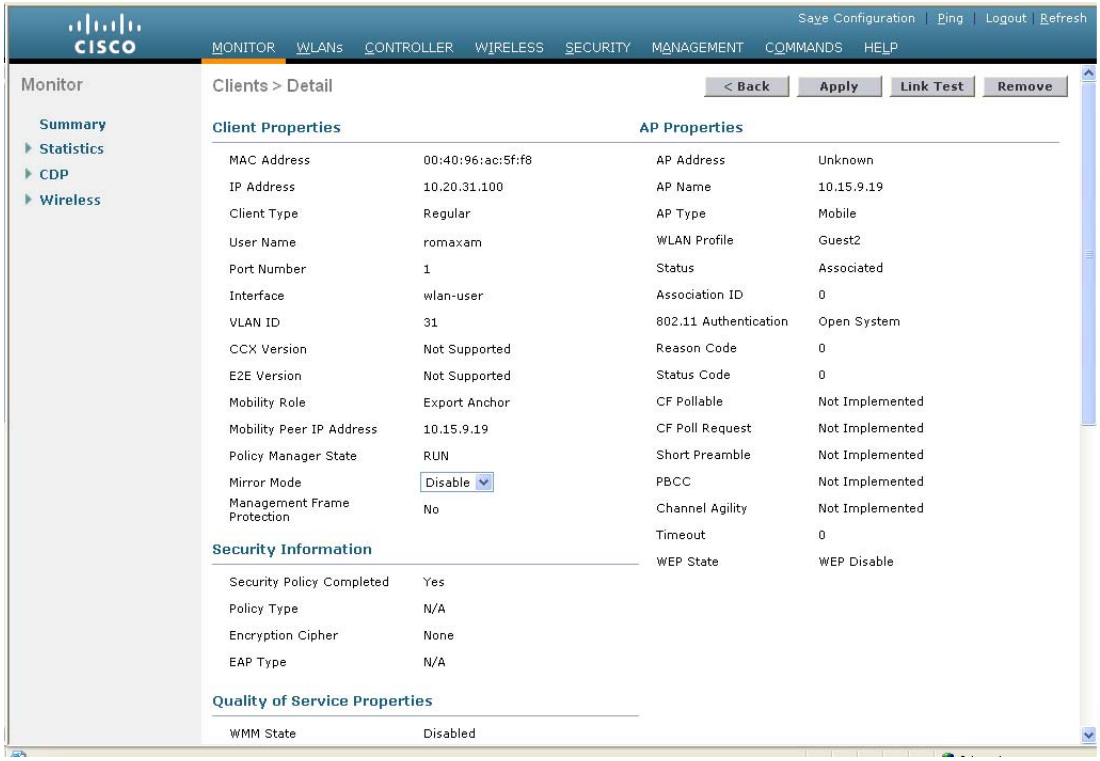
From the summary information, use the client MAC to show more detail:

```
(Cisco Controller) >show client detail 00:40:96:ac:5f:f8
Client MAC Address.............................. 00:40:96:ac:5f:f8
Client Username ................................ romaxam
AP MAC Address.................................. 00:00:00:00:00:00
Client State.................................... Associated
Wireless LAN Id................................. 3
BSSID........................................... 00:00:00:00:00:02
Channel......................................... N/A
IP Address...................................... 10.20.31.100
Association Id.................................. 0
Authentication Algorithm........................ Open System
Reason Code..................................... 0
Status Code..................................... 0
Session Timeout................................. 86316
Client CCX version.............................. No CCX support
Mirroring....................................... Disabled
QoS Level....................................... Silver
Diff Serv Code Point (DSCP)..................... disabled
802.1P Priority Tag............................. disabled
WMM Support..................................... Disabled
Mobility State.................................. Export Anchor
Mobility Foreign IP Address..................... 10.15.9.19
Mobility Move Count............................. 1
Security Policy Completed....................... Yes
Policy Manager State............................ RUN
Policy Manager Rule Created..................... Yes
NPU Fast Fast Notified.......................... Yes
Policy Type..................................... N/A
```

```
Encryption Cipher.............................. None
Management Frame Protection.................... No
EAP Type....................................... Unknown
Interface...................................... wlan-user
VLAN........................................... 31
Client Capabilities:
      CF Pollable.............................. Not implemented
      CF Poll Request.......................... Not implemented
      Short Preamble........................... Not implemented
      PBCC..................................... Not implemented
      Channel Agility.......................... Not implemented
      Listen Interval.......................... 0
Client Statistics:
      Number of Bytes Received................. 0
      Number of Bytes Sent..................... 0
      Number of Packets Received............... 0
      Number of Packets Sent................... 0
      Number of Policy Errors.................. 0
      Radio Signal Strength Indicator.......... Unavailable
      Signal to Noise Ratio.................... Unavailable
Nearby AP Statistics:
        TxExcessiveRetries: 0
        TxRetries: 0
        RtsSuccessCnt: 0
        RtsFailCnt: 0
        TxFiltered: 0
        TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]
```

The same information can be obtained through the web configuration and management interface of the controller under Clients > Detail. (See Figure 10-71.)

Figure 10-71 Anchor WLC Monitor > Client Detail



Campus (Foreign) Controller

From the serial console port:

```
(WiSM-slot3-1) >show client summary

Number of Clients.............................. 2

MAC Address        AP Name            Status         WLAN  Auth  Protocol  Port
-----------------  -----------------  -------------  ----  ----  --------  ----

00:40:96:ac:5f:f8  AP3_.18e5.7fdc     Associated     1     Yes   802.11g   29
```

Note that the protocol field is 802.11g, whereas the protocol field on the anchor controller for the same client is mobile. The campus (foreign) controller always shows the user as authenticated and the AP name reflects the actual AP to which the client is associated.

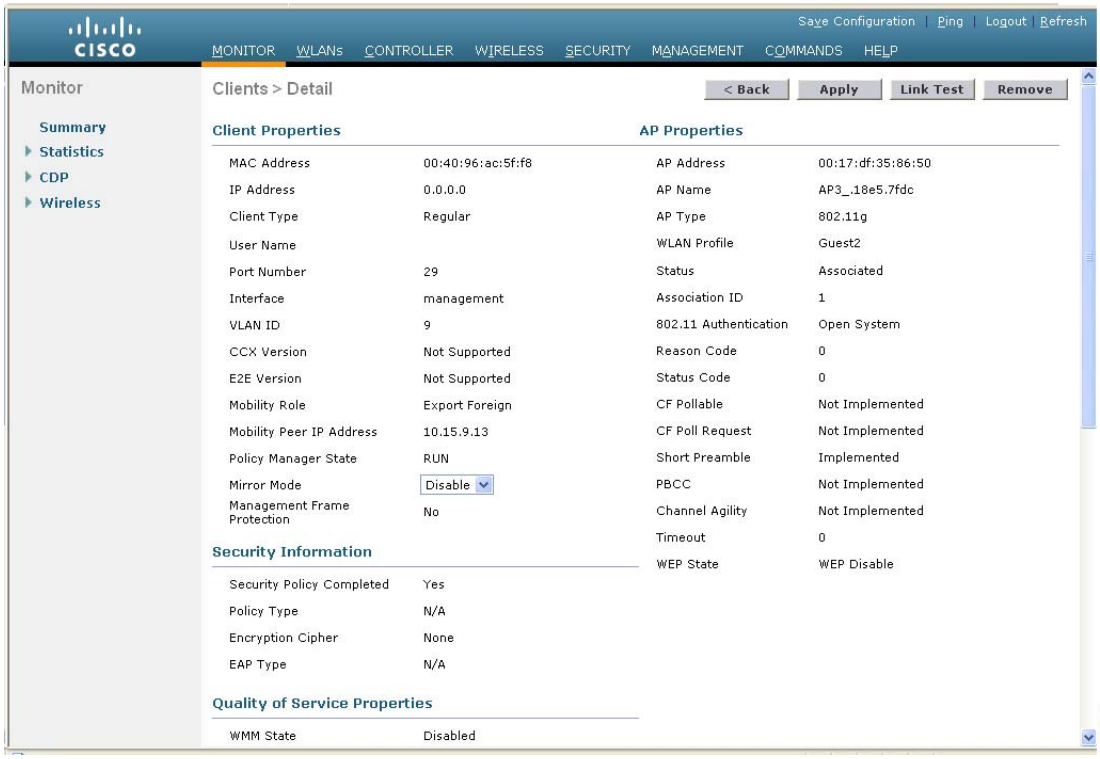
Additional details can be obtained using the following:

```
(WiSM-slot3-1) >show client detail 00:40:96:ac:5f:f8
Client MAC Address............................. 00:40:96:ac:5f:f8
Client Username ............................... N/A
AP MAC Address................................. 00:17:df:35:86:50
Client State................................... Associated
Wireless LAN Id................................ 1
BSSID.......................................... 00:17:df:35:86:50
Channel........................................ 11
IP Address..................................... Unknown
Association Id................................. 1
Authentication Algorithm....................... Open System
Reason Code.................................... 0
Status Code.................................... 0
Session Timeout................................ 0
Client CCX version............................. No CCX support
Mirroring...................................... Disabled
QoS Level...................................... Silver
Diff Serv Code Point (DSCP).................... disabled
802.1P Priority Tag............................ disabled
WMM Support.................................... Disabled
Mobility State................................. Export Foreign
Mobility Anchor IP Address..................... 10.15.9.13
Mobility Move Count............................ 0
Security Policy Completed...................... Yes
Policy Manager State........................... RUN
Policy Manager Rule Created.................... Yes
NPU Fast Fast Notified......................... Yes
Policy Type.................................... N/A
Encryption Cipher.............................. None
Management Frame Protection.................... No
EAP Type....................................... Unknown
Interface...................................... management
VLAN........................................... 9
Client Capabilities:
      CF Pollable.............................. Not implemented
      CF Poll Request.......................... Not implemented
      Short Preamble........................... Implemented
      PBCC..................................... Not implemented
      Channel Agility.......................... Not implemented
      Listen Interval.......................... 0
Client Statistics:
      Number of Bytes Received................. 308244
      Number of Bytes Sent..................... 700059
      Number of Packets Received............... 2527
      Number of Packets Sent................... 1035
```

```
      Number of Policy Errors..................... 0
      Radio Signal Strength Indicator............. -75 dBm
      Signal to Noise Ratio....................... 25 dB
Nearby AP Statistics:
        TxExcessiveRetries: 0
        TxRetries: 0
        RtsSuccessCnt: 0
        RtsFailCnt: 0
        TxFiltered: 0
        TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]
      AP3_.18e5.7fdc(slot 0) .....................
antenna0: 37 seconds ago -73 dBm.................. antenna1: 4294510568 seconds ago -128
dBm
```

The same information can be obtained through the controller web configuration and management interface under Clients > Detail (see Figure 10-72).

Figure 10-72 Foreign WLC Monitor > Client Detail



Debug Commands

Additional debug commands that might be used from the serial console include the following:

```
debug mac addr <client mac address>
debug mobility handoff enable
debug mobility directory enable
debug dhcp packet enable
debug pem state enable
debug pem events enable
debug dot11 mobile enable
debug dot11 state enable
```

CHAPTER 11

Mobile Access Router, Universal Bridge Client, and Cisco Unified Wireless

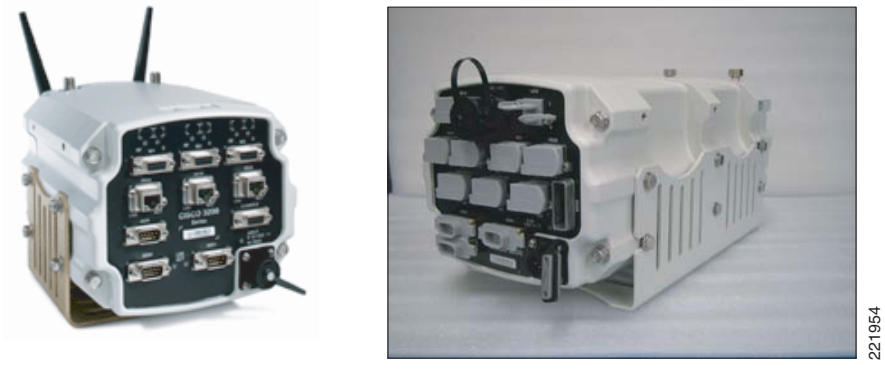
3200 Series Mobile Access Router Overview

The Cisco 3200 Series Mobile Access Router (MAR) is a compact, high-performance network access solution that offers seamless mobility and interoperability across multiple wireless networks. Its size makes it ideal for use in vehicles in defense, public safety, homeland security, and transportation. It delivers seamless communications mobility across multiple radio, cellular, satellite, and WLAN networks and can communicate mission-critical voice, video, and data across peer-to-peer, hierarchical, or meshed networks.

The Cisco 3200 router can be used to create a mobile network where devices such as PCs, surveillance cameras, digital video recorders, printers, PDAs, and scanners can all be backhauled to the home network through a wireless connection on the 3200, such as cellular or WLAN-based.

The Cisco 3200 Series consists of one or more PC104/Plus modules that stack together to form a wireless router configuration. These modular card combinations are available either as card bundles or as complete systems assembled in a Cisco 3200 rugged enclosure. The Cisco 3200 Series router bundles consist of the Cisco 3230 and the Cisco 3270 models. The left of Figure 11-1 shows the Cisco 3200 rugged enclosure bundle, and the right shows the Cisco 3270 rugged enclosure bundle.

Figure 11-1 Rugged Enclosure Bundles—Cisco 3200 (left), Cisco 3270 (right)



MAR3200 Cisco 3270

The Cisco Rugged Enclosure Option for the 3200 Series is designed for in-vehicle use, addressing the specific mobility needs of the public safety, transportation, defense, and homeland security markets. The Rugged Enclosure Option is completely sealed and is designed to withstand harsh environments, including large variations in temperature and altitude, intense shock/vibration, and exposure to dampness, moisture, or dust.

For more information and further details of the rugged enclosure, see the 3200 Rugged Enclosure data sheet at the following URL:
http://www.cisco.com/en/US/products/hw/routers/ps272/products_data_sheet0900aecd8028e3a7.html

For more information on Cisco 3200 card bundles, see the Cisco 3200 Wireless and Mobile Routers data sheet at the following URL:
http://www.cisco.com/en/US/products/hw/routers/ps272/products_data_sheet0900aecd800fe973.html

Cisco 3200 Series and Wireless Network Access

With such a vast array of wireless options and connectivity modes, the Cisco 3200 MAR can deliver *always on* IP connectivity for networks in motion. These routers are intended to be mounted in vehicles. They support Cisco IOS Mobile Networks, and provide the ability to hide the address change that potentially occurs when roaming between Layer 3 subnets from the local IP nodes. This enables IP hosts on a mobile network to connect transparently to the network while a router is in motion.

For example, a bus equipped with the 3200 MAR is able to drive around a city while passengers on board the bus stay connected to the Internet. The client computers do not need any specialized software to maintain the connections. This transparent communication is accomplished by mobile IP devices that tunnel packets to the mobile access router, and is discussed further in this chapter.

Release 4.1 of the Cisco Unified Wireless Network has added support for workgroup bridge (WGB) functionality. Before this feature enhancement, a 3200 MAR would need to use Universal Work Group Bridge (UWGB) mode to connect to a Cisco Unified Wireless network.

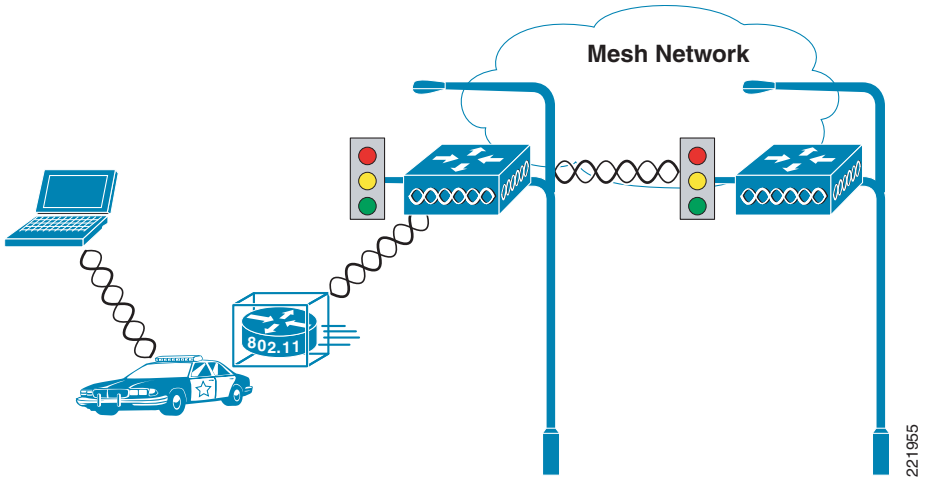
By use of WGB, a 3200 MAR can act as a WGB client to a Cisco Unified Wireless Network. Outside of supporting WGB connections to Cisco 802.11 Unified Wireless Networks, it can be used to connect to other WLAN solutions that support WGB. The UWGB of the mobile access router is not superseded by the WGB feature. In fact, it is very useful in environments where you need to connect the 3200 MAR to 802.11 wireless networks that do not support WGB mode. In these types of network connections, the 3200 MAR in UWGB mode is seen as a normal wireless client to the 802.11 wireless network.

Another wireless access method for the 3200 MAR is through use of its wired Fast Ethernet and serial interface connections. Such connections can be used to integrate cellular and satellite devices. These device type options are beyond the scope of this document; more information can be found at the following URL:
http://www.cisco.com/en/US/products/hw/routers/ps272/prod_brochure0900aecd80374174.html

Vehicle Network Example

This section describes a simple application for the 3200 MAR in a mesh network using its WGB feature to connect to the mesh WLAN (see Figure 11-2.)

Figure 11-2 Vehicle Network Example



Note the following:

- A Cisco 3200 Series router installed in a mobile unit allows the client devices in and around the vehicle to stay connected while the vehicle is roaming.
- Wireless Mobile Interface Cards (WMICs) in vehicle-mounted Cisco 3200 Series routers are configured as access points to provide connectivity for 802.11b/g and 4.9-GHz wireless clients.
- Ethernet interfaces are used to connect any in-vehicle wired clients, such as laptop, camera, or telematics devices, to the network.
- Another WMIC is configured as a WGB for connectivity to a mesh AP, allowing transparent association and authentication through a root device in the architecture as the vehicle moves about.
- Serial interfaces provide connectivity to wireless WAN modems that connect to cellular networks such as CDMA or GPRS. The wireless 802.11 connections are treated as preferred services because they offer the most bandwidth; however, when a WLAN connection is not available, cellular technology provides a backup link. Connection priority can be set by routing priority or by the priority for Mobile IP.

Simple Bridge Client Data Path Example

The IP devices connected to the MAR are not aware that they are part of a mobile network. When they must communicate with another node in the network, their traffic is sent to their default gateway, the Cisco 3200 Series router. The Cisco 3200 Series router forwards the traffic to the WLAN of the mesh AP, which then encapsulates the data packets in LWAPP and forwards them through the network to the controller.

As shown in Figure 11-3, the Cisco 3200 Series router sends traffic over the WGB backhaul link. This traffic then crosses the WLAN to the controller, where it is then forwarded out the controller interface to the wired network. Return traffic destined for any client attached to the MAR is forwarded via a static route pointing back to the controller of the mesh network.

Figure 11-3 Simple Layer 2 Data Path Example

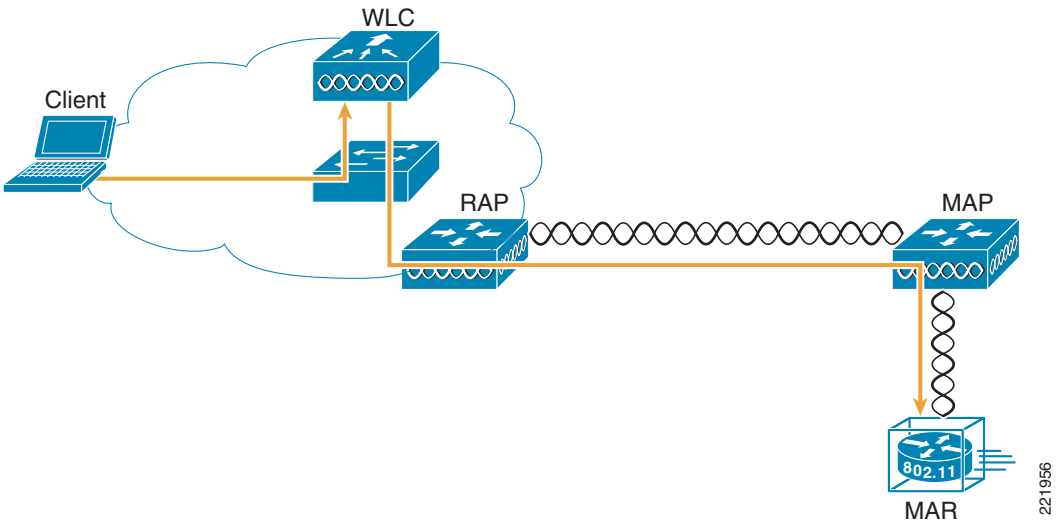
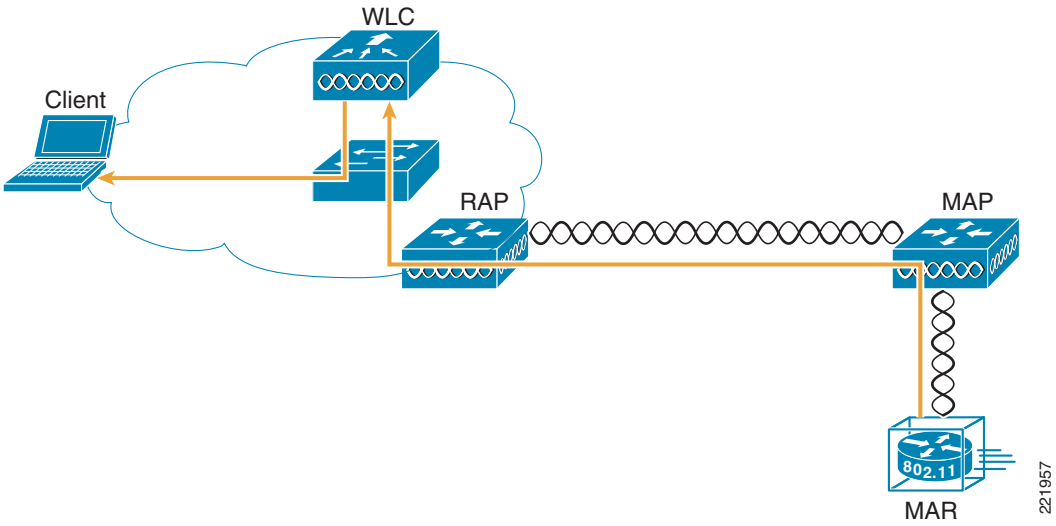


Figure 11-4 shows the return path to the MAR. Mobile IP eliminates the need for static routing and is discussed further in this chapter. NAT may be used in simple deployments when Mobile IP is not available.

Figure 11-4 Client Return Data Path



This data path example shows the traffic in a pure Layer 2 mesh when the MAR is using only the WMIC for backhaul. If the deployment calls for more complexity (such as secondary cellular backhaul links), Mobile IP is required.

Cisco 3200 Series in Mobile IP Environments

The wireless technologies used in many modern metropolitan mobile networks include 802.11 wireless mesh networks for general city-wide coverage, providing high-speed access for bandwidth-intensive applications such as in-car video. For coverage areas where it is not practical to extend the wireless mesh

network, it can be supplemented by cellular services such as CDMA 1x RTT. By using this approach, cellular services can be used to fill gaps in connections and to provide backup wireless connectivity. This added backup interface requires Mobile IP to enable client roaming between the two separate networks.

In IP networks, routing is based on stationary IP addresses, similarly to how a postal letter is delivered to a fixed address on an envelope. A device on a network is reachable through IP routing by the IP address to which it is assigned on the network. However, when networks are in motion, problems occur when a device roams away from its home network and is no longer reachable using its existing IP route. This causes the active sessions of the device to be terminated.

Mobile IP offers a solution to these roaming problems by enabling users to keep the same IP address while traveling to a different network (which may even be operated by a different wireless operator), thus ensuring that a roaming client can continue communication without sessions or connection drops.

Because the mobility functions of Mobile IP are performed at the network layer rather than the physical or link layer, mobile devices such as the Cisco 3200 can span different types of wireless and wired networks while maintaining connections and ongoing applications. Any application that requires that the Session layer be maintained is a candidate for use on a Mobile IP-enabled network connection.

For a comprehensive overview of Mobile IP networking, see Chapter 12, "Cisco Unified Wireless and Mobile IP."

WMIC Roaming Algorithm

The following four basic triggers start the WMIC scanning for a better root bridge or access point:

1. Loss of eight consecutive beacons
2. Data rate shift
3. Maximum data retry count is exceeded (the default value is 64 on the WMIC)
4. A measured period of time of a drop in the signal strength threshold

Only #3 and #4 above are configurable via the **packet retries** command and **mobile station period** *X* **threshold** *Y* (in dBm); the remainder are hard-coded.

If a client starts scanning because of a loss of eight consecutive beacons, the following message is displayed on the console: "Too many missed beacons". The WMIC in this case is acting as a universal bridge client much like any other wireless client in its behavior. An additional triggering mechanism, "mobile station," is not periodic but does have two variables; *period* and *threshold*. If a mobile station is configured, the mobile station algorithm evaluates two variables (data rate shift and signal strength) and responds as follows:

- If the driver does a long-term downshift in the transmit rate for packets to the parent, the WMIC initiates a scan for a new parent (no more than once every configured period).
- If the signal strength (threshold) drops below a configurable level, the WMIC scans for a new parent (no more than once every configured period).

The data-rate shift can be displayed with the following command.

```
debug dot11 dot11Radio 0 trace print rates
```

However, this does not show the actual "data rate shift" algorithm in action, but only the changes in data rate. This determines the time period to scan depending on how much the data rate was decreased.

The period should be set depending on the application; default is 20 seconds. This delay period prevents the WMIC from constantly scanning for a better parent if, for example, the threshold is below the configured value.

The threshold sets the level at which the algorithm is triggered to scan for a better parent. This threshold should be set to *noise+20dBm* but not more than -70dBm (+70 because input for threshold is positive). The default is -70 dBm.

Basic Configuration Examples

This section provides a configuration example for the 3200 MAR. It can be used as a step-by-step process to configure the UWGB client using open authentication and WEP encryption. This section also covers other basic configuration steps such as VLAN creation, assignment, and DHCP.

Connecting to the Cisco 32XX

Step 1 Attach the console cable to both the serial port of your PC and the Mobile Access Router console port (DB9 female). Use a straight through DB9-to-DB9 cable.

Note You can also use the same console cable used to access the HA, with the addition of an RJ-45 to DB9 female adapter.

Configure IP Address, DHCP, VLAN on 3200 Series

Step 2 Connect to and log into the mobile router. Create a loopback interface and assign an IP address.

Step 3 Create VLAN 2 in the VLAN database using the **vlan database** CLI command.

Step 4 Configure the VLAN 3 and VLAN 2 interfaces.

VLAN 3 is used for the 2.4 GHz WMIC2 (W2), which is acting as AP. VLAN 2 is used for the 4.9 GHz WMIC (W3). Configure FA2/0, FA2/1, and FA2/3 to be in VLAN 3, and FA 2/2 to be in VLAN 2.

Step 5 Create VLAN 4 in the VLAN database for connection between WMIC 1 and MARC. (See Table 11-1.)

Table 11-1 Interface Examples

Connected to	Interface	Radio Type	VLAN	Description
PC	FastEthernet2/0	None	3	Fast Ethernet link for end device.
WMIC 1 (W1)	FastEthernet2/1	2.4 GHz	4	2.4 GHz UWGB connection to mesh network
WMIC 2 (W2)	FastEthernet2/3	2.4 GHz	3	Provides 2.4 GHz AP hotspot around mobile router
WMIC 3 (W3)	FastEthernet2/2	4.9 GHz	2	4.9 GHz uplink as workgroup bridge

Step 6 Configure DHCP server for VLAN 3 using following command:

```
ip dhcp pool mypool
   network 10.40.10.0  /28
default-router 10.40.10.1
ip dhcp excluded-address 10.40.10.1 10.40.10.3
```

Step 7 Verify that the wired client on VLAN 3 is properly assigned a DHCP IP address in the 10.40.10.0/28 subnet.

WMIC Configurations

WMIC Work Group Bridge Configuration

WMICs can support the WGB client mode for 802.11 associated connections. This is the only operating mode that supports the **distance** command. It is also the suggested mode to configure for the MAR in a Cisco mesh environment because it overcomes limitations known to the UWGB client mode. For more information on UWGB including its limitations, see WMIC Universal Bridge Client Configuration, page 11-8.

There are the following three install modes for WGB:

- *Automatic* activates the bridge install and alignment mode, and specifies that the unit automatically determines the network role. If the unit is able to associate to another Cisco root device within 60 seconds, the unit assumes a non-root bridge role. The device can be configured into root bridge or non-root bridge modes to avoid the 60-second automatic detection phase.
- *Root* specifies that the device is operating as a root bridge and connects directly to the main Ethernet LAN network. In this mode, the unit accepts associations from other Cisco bridges and wireless client devices.
- *Non-root* specifies that the device is connecting to a remote LAN network, and that it must associate with a Cisco root device by using the wireless interface.

Follow these steps to configure the WMIC to determine is role automatically:

Step 1 Under the dot11 interface, enter the following command.

```
station-role {root [bridge | non-root workgroup-bridge install [automatic | root |
non-root]}
```

The **station-role** command specifies that the role of the WMIC is chosen based on the device to which it is associated.

Step 2 Set the WMIC role.

- **station-role root bridge**—Specifies that the 3200 MAR WMIC operates as the root bridge device. This mode does not support wireless client associations.
- **station-role workgroup-bridge**—Specifies that the 3200 MAR WMIC operates in workgroup bridge mode. As a workgroup bridge, the device associates to an Aironet access point or bridge as a client and provides a wireless LAN connection for devices connected to its Ethernet port.

Step 3 Issue the mobile station command.

```
mobile station
```

Use this command to configure a non-root bridge or workgroup bridge as a mobile station. When this feature is enabled, the bridge scans for a new parent association whenever it encounters a poor received signal strength indicator (RSSI), excessive radio interference, or a high frame loss percentage. Using

these criteria, the WMIC searches for a new root association and roams to a new root device before it loses its current association. When the mobile station setting is disabled (the default setting) the WMIC does not search for a new association until it loses its current association.

WMIC Universal Bridge Client Configuration

The WMIC can be configured as a UWGB, as is discussed in the beginning of this section. UWGB mode enables support for the WMIC in a network 802.11 network environment that does not support WGB. For example, this may be a non-Cisco mesh network. The current limitation of using UWGB mode clients on a Cisco Unified Wireless Network is that you can only have one UWGB client per AP.

In this role, the WMIC has the following functionality:

- Associates to IOS and non-IOS access points.
- Interoperability—The UWGB can forward routing traffic using a non-Cisco root device as a universal client. The UWGB appears as a normal wireless client to the root device. As a root device, the WMIC supports Cisco Compatible Extension clients, with all Cisco Compatible Extension v3 features and many v4 features.

```
station-role workgroup-bridge universal (mac address)
```

Note You must use the MAC address of the associated VLAN to which the WMIC is bridged. As an example use the MAC address of VLAN one. To acquire the MAC address of VLAN one, console in to the MAR router card and issue the command **show mac-address-table**.

WMIC as an Access Point Configuration

The WMIC can be configured as a root access point. In this role, it accepts associations from wireless clients. This can be a useful configuration if you are planning to deploy a mobile hotspot. Issue the following command in the dot11 interface configuration to configure the WMIC as an access point:

```
station-role root access-point
```

This specifies that the WMIC functions as a root access point.

Security

The security section of this chapter does not fully discuss in detail the underlying concepts behind the security features of the 3200 MAR; for more in depth information on these security mechanisms, see Chapter 4, “Cisco Unified Wireless Network Architecture—Base Security Features.”

Authentication Types

This section describes the authentication types that you can configure on the WMIC. The authentication types are tied to the SSID that you configure on the WMIC. Before wireless devices can communicate, they must authenticate to each other using open, 802.1x/EAP-based, or shared-key authentication. For maximum security, wireless devices should also authenticate to your network using EAP authentication, which is an authentication type that relies on an authentication server on your network.

The WMIC uses four authentication mechanisms or types and can use more than one at the same time.

The following are the four authentication types that the WMIC can use:

- Open authentication to the WMIC
- Shared key authentication to the WMIC
- EAP authentication to the network
- MAC address authentication to the network

For more information on authentication mechanisms, see Chapter 4, "Cisco Unified Wireless Network Architecture—Base Security Features."

Encryption and Key Management

The 3200 MAR WMIC supports Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Cisco Centralized Key Management (CCKM) for encryption and key management. Further information on these security topics can be found in Chapter 4, "Cisco Unified Wireless Network Architecture—Base Security Features."

Security Configuration

The default SSID on the WMIC is *autoinstall*, which is also configured as guest mode. In guest mode, the WMIC broadcasts this SSID in its beacon and allows client devices with no SSID to associate. Also by default, the authentication types assigned to autoinstall are open. This enables clients with no security settings whatsoever to connect to the 3200 MAR. To secure the MAR, this configuration default must be changed.

Assigning Authentication Types to an SSID

The commands following in this section cover the steps to configuring authentication types for SSIDs on a WMIC in root device mode. Each command is followed by a description of the command components and any optional configuration components.

- **dot11 ssid** *ssid-string*

  This command defines an SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.

- **authentication open [mac-address** *list-name* [alternate]] [[optional] **eap** *list-name*]
  - (Optional) Sets the authentication type to open for this SSID. Open authentication allows any client device to authenticate and then attempt to communicate with the WMIC.
  - (Optional) Sets the SSID authentication type to open with MAC address authentication. The access point forces all client devices to perform MAC address authentication before they are allowed to join the network. For *list-name*, specify the authentication method list. Additional information on method lists may be found at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfathen.html.

    Use the alternate keyword to allow client devices to join the network using either MAC or EAP authentication; clients that successfully complete either authentication are allowed to join the network.

  - (Optional) Sets the SSID authentication type to open with EAP authentication. The WMIC forces all other client devices to perform EAP authentication before they are allowed to join the network. For *list-name*, specify the authentication method list. Use the optional keyword to allow client devices using either open or EAP authentication to associate and become authenticated. This setting is used mainly by service providers that require special client accessibility.

Note A root device configured for EAP authentication forces all client devices that associate to perform EAP authentication. Client devices that do not use EAP cannot communicate with the root device.

- **authentication shared**

  [**mac-address** *list-name*] [**eap** *list-name*]

  - (Optional) Sets the authentication type for the SSID to shared key.

Note Because of shared key's security flaws, Cisco recommends that you avoid using it.

Note You can assign shared key authentication to only one SSID.

  - (Optional) Sets the SSID authentication type to shared key with MAC address authentication. For *list-name*, specify the authentication method list.
  - (Optional) Sets the SSID authentication type to shared key with EAP authentication. For *list-name*, specify the authentication method list.
- **authentication network-eap** *list-name* [**mac-address** *list-name*]
  - (Optional) Sets the authentication type for the SSID to use EAP for authentication and key distribution.
  - (Optional) Sets the SSID authentication type to Network-EAP with MAC address authentication. All client devices that associate to the access point are required to perform MAC address authentication. For *list-name*, specify the authentication method list.
- **authentication key-management** {[wpa] [cckm]} [optional]
  - (Optional) Sets the key-management type for the SSID to WPA, CCKM, or both. If you use the **optional** keyword, client devices not configured for WPA or CCKM can use this SSID. If you do not use the **optional** keyword, only WPA or CCKM client devices are allowed to use the SSID. To enable CCKM for an SSID, you must also enable Network-EAP authentication. To enable WPA for an SSID, you must also enable Open authentication or Network-EAP, or both.

Note Only 802.11b and 802.11g radios support WPA and CCKM simultaneously.

Note Before you can enable CCKM or WPA, you must set the encryption mode to a cipher suite that includes TKIP/AES-CCMP. To enable both CCKM and WPA, you must set the encryption mode to a cipher suite that includes TKIP.

Note If you enable WPA for an SSID without a pre-shared key, the key management type is WPA. If you enable WPA with a pre-shared key, the key management type is WPA-PSK.

Note To support CCKM, your root device must interact with the WDS device on your network.

Configuring dot1x Credentials

The commands in this section cover the steps to configure dot1x credentials for use with EAP. Each command is followed by a description of the commands components and any optional configuration components.

1. **eap profile** *profile-name-string*

   Creates the EAP profile.

2. **dot1x credentials** *profile*

   Creates a dot1x credentials profile and enters the dot1x credentials configuration submode.

3. **method [fast|gtc|leap|md5|mschapv2|tls]**

   Chooses an EAP authentication method for authentication purposes.

Note A device configured for EAP authentication forces all root devices that associate to perform EAP authentication. Root devices that do not use EAP cannot communicate with the device.

4. **dot11 ssid** *ssid-string*
5. **authentication network-eap** *list-name*

   (Optional) Sets the authentication type for the SSID to use EAP for authentication and key distribution.

6. **dot1x credentials** *profile*

   Creates a dot1x credentials profile and enters the dot1x credentials configuration submode.

7. **dot1x eap profile** *profile-name-string*

   Specifies the EAP profile. This is the profile created in step 2 above.

8. **authentication key-management {[wpa] [cckm]} [optional]**

   (Optional) Sets the key-management type for the SSID to WPA, CCKM, or both. If you use the **optional** keyword, client devices not configured for WPA or CCKM can use this SSID. If you do not use the **optional** keyword, only WPA or CCKM client devices are allowed to use the SSID. To enable CCKM for an SSID, you must also enable Network-EAP authentication. To enable WPA for an SSID, you must also enable Open authentication or Network-EAP or both.

Note Only 802.11b and 802.11g radios support WPA and CCKM simultaneously.

Note Before you can enable CCKM or WPA, you must set the encryption mode to a cipher suite that includes TKIP/AES-CCMP. To enable both CCKM and WPA, you must set the encryption mode to a cipher suite that includes TKIP.

Note If you enable WPA for an SSID without a pre-shared key, the key management type is WPA. If you enable WPA with a pre-shared key, the key management type is WPA-PSK.

Note To support CCKM, your root device must interact with the WDS device on your network.

EAP-TLS Authentication with AES Encryption Example

Use the **no** form of the SSID commands to disable the SSID or to disable SSID features. This example sets the authentication type for the SSID *bridgeman* to open with EAP authentication. Bridges using the SSID *bridgeman* attempt EAP authentication using the EAP method name *adam*. This example sets the authentication type for the SSID *bridgeman* to perform EAP-TLS authentication with AES encryption. Bridges using this SSID attempt EAP authentication using a server ID named *adam*.

```
!
dot11 ssid bridgeman
authentication open eap eap_adam
authentication network-eap eap_adam
authentication key-management wpa
infrastructure-ssid
!
!
interface dot11radio 0
encryption mode ciphers aes-ccm
ssid bridgeman
!
```

The configuration on workgroup bridges, non-root bridges, and repeater bridges associated to this bridge would also contain the following commands:

```
!
eap profile authProfile
method tls
exit
!
dot1x credentials authCredentials
username adam
password adam
!
dot11 ssid bridgeman
authentication open eap eap_adam
authentication network-eap eap_adam
authentication key-management wpa
dot1x eap_profile authProfile
dot1x credentials authCredentials
infrastructure-ssid
!

interface dot11radio 0
encryption mode ciphers aes-ccm
ssid bridgeman
```

```
!
!
```

This example shows the RADIUS/AAA configuration on the root side for EAP authentication.

```
!
aaa new-model
aaa group server radius rad_eap
server 13.1.1.99 auth-port 1645 acct-port 1646
!
aaa authentication login eap_adam group rad_eap
aaa session-id common
radius-server host 13.1.1.99 auth-port 1645 acct-port 1646 key 7 141B1309
radius-server authorization permit missing Service-Type
ip radius source-interface BVI1
!
```

Configuring the Root Device Interaction with WDS

To support non-root bridges using CCKM, your root device must interact with the WDS device on your network, and your authentication server must be configured with a username and password for the root device. For detailed instructions on configuring WDS and CCKM on your wireless LAN, see Chapter 11 in the *Cisco IOS Software Configuration Guide for Cisco Access Points* at the following URL: http://www.cisco.com/en/US/docs/wireless/access_point/12.2_13_JA/configuration/guide/i12213sc.html.

On your root device, enter the following command in global configuration mode:

```
bridge(config)# wlccp ap username username password password
```

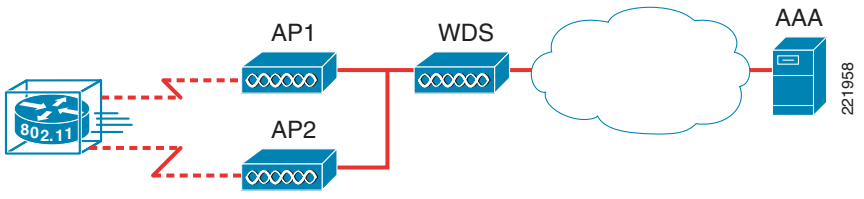
Note You must configure the same username and password pair when you set up the root device as a client on your authentication server.

In this WDS/CCKM configuration, the client and APs interact as follows:

- AP1 and AP2 authenticate with WDS
- WDS caches the client security credentials
- At association, AP1 gets the key materials to derive dynamic keys for session
- At re-association, AP2 gets the key materials to derive dynamic keys for session
- Client authenticates with RADIUS server only once

Figure 11-5 shows the client, AP, and WDS relations.

Figure 11-5 WDS/CCKM Interactions



Configuring Additional WPA Settings

Use two optional settings to configure a pre-shared key on the bridge and adjust the frequency of group key updates.

Setting a Pre-Shared Key

To support WPA on a wireless LAN where 802.1x-based authentication is not available, you must configure a pre-shared key on the bridge. You can enter the pre-shared key as ASCII or hexadecimal characters. If you enter the key as ASCII characters, you enter between 8 and 63 characters, and the bridge expands the key using the process described in the *Password-based Cryptography Standard* (RFC2898). If you enter the key as hexadecimal characters, you must enter 64 hexadecimal characters. Keep in mind that WPA-PSK is susceptible to some known attack tools. However, note that the WPA-PSK authentication mechanism was intended to be used for consumer networks, not small-to-medium businesses or enterprise networks, and is not suggested to be used in an enterprise-class WGB or mesh environment.

Fortunately, off-line dictionary attacks are not very effective against WPA-PSK networks, because of the IEEE selection of the pbkdf2 algorithm for PSK hashing. A key generated from a passphrase of less than approximately 20 characters is likely to be vulnerable to a dictionary attack. If you intend to use WPA-PSK, it is recommended that you use only truly random keys.

Configuring Group Key Updates

In the last step in the WPA process, the root device distributes a group key to the authenticated non-root bridge. You can use the following optional settings to configure the root device to change and distribute the group key based on association and disassociation of non-root bridges:

- Membership termination—The root device generates and distributes a new group key when any authenticated non-root bridge disassociates from the root device. This feature keeps the group key private for associated bridges.
- Capability change—The root device generates and distributes a dynamic group key when the last non-key management non-root bridge disassociates, and it distributes the statically configured key when the first non-key management non-root bridge authenticates. In WPA migration mode, this feature significantly improves the security of key-management capable clients.

Beginning in privileged EXEC mode, follow these steps to configure a WPA pre-shared key and group key update options:

1. Enter SSID configuration mode for the SSID:

   ```
   dot11 ssid ssid-string
   ```

2. Enter a pre-shared key for bridges using WPA that also use static WEP keys.

   ```
   wpa-psk { hex | ascii } [ 0 | 7 ] encryption-key
   ```

   Enter the key using either hexadecimal or ASCII characters. If you use hexadecimal, you must enter 64 hexadecimal characters to complete the 256-bit key. If you use ASCII, you must enter a minimum of 8 letters, numbers, or symbols, and the bridge expands the key for you. You can enter a maximum of 63 ASCII characters.

WPA and Pre-shared Key Configuration Example

The following example shows how to configure a pre-shared key for non-root bridges using WPA and static WEP, with group key update options:

```
!
!
dot11 ssid given-ssid
wpa-psk ascii talboeitm65
!
!
```

Cisco 3200 Series Product Details

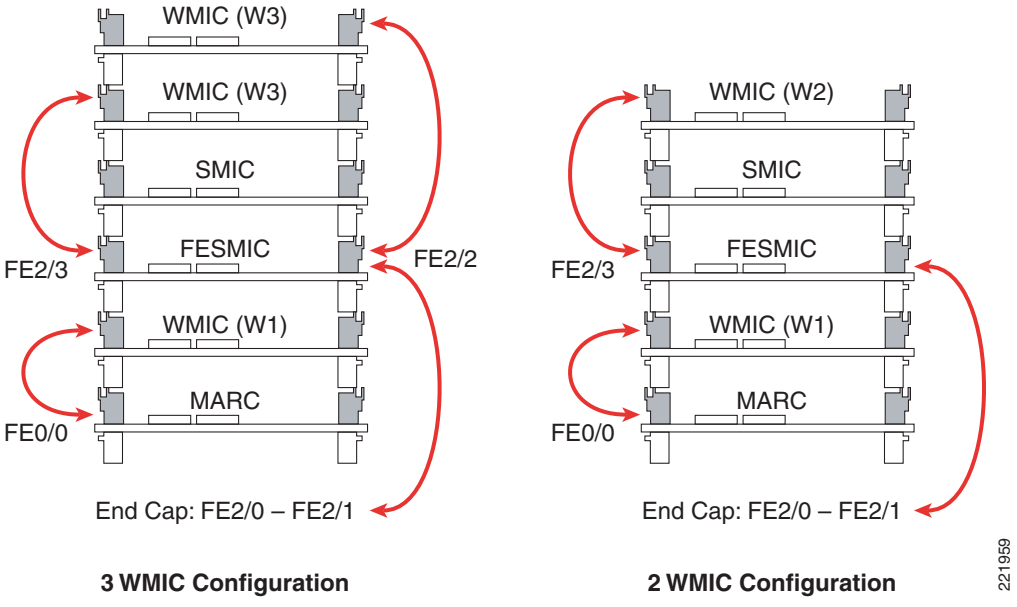
Cisco 3200 Series Interfaces

As mentioned in the previous section, the 3200 MAR Series router can be custom-designed with an assortment of PC104/Plus modules per your application needs. It is possible to design the routers for multiple Ethernet and serial interfaces as well as up to three WMIC cards. The router itself consists of stackable PC104/Plus modules referred to as *cards*. It can have up to the following card configurations:

- Two 2.4 GHz wireless WMICs
- One 4.9 GHz WMIC
- One Fast Ethernet Switch Mobile Interface Card (FESMIC)
- One Serial Mobile Interface Card
- One Mobile Access Router Card (MARC)

Figure 11-6 shows this stackable card configuration. For the more common applications, the ruggedized enclosure 3230 and 3270 bundles are available.

Figure 11-6 Card Connections



As displayed in Figure 11-6, there are two examples of possible 3200 MAR configurations:

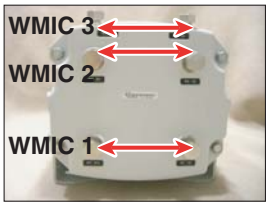
- Two WMICs, a FESMIC, a SMIC, and a MARC
- Three WMICs, a FESMIC, a SMIC, and a MARC

For more information on 3200 MAR configuration options, see the following URL: http://www.cisco.com/en/US/products/hw/routers/ps272/products_data_sheet0900aecd800fe973.html.

Cisco 3230 Enclosure Connections

On the back of the Cisco 3230 MAR enclosure, there are three pairs of RP-TNC connectors. Each pair corresponds to a single WMIC card. The pair on the bottom belongs to the W1 card. The next pair above this belongs to W2. The pair on the very top of the mobile router belongs to W3. Figure 11-7 shows the antenna connections.

Figure 11-7 WMIC RP TNC Locations



The following tables mark the port to interface relations, to assist in configurations when you need to plug other devices into the 3200 MAR.

Table 11-2 shows the setup of WMICs on the Cisco 3230 MAR.

Table 11-2 WMIC Ports

	Internal Wiring Ports
WMIC 1 (W1)	FastEthernet 2/1
WMIC 2 (W2)	FastEthernet 2/3
WMIC 3 (W3)	FastEthernet 2/2

Table 11-3 shows the setup of serial interfaces on the Cisco 3230 MAR.

Table 11-3 SMIC Ports

	Internal Wiring Ports	Interface Type
Serial 0	Serial 1/0	DSCC4 Serial
Serial 1	Serial 1/1	DSCC4 Serial
Internal	Serial 1/2	DSCC4 Serial
Internal	Serial 1/3	DSCC4 Serial

Cisco 3270 Rugged Enclosure Configuration

The newly-released Cisco 3270 mobile access router offers increased port density, fiber, and Gigabit Ethernet capabilities. Because of the internal changes of the platform, a larger profile was needed. To accommodate the high performance 3270 router card and its additional interfaces, the rugged enclosure

for the 3270 is approximately double the size of the rugged enclosure used to house the 3230 bundles. This allows for greater expansion of PC104+ cards when compared to the maximum capacity of seven cards in the rugged enclosure for the Cisco 3230 bundles.

The Cisco 3270 router maintains the similar concept of having internally-connected WMICs. The interconnectivity of the WMICs is identical to that described in the previous section for the 3230 bundle. To maximize the real estate on the 3270 enclosure end cap, the RJ-45 WMIC console ports are dynamic in the sense that they are converted to Fast Ethernet ports when the associated WMIC is absent. These connections are shown in Figure 11-8.

Figure 11-8 Cisco 3270

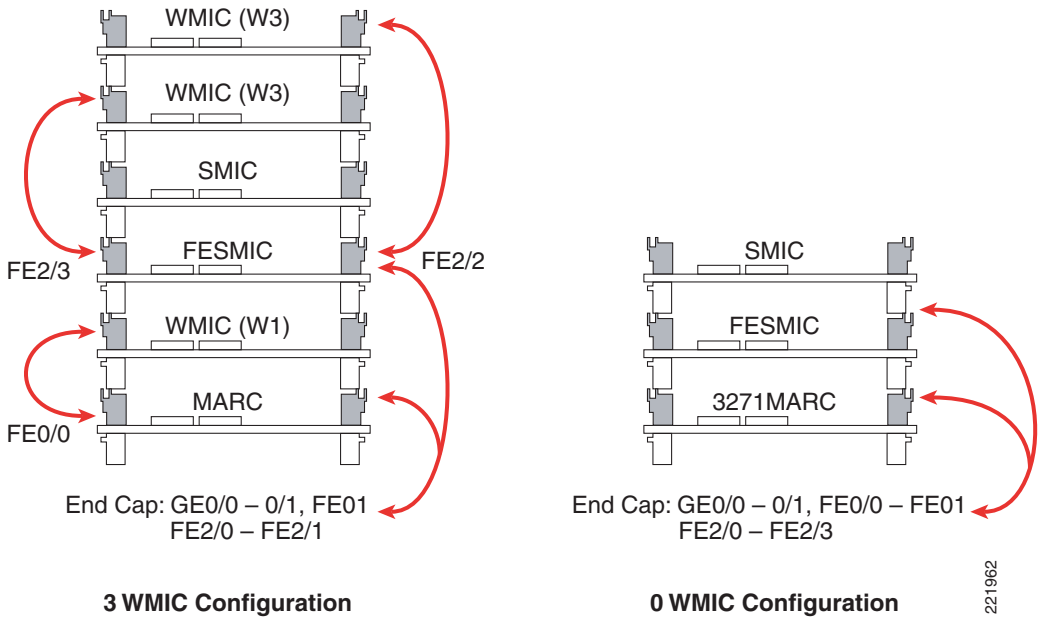
Because the 3270 enclosure has the capability to convert the unused RJ-45 WMIC console ports into Fast Ethernet interfaces on the end cap, it has the capacity to allow all eight ports of the 3270 to be brought out to the end cap. The 3270 also maintains the capability of an async/sync serial port through the smart serial interface that is brought out on the end cap.

The Cisco 3270 Rugged Router has a high-performance processor card designed to support multiple applications running concurrently over wired or wireless networks. With onboard hardware encryption, the Cisco 3270 offloads encryption processing from the router CPU to provide secure data services for mobile networks.

With a form factor roughly twice that of the Cisco 3251 Mobile Access Router Card (MARC), the Cisco 3270 allows for connection of a greater number of peripheral devices, including a broader selection of network interfaces such as fiber, Gigabit Ethernet copper, and universal serial bus (USB). In addition, the Cisco 3270 can support a second stack of PC/104-Plus cards for future card expansion, and it fully supports the 3201 Mobile Interface Cards listed above.

Figure 11-9 shows two configuration option examples for the Cisco 3270 MAR.

Figure 11-9 3270 WMIC Configuration Options



For further details, see the Cisco 3200 Rugged Enclosure data sheet at the following URL: http://www.cisco.com/en/US/products/hw/routers/ps272/products_data_sheet0900aecd804c207b.html

Cisco 3200 Series WMIC Features

WMICs running Cisco IOS offer the following software features:

- VLANs

  Allows dot1Q VLAN trunking on both wireless and Ethernet interfaces. Up to 32 VLANs can be supported per system.

- QoS

  This feature supports quality of service for prioritizing traffic on the wireless interface. The WMIC supports the required elements of WMM for QoS, which improves the user experience for audio, video, and voice applications over a Wi-Fi wireless connection and is a subset of the IEEE 802.11e QoS specification. WMM supports QoS prioritized media access through the EDCA method.

- Multiple BSSIDs

  Supports up to eight BSSIDs in access point (AP) mode.

- RADIUS accounting

  When running the WMIC in AP mode, you can enable the WMIC to send accounting data about authenticated wireless client devices to a RADIUS server on your network.

- TACACS+ administrator authentication

  TACACS+ for server-based, detailed accounting information and flexible administrative control over authentication and authorization processes. This provides secure, centralized validation of administrators attempting to gain access to your WMIC.

- Enhanced security

Supports three advanced security features:

  - WEP keys—Message Integrity Check (MIC) and WEP key hashing CKIP
  - WPA
  - WPA2

- Enhanced authentication services

  Allows non-root bridges or workgroup bridges to authenticate to the network like other wireless client devices. After a network username and password for the non-root bridge or workgroup bridge are set, LEAP, EAP-TLS, or EAP-FAST can be used for authentication in dynamic WEP, WPA, or WPA2 configurations.

- 802.1x Authenticator

  In AP mode, the MAR supports standard 802.1x EAP types for WLAN clients.

- Fast secure roaming

  Uses CCKM in WGB mode and UWGB mode.

- Universal workgroup bridge

  Supports interoperability with non-Cisco APs as a client.

- Repeater mode

  Allows the access point to act as a wireless repeater to extend the coverage area of the wireless network.

Cisco 3200 Series Bridge Considerations

The **C**isco **C**ompatible eXtensions program delivers advanced WLAN system-level capabilities and Cisco-specific WLAN innovations to third-party Wi-Fi-enabled laptops, WLAN adapter cards, PDAs, Wi-Fi phones, and application-specific devices (ASDs). The 2.4 GHz WMIC provides CCX client support. When the 2.4 GHz WMIC is configured as a universal workgroup bridge client, it does not identify itself as a Cisco Compatible Extensions client; however, it does support Cisco Compatible Extensions features. Table 11-4 lists the supported features.

More information on the Cisco Compatible Extensions program can be found on the Cisco Compatible Extensions home page at the following URL: http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_concept_home.html.

Table 11-4 Cisco Compatible Extensions Version Feature Support

Feature	v1	v2	v3	v4	AP	WGB	WGB Client
Security							
Wi-Fi Protected Access (WPA)		X	X	X	X	X	X
IEEE 802.11i –WPA2			X	X	X	X	X
WEP	X	X	X	X	X	X	X
IEEE 802.1X	X	X	X	X	X	X	X
• LEAP	X	X	X	X	X	X	X
• EAP-FAST			X	X	X	X	X
CKIP (encryption)	X				X	X	

Table 11-4 Cisco Compatible Extensions Version Feature Support (continued)

Wi-Fi Protected Access (WPA): 802.1X + WPA TKIP		X	X	X	X	X	X
• With LEAP		X	X	X	X	X	X
• With EAP-FAST			X	X	X	X	X
IEEE 802.11i- WPA2: 802.1X+AE			X	X	X	X	X
• With LEAP			X	X	X	X	X
• With EAP-FAST			X	X	X	X	X
CCKM EAP-TLS				X	X	X	X
EAP-FAST				X	X	X	X
Mobility							
AP-assisted roaming		X	X	X	X	X	X
Fast re-authentication via CCKM, with LEAP		X	X	X	X	X	X
Fast re-authentication via CCKM, with EAP-FAST			X	X	X	X	X
MBSSID				X	X		
Keepalive				X	X	X	
QoS and VLANs							
Interoperability with APs that support multiple SSIDs and VLANs	X	X	X	X	X	X	
Wi-Fi Multimedia (WMM)			X	X	X	X	X
Performance and Management							
AP-specified maximum transmit power		X	X	X	X	X	X
Recognition of proxy ARP information element for automatic switching protection (ASP)			X	X	X		
Client Utility Standardization							
Link test				X	X	X	X

For a detailed list of software features and Mobile IOS feature support, see the *Cisco 3200 Series Mobile Access Router Software Configuration Guide* at the following URL: http://www.cisco.com/en/US/docs/routers/access/3200/software/configuration/guide/M640mib.html.

Cisco 3200 Series Management Options

You can manage the WMICs through the following interfaces:

- The IOS command-line interface (CLI), which you use through a PC running terminal emulation software or a Telnet/SSH session. IOS CLI is accessible through the WMIC console connection, Telnet, or SSH.
- Simple Network Management Protocol (SNMP)
- Web GUI management

CHAPTER 12

Cisco Unified Wireless and Mobile IP

Introduction

In IP networks, routing is based on stationary IP addresses, similar to how a postal letter is delivered to a fixed address on an envelope. A device on a network is reachable through normal IP routing by the IP address to which it is assigned on the network. However, when networks are in motion, problems occur when a device roams away from its home network and is no longer reachable using normal IP routing. This causes the active sessions of the device to terminate.

Mobile IP offers a solution to these roaming problems by enabling users to keep the same IP address while traveling to a different network (which may even be operated by a different wireless operator), thus ensuring that a roaming individual can continue communication without sessions or connections being dropped. Because the mobility functions of Mobile IP are performed at the network layer rather than the physical layer, the mobile device can span different types of wireless and wireline networks while maintaining connections and ongoing applications. Remote login, remote printing, and file transfers are examples of applications where it is undesirable to interrupt communications while an individual roams across network boundaries. Also, certain network services, such as software licenses and access privileges, are based on IP addresses. Changing these IP addresses can compromise the network services.

This chapter describes the interaction of a mobile IP client over a Cisco Unified Wireless Network and covers the following topics:

- Different levels of mobility
- Requirements for a mobility solution
- Roaming on the Cisco Unified Wireless Network
- Roaming on a Mobile IP-enabled network
- Mobile IP client characteristics when roaming on a Cisco Unified Wireless Network

Different Levels of Network Mobility

There are two different levels of network mobility:

- Layer 2 roaming across a single Layer 2 network:
  - All of the APs are on the same subnet without trunking
- Layer 3 roaming across a single Layer 2 network:
  - Cisco Unified Wireless Network
  - Mobile IP Client

One example of Layer 2 roaming across a single Layer 2 network (shown in Figure 12-1) is a wireless network where all the APs WLANs are on the same subnet and the clients roam between them. This type of deployment allows the clients to roam from one AP to another AP without requiring a client IP address change or the network being mobility-aware.

Layer 3 roaming across a single Layer 2 network follows the previous AP example, but allows the WLANs to be on different subnets while also allowing the clients to remain in the same subnet as they roam from WLAN to WLAN. This example is depicted in Figure 12-2. Layer 3 roaming with Mobile IP allows roaming across completely different Layer 2 networks (cellular, wired, and 802.11 wireless). Figure 12-3 illustrates an example where a client roams from its wired network to a wireless network on a different subnet.

Seamless mobility is where both the mobile client applications and the remote applications do not notice any change in end-to-end IP addressing end applications can use or embed these IP addresses into their data packets without concern that they will be undeliverable. This emulates the case where two clients are on a wired network and not mobile. The Cisco Unified Wireless Network and Mobile IP both provide seamless mobility.

The Cisco Unified Wireless Network is an example of seamless Layer 3 roaming across a single Layer 2 network, while the client using Mobile IP (RFC 3344) is an example of seamless Layer 3 roaming across any Layer 2 network. That is, in the Cisco Wireless Unified Network, Layer 3 roaming is restricted to roaming across APs in the mobility group. With Mobile IP, any Layer 2 network (wired, 802.11 wireless, or cellular) can be used for roaming. Both the Cisco Unified Wireless Network and Mobile IP solutions perform similar functionality, so they require similar components.

Figure 12-1 Layer 2 Network Roam Example

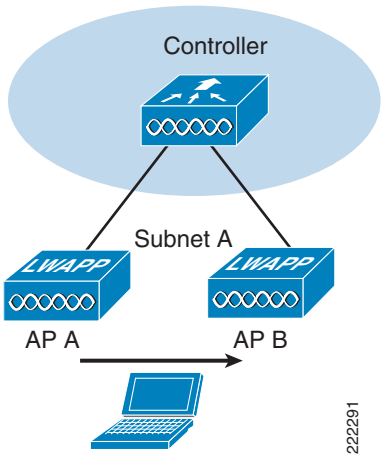


Figure 12-2 Layer 3 CUWN Roam Example

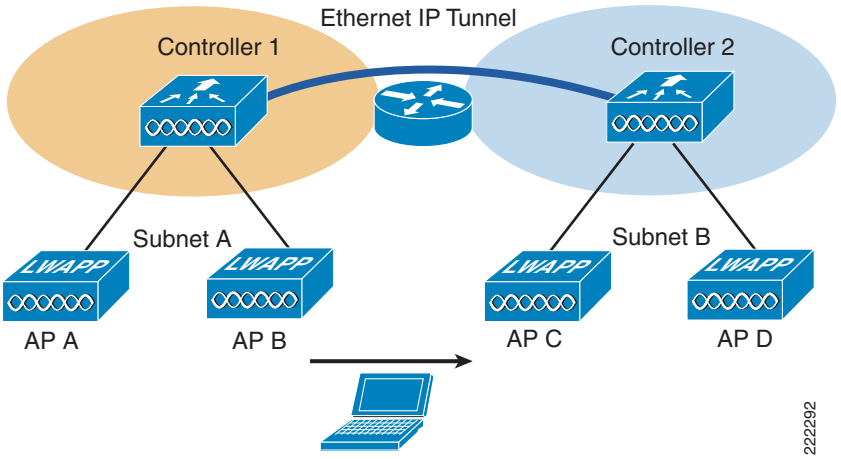
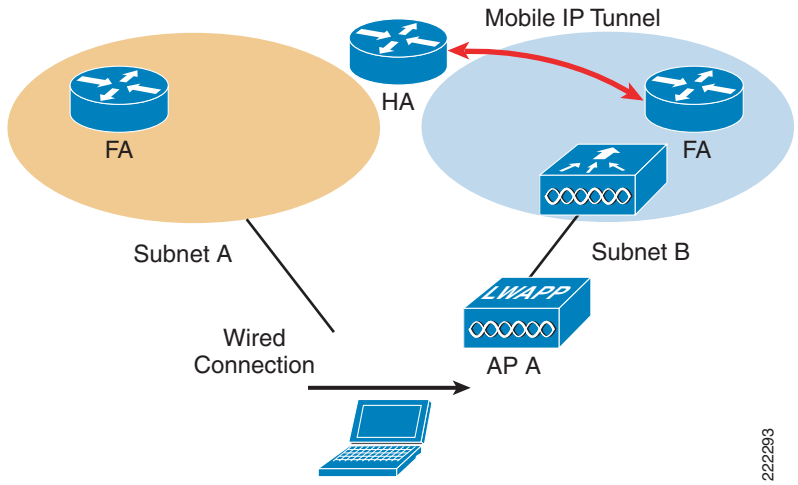


Figure 12-3 Layer 3 Mobile IP Roaming Example



Requirements for a Mobility Solution

The following are required for every mobility solution:

- Location database
- Move discovery
- Location discovery
- Update signaling
- Path re-establishment

These requirements are covered in the following sections.

Note The location database discussed in this section has no relation to the location database as known in location-based services (LBS) covered in Chapter 13, "Cisco Unified Wireless Location-Based Services."

Location Database

In the Cisco Unified Wireless Network, the first hop router receives packets for the wireless clients through the routing protocol running on that network, and forwards them via a trunk to the WLC. Each WLC keeps a database of wireless clients as they roam between APs registered to the WLC. If the wireless client then roams to an AP on another WLC (a foreign WLC), that WLC can query other WLCs in the mobility group to see if this is a new client or a roaming client. If it is a roaming client, the first hop router near the home WLC still receives packets destined to the wireless client, but instead of the WLC forwarding them on to one of its associated APs, it forwards the packets to the foreign WLC, which then forwards them on to the client. Roaming on a Cisco Unified Wireless Network is covered in greater depth in the Chapter 2, "Cisco Unified Wireless Technology and Architecture." For more information refer to Roaming, page 2-17.

In Mobile IP, the Home Agent (HA) contains the location database. Because it runs the network routing protocol, it attracts packets for the Mobile IP Client and forwards them to the current location of the client. Unlike the Cisco Unified Wireless Network, the HA does not maintain a distributed database between WLCs. It does not query other HAs. As far as it is concerned, there is only one location database: itself. This is where the location database mechanisms for the two solutions differ.

Move Discovery, Location Discovery, and Update Signaling

When the wireless client roams to a new AP, it needs to associate to the wireless network. During the association process, the association packets are forwarded to the WLC to identify the wireless client and the location (AP) from where the wireless client is trying to associate. This information is used by the WLC to update its location database (the WLC mobility database). If the client has roamed to another WLC, the original WLC for the wireless client forwards packets destined to the wireless client to the remote WLC.

In Mobile IP, the Mobile IP Client joining the wireless network does not provide the HA with any information. Additionally, the client is responsible for recognizing when it has moved between networks. The client typically detects movement in two ways. One way is through the Windows operating system's Layer 2 notification feature called Media Sense. This feature detects disconnect and reconnect of different Layer 2 media when roaming between APs and sends the Windows operating system a signal when it occurs. This allows the interface to try and renegotiate its DHCP address with the DHCP server. The second method for detecting movement is through Foreign Agent (FA) advertisements. These advertisements tell the Mobile IP Client which subnet it is on. If the Mobile IP Client receives one of these periodic messages, it can tell it has moved to a new subnet. These move discovery methods are typically used for Mobile IP. There are other methods specified in RFC 3344, but generally these are not used.

Location discovery is typically done in one of two ways in Mobile IP. In the first method, the Mobile IP Client receives an FA advertisement telling it what the IP address is for the FA. The Mobile IP Client can check this address against the address it already has from the FA and tell if the FA advertisement is from a new FA. The Mobile IP Client can then forward this IP address to its HA so that the HA can build a new tunnel to the new FA and proceed forward packets to the Mobile IP Client. In the second method,

the client, acting as its own FA, receives a new DHCP IP address and informs the HA it has a new location. At this time, the HA can then build a tunnel to the client for forwarding packets. This is called a collocated care of address.

Move discovery is done in the Cisco Unified Wireless Network by the network that knows which AP the wireless client is currently associated to. Update signaling is done by the first packets sent to the WLC from the wireless client. The Update process is described in detail in Chapter 2, "Cisco Unified Wireless Technology and Architecture." For more information, see the following URL: http://www.cisco.com/en/US/products/ps6590/products_ios_protocol_group_home.html.

Path Re-establishment

Path re-establishment is the mechanism used to allow the client to receive packets that are destined for it from the HA that contains the location database. Typically a tunneling mechanism is used to encapsulate the original packet. In the Cisco Unified Wireless Network, packets are forwarded to wireless clients on associated APs through the "always up" LWAPP tunnel. For wireless clients that have roamed to another WLC, the WLCs use a dynamic Ethernet-over-IP tunnel for all packets forwarded to other WLCs in the mobility group.

In Mobile IP, there are several types of tunnels available (GRE, UDP, and IP in IP) and the type of tunnel used depends on the equipment between the Mobile IP Client and HA, and whether the HA supports that type of encapsulation. For example, if the HA detects that the client is behind a NAT gateway, it uses UDP tunneling. If the Mobile IP Client requests GRE tunneling and the HA can support the tunneling, it uses GRE. Typically, the Mobile IP Client requests IP in IP tunneling, and all RFC-compliant clients can support this type of tunneling.

Roaming on a Cisco Unified Wireless Network

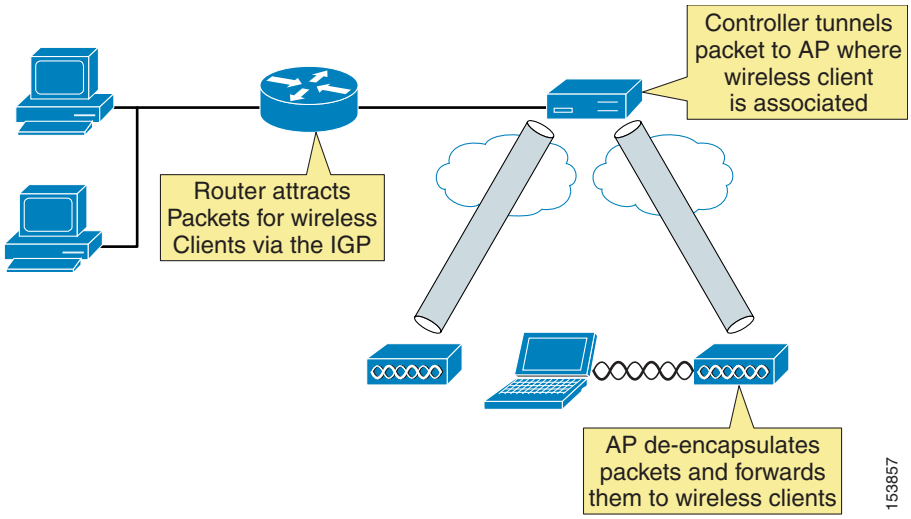
A Cisco Unified Wireless Network acts as a mobility proxy for the wireless client. This allows the network to provide seamless mobility to the wireless client without any extra software or additional configuration on the wireless client (see Figure 12-4).

When a wireless client associates to an AP, the AP forwards the client packets to the WLC via the LWAPP tunnel set up between the WLC and AP (the LWAPP tunnel is set up between the AP and WLC at AP boot time). For the WLC, the LWAPP tunnel allows it to do the following:

- Know to which AP the client is associated (LWAPP tunnel endpoint)
- Forward packets back to the client via the tunnel
- Be multiple hops away from the AP and still receive the client traffic
- Filter the packets to and from the wireless client

For the client, the LWAPP tunnel allows the client to see its default gateway as being one hop away, even though it might physically be several hops away.

Figure 12-4 Roaming on a Cisco Unified Wireless Network



If the client requests a DHCP address, the WLC either gives the client an address from its local DHCP pool (if defined) or fills in the gateway address in the DHCP request for an external DHCP server. In either case, the WLC modifies any returning DHCP offers so that the DHCP server's address is set to the address on WLCs virtual interface. Even though the virtual IP address is not in any routing table (typically 1.1.1.1), it still allows the WLC to intercept any DHCP renewals on wireless clients that occur with the Microsoft Windows operating system (using Microsoft Media Sense) when it roams between APs. In addition, if the same address is on all WLCs' virtual interfaces, it allows other WLCs to intercept the DHCP renewal from the client when it roams to a new AP associated to a different WLC.

The wireless client can easily roam between any APs registered to the WLC because the WLC simply keeps track of the wireless client's current location and forwards the packets destined to that client into the correct LWAPP tunnel and on to the associated AP. When the client roams to an AP registered to a different WLC, the remote WLC queries the mobility group to see if the client has roamed. If so, an Ethernet-over-IP tunnel is set up to forward client traffic from the original WLC to the WLC registered to the AP with which the client is currently associated.

Traffic originating from the wireless client that has roamed to an AP associated to another WLC can be handled in two ways. Typically, the foreign WLC modifies the destination MAC address of any packet from the wireless client to be its gateway MAC address before forwarding it on. The second method occurs if mobility anchoring is enabled on the original WLC. In this case, the traffic is forwarded back to the original WLC. This allows traffic to be sent to the correct gateway in case address policies such as Reverse Path Forwarding (RPF) checks are enabled.

For more information about Cisco Unified Wireless Roaming, see Roaming, page 2-17.

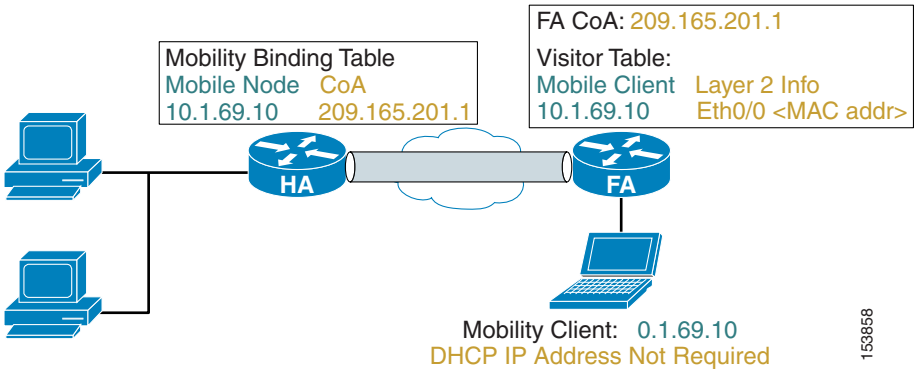
Roaming on a Mobile IP-enabled Network

A Mobile IP-enabled network has three components:

- Mobile node (MN)—Mobile IP Clients
- Home Agent (HA)—Contains the location database for MNs advertises reachability to the MN in the Interior Gateway Protocol (IGP). It also tunnels packets to MN.
- Foreign Agent (FA)—(Optional) offloads CPU processing of encapsulation and decapsulation from the MN and saves IP address space. FAs are not often deployed in enterprise campus environments.

Only two of the three components (MN and HA) are actually required for a mobility solution. The third component, FA, is optional because the MN can act as its own FA by using DHCP for a local IP address. In this case, the tunnel ends at the MN. In HA and FA Tunneling5, the MN is given an IP address (10.1.69.10) local to the HA. To the rest of the network, the MN looks like it is directly attached to the HA. The HA then uses its mobility binding table to forward packets to wherever the MN is currently located. It is the responsibility of the MN to update its location with the HA. The FA decapsulates the packets destined for the MN and forwards them out its interface. It gleans the information it needs by being an active party in the registration process with the HA. The MN actually sends its packets to the FA, and the FA checks the packets and generates new IP headers to forward the information onward to the HA. The FA can also provide reverse tunneling for the MN originated packets back to the HA, instead of simply forwarding through the normal switching process. Reverse tunneling allows packets from the MN to always exit the HA and pass any reverse path forwarding (RPF) checks.

Figure 12-5 HA and FA Tunneling



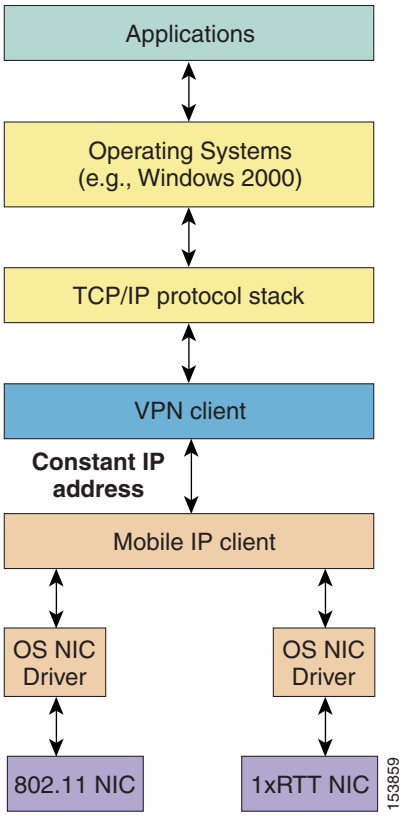
Unlike the Cisco Unified Wireless Network where the network proxies or provides the wireless client with seamless mobility, the Mobile IP Client (or MN) needs to know three pieces of information to function:

- • Its home address (on a locally connected subnet on the HA)
- • Its HA address (so it can update the HA with its current location)
- • Its shared secret key (used to authenticate packets between the MN and HA)

Both the mobile node's home address and HA address can be dynamically discovered or generated but are typically manually configured on the MN. DHCP can be used to convey the HA address to the MN via option 68. The HA can dynamic assign an IP address to the MN to be used as its home address when it registers for the first time. Depending on your mobile IP client software and its capabilities, the shared secret key most likely needs to be manually configured.

When a Mobile IP Client is loaded on a Windows host, the Mobile IP Client function rests between the physical interfaces and TCP/IP stack (see Figure 12-6). The Mobile IP Client function sends its home address up the TCP/IP stack so that the host applications, including a VPN client, see a constant IP address as the MN roams across the different network locations or different networks. The physical interfaces might or might not have IP addresses during roaming depending on whether an FA is present on the subnet.

Figure 12-6 Example of Mobile IP Function Position in the Microsoft Operating System



The mobile IP client controls that interface with host-originated packets are transmitted by:

- Installing a new virtual interface adapter at install time.
- Modifying the host forwarding table.

This virtual adapter looks like any physical adapter to the host (see the example in Configuration 1: Sample Mobile IP Client Interface and Host Table Manipulation). When the adapter is enabled, the Mobile IP Client modifies the forwarding table to give the virtual adapter the best metric, and the Windows operating system forwards host-originated packets to the virtual adapter. This allows the Mobile IP Client to hide the true interface used to transmit the packet and to modify the host's forwarding behavior. In the example, there are three interfaces:

- A local area connection with a static IP address and no gateway.
- A Mobile IP Client interface with a configured home address and gateway.
- A wireless connection that has an address filled in by Mobile IP as 0.0.0.0. The actual address is not shown to the Windows operating system.

Note that the Mobile IP Client has manipulated the host's forwarding table so that the lower metric interface is the Mobile IP Client's interface. The higher metric routes can be safely ignored when looking at the table. The real DHCP IP address on the wireless interface is 10.20.41.12. Any route with a destination address to this gateway has had its metric raised and the default gateway is via the virtual interface "Ethernet Adapter MIPDRV in Configuration 1."

Configuration 1: Sample Mobile IP Client Interface and Host Table Manipulation

```
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address . . . . . . . . . . . . : 10.20.30.249
Subnet Mask. . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . :
Ethernet adapter MIPDRV:
Connection-specific DNS Suffix . : srnd3.com
IP Address . . . . . . . . . . . . : 10.20.32.11
Subnet Mask. . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 10.20.32.1
Ethernet adapter Wireless Connection:
Connection-specific DNS Suffix . :
IP Address . . . . . . . . . . . . : 0.0.0.0
Subnet Mask. . . . . . . . . . . . : 0.0.0.0
Default Gateway . . . . . . . . . :
C:\>route print
===========================================================================================
Interface List
0x1...........................MS TCP Loopback interface
0x2...00 d0 b7 a6 b8 47........Intel (R) 82559 Fast Ethernet LAN on Motherboard
- Packet Scheduler Miniport
0x3...00 4d 69 70 56 61 .......Cisco Systems Mobile Adapter - Packer Scheduler
Miniport
0x10005...00 12 f0 7c a5 ca......Intel (R) PRO/Wireless 2915ABG Network Connec
tion - Deterministic Network Enhancer Miniport
===========================================================================================
=
===========================================================================================
=
Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 10.20.32.1 10.20.32.11 1
10.20.30.0 255.255.255.0 10.20.30.249 10.20.30.249 1
10.20.30.0 255.255.255.0 10.20.32.1 10.20.32.11 1
10.20.30.249 255.255.255.255 127.0.0.1 127.0.0.1 1
10.20.32.0 255.255.255.0 10.20.32.11 10.20.32.11 20
10.20.32.11 255.255.255.255 127.0.0.1 127.0.0.1 20
10.20.41.0 255.255.255.0 10.20.41.12 10.20.41.12 25
10.20.41.0 255.255.255.0 10.20.32.1 10.20.32.11 1
10.20.41.12 255.255.255.255 127.0.0.1 127.0.0.1 25
10.255.255.255 255.255.255.255 10.20.30.249 10.20.30.249 1
10.255.255.255 255.255.255.255 10.20.32.11 10.20.32.11 20
10.255.255.255 255.255.255.255 10.20.41.12 10.20.41.12 25
127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1
224.0.0.0 240.0.0.0 10.20.30.249 10.20.30.249 1
224.0.0.0 240.0.0.0 10.20.32.11 10.20.32.11 20
224.0.0.0 240.0.0.0 10.20.41.12 10.20.41.12 25
255.255.255.255 255.255.255.255 10.20.30.249 10.20.30.249 1
255.255.255.255 255.255.255.255 10.20.32.11 10.20.32.11 1
255.255.255.255 255.255.255.255 10.20.41.12 10.20.41.12 1
Default Gateway: 10.20.32.1
===========================================================================================
=
Persistent Routes:

None
```

When an MN makes a Layer 2 connection, it starts two different threads. One thread is a DHCP process to obtain a local IP address so that it can be used for a collocated care of address (CCoA) registration to the HA if there is no FA on the subnet. The other thread looks for a FA on the subnet to which it is attached. If the MN finds an FA on the subnet, it uses the care of address (CoA) advertised by the FA to register (update) with the HA, and reject any DHCP offers. An FA on the subnet does two things for the Mobile IP Client:

- The HA forms a tunnel with the FA CoA to forward packets destined for the MN, thereby relieving the MN of having to obtain a local address. The FA forwards packets to the MN home address on its local interfaces via Layer 2 information it derived during registration with the HA.
- It offloads the tunnel packet processing of encapsulation or de-encapsulation to the FA. The FA can forward traffic to the MN because the MN is on a directly attached interface.

The FA maintains an entry in a table, called a visitor table, which has the MN home address, and to which interface the MN is currently attached as well as Layer 2 encapsulation information. This way, when the HA tunnels a packet for the MN to the FA, the FA simply de-encapsulates the packet and looks into its visitor table for the interface the MN is on and forwards it directly out the interface. Because of this table, the MN does not need a local IP address on the subnet.

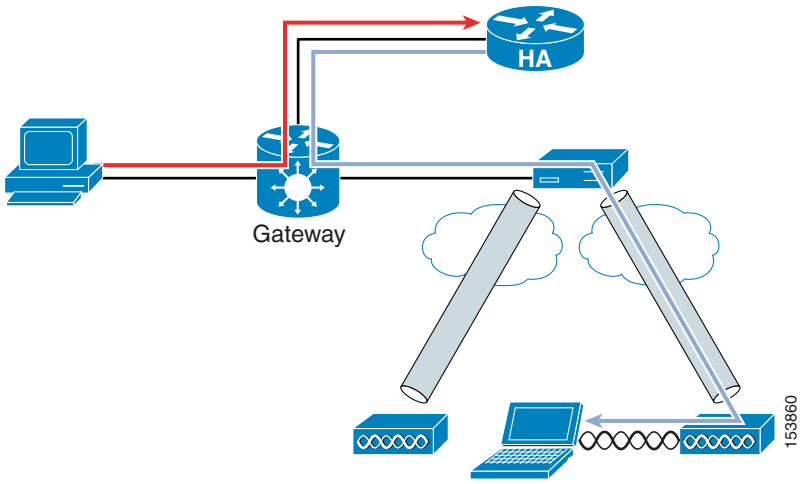
If there is no FA on the subnet, the MN requires a local IP address to which the HA can forward packets. After it receives a DHCP address, the MN registers (updates) the HA and builds a tunnel directly between the MN and the HA. All de-encapsulation of packets is performed by the MN. If reverse tunneling (where the host packets are tunneled back to the HA) is enabled, the overall solution is analogous to the Cisco Unified Wireless Network. Packets from the client are tunneled and forwarded to a HA and packets destined to the client are received by the HA and tunneled and forwarded to the current location of the client.

Figure 12-5 and Figure 12-6 are similar in functionality except that the HA is a router and can also advertise itself to the Mobile IP Client through the use of an IGP and tunnel packets to the MN.

Mobile IP Client Characteristics When Roaming on a Cisco Unified Wireless Network

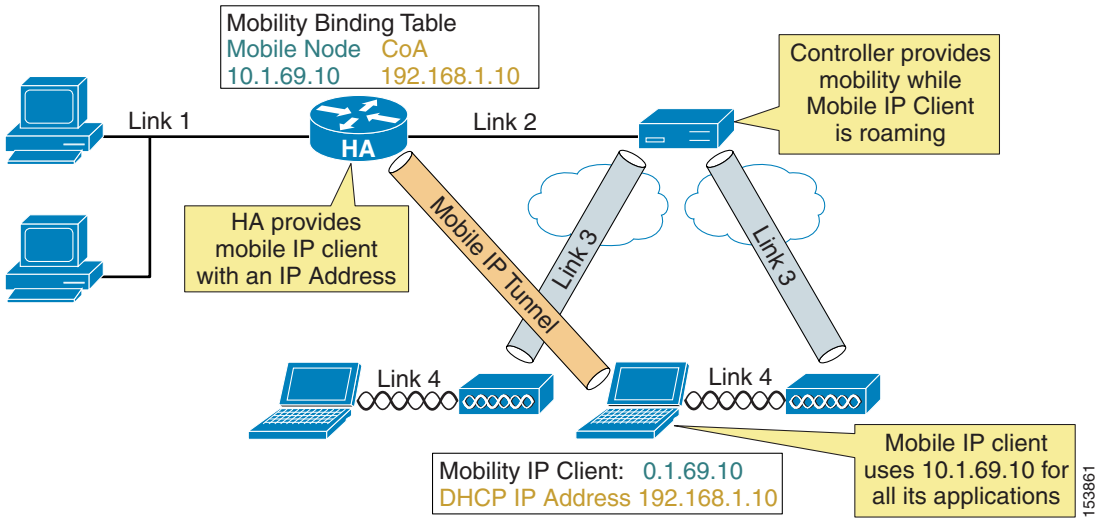
Traffic destined for the MN must pass through the HA and the WLC to reach a MN on the wireless network. If reverse tunnel is enabled, the packet must pass back through the HA before being forwarded to any other host. Figure 12-7 shows the traffic patterns from a remote host to the MN. The red flow line shows that the network believes the MN is attached to the HA. The blue flow line shows the tunneled packet to the MN. If another wireless client sent packets to the MN, that traffic would also have to traverse the HA.

Figure 12-7 Traffic Flow to MN



Because of the routing of traffic to and from the MN from other hosts, the general goal in the placement of the WLC and HA is to minimize the summation of all links. In Mobile IP and Cisco Unified Wireless Network8, link 1 cannot be minimized because the hosts' locations are random. The same goes for link 4 because mobile hosts' locations cannot be fixed. Link 3 cannot be minimized because the RF survey determines AP placement. This leaves the link between the WLC and HA, link 2.

Figure 12-8 Mobile IP and Cisco Unified Wireless Network



There are two basic HA placement principles:

- HA placement must be as close to the core as possible
- HA placement when in use with a Cisco Unified Wireless Network must be as close to the WLC as possible

The first principle is simply a way to minimize traffic links from any host in the network to any place in the network. The second principle follows the logic that the only link you can minimize is Link 2 between the HA and WLC. This means the WLC and HA should be collocated whenever possible. The

best location is directly off the core with the centralized WLCs. If there is a case where Mobile IP is being used in a distributed WLC placement network, the HA should be placed at a aggregation point in the network that best minimizes the links between itself and the WLCs.

When a Mobile IP Client is roaming on a Cisco Unified Wireless Network, it maintains the same DHCP IP address while roaming, allowing it to maintain the same CCoA address. The Cisco Unified Wireless Network handles the underlying mobility and the Mobile IP Client does not see any changes as it roams from AP to AP. To the Mobile IP Client, it is as if it is roaming on a single large subnet. Accordingly, nothing changes at the Mobile IP Client level until it roams off of the wireless network.

Note CCoA mode for the Mobile IP client is recommended on the Cisco Unified Wireless Network because of unwanted multicast traffic over the shared wireless network when multicast is enabled at the WLC. Because multicast traffic is disabled at the WLC by default, there is no requirement for FAs on the wireless network. See Chapter 6, "Cisco Unified Wireless Multicast Design," for more information about the multicast traffic on a Cisco Unified Wireless Network.

CHAPTER 13

Cisco Unified Wireless Location-Based Services

Introduction

With integrated location tracking, enterprise wireless LANs become more valuable as a corporate business asset. By identifying and tracking the location of wireless users, companies can improve the accuracy of WLAN planning and deployment to optimize ongoing network performance, enhance wireless security, and improve both the usefulness and value of important business applications. Location tracking provides visibility and control of the RF environment, and helps IT staff deploy wireless networks that are easier to manage and deploy.

Enterprise network administrators, security personnel, users, and asset owners have expressed great interest in location-based services to allow them to better address requirements such as the following:

- Quickly and efficiently locating valuable assets and key personnel
- Improving productivity via effective asset and personnel allocation
- Reducing loss because of the unauthorized removal of high-value assets from company premises
- Improving customer satisfaction by rapidly locating critical service-impacting assets
- Improving WLAN planning and tuning capabilities
- Improving workflow automation
- Coordinating Wi-Fi device location with security policy enforcement

This chapter discusses the location-aware Cisco Unified Wireless Network (UWN). It focuses primarily on design considerations but mentions topics meriting special consideration during deployment as well. These areas are described in brief and references are made to a comprehensive white paper entitled *Wi-Fi Location-Based Services 4.1 Design Guide*, which contains in-depth discussion and analysis and is available at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html.

The following topics are addressed in this chapter:

- The fundamentals of positioning technologies including lateration, angulation, and location patterning approaches
- Cisco RF Fingerprinting and its advantages over traditional positioning techniques
- Cisco Location Control Protocol (LOCP)
- Chokepoints (and the use of chokepoint triggers) to further enhance location granularity within the Cisco UWN
- Various RFID tag technologies including active, passive, and multimode
- External third-party location client application interfaces to the Cisco Wireless Location Appliance

Reference Publications

The following supplemental documents contain valuable supporting information and are recommended for review:

- Wi-Fi Location-Based Services 4.1 DesignGuide—
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html

Additionally, review the following supplemental documents:

- Release Notes for Cisco Wireless Location Appliance—
http://www.cisco.com/en/US/docs/wireless/location/2700/release/notes/larn4032.html
- Cisco Wireless Location Appliance: Installation Guide—
http://www.cisco.com/en/US/docs/wireless/location/2700/quick/guide/li31main.html
- Cisco Wireless Location Appliance: Deployment Guide—
http://www.cisco.com/en/US/docs/wireless/technology/location/deployment/guide/depgd.html
- Cisco Wireless Control System Release Notes, Release 4.0—
http://www.cisco.com/en/US/docs/wireless/wcs/release/notes/wcsrn_MR2.html
- Cisco Wireless Control System Configuration Guide, Release 4.0—
http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wcscfg40.html
- Cisco 4400 Series WLAN Controller Support Documentation for Release 4.1—
http://www.cisco.com/en/US/products/ps6366/tsd_products_support_series_home.html
- Cisco 2100 Series WLAN Controller Support Documentation for Release 4.1—
http://www.cisco.com/en/US/products/ps7206/index.html
- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers Support Documentation—
http://www.cisco.com/en/US/products/ps6915/index.html
- Cisco Wireless LAN Controller Module Support Documentation—
http://www.cisco.com/en/US/products/ps6730/tsd_products_support_model_home.html
- Cisco Catalyst 6500 Series Wireless Services Module (WiSM) Support Documentation—
http://www.cisco.com/en/US/products/ps6526/tsd_products_support_model_home.html

For design considerations concerning the use of the InnerWireless Vision (formerly PanGo) Locator location client in the location-aware Cisco UWN, refer to the following white paper:

- Design Considerations for Cisco–PanGo Asset Tracking—
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/pango/PanGoEx.html.

Note Software Release 3.0 of the Cisco Location Appliance is intended to be included in any reference made to software Release 4.1 of the Cisco Unified Wireless Network (UWN) within this document, unless otherwise noted.

Cisco Location-Based Services Architecture

Positioning Technologies

Location tracking and positioning systems can be classified by the measurement techniques employed to determine mobile device location (*localization*). These approaches differ in terms of the specific technique used to sense and measure the position of the mobile device in the environment under observation. Typically, real-time location systems (RTLS) can be grouped into four basic categories of systems that determine position on the basis of the following:

- Cell of origin *(nearest cell)*
- Distance *(lateration)*
- Angle *(angulation)*
- Location patterning *(pattern recognition)*

An RTLS system designer can choose to implement one or more of these techniques. This may clearly be seen in some approaches attempting to optimize performance in two or more environments with very different propagation characteristics. It is not unusual to hear arguments supporting the case for a fifth category that encompasses RTLS systems that sense and measure position using a combination of at least two of these methods.

Keep in mind that regardless of the underlying positioning technology, the "real-time" nature of an RTLS is only as real-time as its most current timestamps, signal strength readings, or angle-of-incidence measurements. The timing of probe responses, tag beacons, and location server polling intervals can introduce discrepancies between the actual and reported device position observed during each reporting interval.

The "Location Tracking Approaches" section of *Wi-Fi Location-Based Services 4.1 Design Guide* provides a foundation in the technical aspects of traditional location tracking and positioning systems. This section is recommended reading for a better understanding of the differences between traditional approaches and RF Fingerprinting. It thoroughly explains the concepts of cell of origin, time of arrival (ToA), time difference of arrival (TDoA), angle of arrival (AoA), and location patterning.

What is RF Fingerprinting?

Cisco RF Fingerprinting refers to an innovative localization approach that significantly improves the accuracy and precision over that available from traditional signal strength lateration techniques. Cisco RF Fingerprinting offers the simplicity of an received signal strength indication (RSSI)-based lateration approach with customized calibration capabilities and improved performance over traditional approaches.

RF Fingerprinting significantly enhances received signal strength (RSS) lateration through the use of RF propagation models developed from data gathered in the target or similar environments. RF Fingerprinting offers the ability to calibrate an RF model to a particular environment in a fashion analogous to (but more expeditious than) that of location patterning. But unlike location patterning, RF Fingerprinting allows for the reuse of calibration models in situations where multiple floors of similar construction, contents, and layout are deployed.

In addition, Cisco RF Fingerprinting offers the following key advantages over the traditional approaches described in the "Location Tracking Approaches" section of *Wi-Fi Location-Based Services 4.1 Design Guide*:

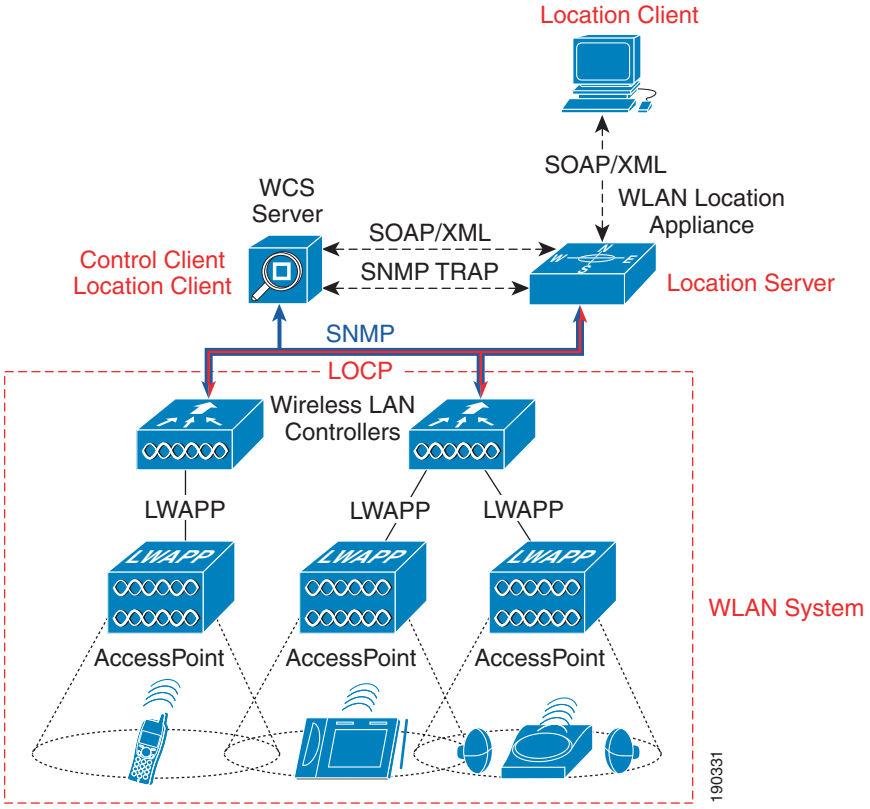
- Uses existing LWAPP-enabled Cisco Unified Networking components—Unlike some other solutions, the location-aware Cisco UWN with RF Fingerprinting does not require added-cost specialized receivers or other hardware that must be mounted alongside each access point. This helps keep the capital and ongoing maintenance costs of the location-aware Cisco UWN low in comparison to solutions requiring a dedicated overlay location infrastructure. The Cisco Location Appliance is added as a centralized component to support location and statistics history and serves as a location positioning engine for the simultaneous tracking of up to 2500 devices per appliance.
- No proprietary client hardware or software required—Location-based services in the Cisco UWN are implemented as a network-side model, not client-side. Because of this, Cisco RF Fingerprinting can provide location tracking for a wide variety of industry-standard Wi-Fi clients *without the need to load proprietary tracking software or location-enabling drivers in each client.* Any IEEE 802.11 client can be located in most cases, with WLAN enhanced client localization for clients compatible with the Cisco Compatible Extensions for WLAN clients specification version 2 or higher. This includes popular VoWLAN handsets such as the Cisco 792x series and others for which proprietary location tracking client software is neither readily available or installable.
- Support of Wi-Fi active RFID asset tags compliant with the Cisco Compatible Extensions for Wi-Fi Tags specification—Because the location-aware Cisco UWN solution implements RF Fingerprinting as a network-side model, there is no requirement for proprietary software in asset tags to detect access point RSSI and relay this information back to the network in order for the asset tag to be successfully localized. This enables the location-aware Cisco UWN to interoperate with active RFID asset tags from various vendors meeting the Cisco Compatible Extensions for Wi-Fi Tags specification, such as AeroScout, WhereNet, G2 Microsystems, InnerWireless (formerly PanGo Networks) and others. RFID asset tags that support the Cisco Compatible Extensions for Wi-Fi Tags specification allow for improved performance and the support of advanced features such as:
  - Telemetry and sensor information
  - Battery, panic, and tampering alerts
  - Motion sensing notification
  - High fidelity deterministic location using chokepoint triggers
- Better accuracy and precision—Cisco RF Fingerprinting yields significantly better performance than solutions employing only pure triangulation or signal strength lateration techniques. These techniques typically do not account for the effects of attenuation in the environment, making them highly susceptible to performance reductions. The advantages of Cisco RF Fingerprinting technology start where traditional approaches leave off. Cisco RF Fingerprinting begins with a significantly better understanding of RF propagation as it relates specifically to the environment in question. Except for the calibration phase in location patterning approaches, traditional lateration or angulation techniques typically do not take such environmental considerations directly into account. RF Fingerprinting goes a step further and applies statistical analysis techniques to the set of collected calibration data. This allows the Cisco Location Appliance to further refine predicted location possibilities for mobile clients, culling out illogical or improbable data and further refining accuracy. The net result of these methods is not only better accuracy but significantly improved precision over traditional solutions.
- Reduced calibration effort—Cisco RF Fingerprinting technology offers the key advantages of a location patterning solution but with significantly less calibration effort. Although both approaches support on-site calibration, the Cisco RF Fingerprinting approach requires less frequent re-calibration and can operate with larger inter-access point spacing. Cisco RF Fingerprinting can also share calibration models among similar types of environments and includes several pre-packaged models that can facilitate rapid deployment in typical indoor environments.

Additional information on these and other key advantages of Cisco RF Fingerprinting can be found in the "Location-Based Services Architecture" section of *Wi-Fi Location-Based Services 4.1 Design Guide*.

Overall Architecture

The overall architecture of location-aware Cisco UWN is shown in Figure 13-1.

Figure 13-1 Location-Aware Cisco Unified Wireless Network Architecture



Access points forward the received signal strength of any Wi-Fi clients, 802.11 active RFID tags, rogue access points, or rogue clients to their registered WLAN controllers. In normal operation, access points focus their collection activities for this information on their primary channel of operation, going off-channel and scanning the other channels in their regulatory frequency domain periodically. The collected signal strength information is forwarded to the WLAN controller to which the access point is currently registered, which aggregates the information. The location appliance uses SNMP to poll each controller for the latest signal strength information for each tracked category of device. In the case of a location tracking system deployed without a location appliance, the Cisco Wireless Control System (WCS) retrieves this information from the appropriate controller(s) directly. The Cisco Wireless Location Appliance performs location computations based on the RSSI information received from the Cisco WLAN controllers. Introduced in software Release 4.1, access point antenna height and azimuth is taken into account during these RSSI-based location calculations to improve accuracy.

Beginning with software Release 4.1 of the location-aware Cisco UWN, the location appliance augments its SNMP-based data collection capabilities by using LOCP to periodically poll WLAN controllers for asset tag telemetry data, such as battery status and other telemetry data from onboard-tag sensors or

external environmental sensors. LOCP is also used for priority forwarding of chokepoint proximity and emergency notifications that WLAN controllers receive from tags that are compliant with the Cisco Compatible Extensions for Wi-Fi Tags specification.

WCS and the location appliance exchange information (such as calibration maps and network designs) during a process known as *synchronization*, where the "up-to-date" partner updates the design and calibration information of the "out-of-date" partner. Synchronization occurs either on-demand or as a scheduled task, the timing of which is determined by the Administration > Scheduled Tasks menu option under the WCS main menu bar.

Information about device location information is made available to the end user using a *location client* application. Typically, this role is fulfilled by the Cisco WCS, which displays location information visually and provides a readily available location client application for customers who want to enhance their basic RF capacity management, perform rogue access point and client detection, and have asset visibility for WLAN devices.

For important information regarding compatibility between versions of WCS and the Cisco Wireless Location Appliance, see *Release Notes for Cisco Wireless Location Appliance 3.0* at the following URL: http://www.cisco.com/en/US/products/ps6386/prod_release_notes_list.html.

This location information is also made available to optional third-party location client applications through a Simple Object Access Protocol/Extensible Markup Language (SOAP/XML) API on the appliance. Using the SOAP/XML protocol, these third-party applications may offer extended location client capabilities more specific to particular vertical applications such as healthcare, retail, manufacturing, and logistics.

The Cisco Location Appliance is also capable of issuing notifications to external systems. This provides the ability to proactively send location notifications based on device movement, device absence, zone entry and exit of tracked devices, tag battery level, device position change, emergency groups, and chokepoint information. All of these notifications can be delivered over multiple transport types: UDP-Syslog, Simple Network Management Protocol (SNMP) traps, e-mail (SMTP), and SOAP/XML.

Additional information regarding the architecture of the Cisco LBS solution can be found in the "Location-Based Services Architecture" section of the *Wi-Fi Location-Based Services 4.1 DesignGuide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html.

Role of the Cisco Wireless Location Appliance

When a Cisco Location Appliance is added to a Cisco Unified Wireless Network with an appropriately licensed version of WCS, the location appliance assumes responsibility for several important tasks, including the following:

- Execution of positioning algorithms
- Maintenance of calibration information
- Triggering and dispatch of location notifications
- Processing of statistics and historical location

WCS acts in concert with the location appliance by serving as both the *control client* as well as the *location client* user interface (UI) for the services the location appliance provides, as shown in Figure 13-1. Although it is possible to access the location appliance directly via SSH or a console session for maintenance and diagnostic purposes, all operator and user interaction with the location appliance is typically via WCS or a third-party location client application.

The integration of a Cisco Location Appliance into a Cisco Unified Wireless Network architecture immediately enables improvements to base-level location capabilities. These improvements include:

- Scalability—Adding a Cisco Location Appliance increases the scalability of the Cisco UWN from on-demand tracking of a single device at a time to a maximum tracking capacity of 2500 simultaneous devices (WLAN clients, RFID tags, rogue access points, and rogue clients) per location appliance. For deployments requiring support of greater numbers of devices, additional location appliances can be deployed and managed under one or more WCS servers.
- Historical and statistics trending—The appliance records and maintains historical location and statistics information, which is available for viewing via WCS or other location clients. This historical information can be used for location trending, asset loss investigation, RF capacity management, and to facilitate network problem resolution.
- Chokepoint location—Beginning with Release 4.1 of the UWN, the inclusion of a location appliance allows for granular and deterministic localization based on the passage of an asset through a constrained physical area known as a *chokepoint*. *Chokepoint triggers* located within these areas and in proximity to tagged assets stimulate the tags using low-frequency (125 kHz) signalling. The asset tags in turn transmit the identity of the chokepoint trigger to the location-aware Cisco UWN. This provides for accurate proximity location, which can range from a radius of under one foot to over twenty feet, depending on the capabilities of the chokepoint trigger. Applications for chokepoint location vary from general purpose uses such as theft prevention of high value assets to industry-specific process control events such as those used in manufacturing plants.
- Cisco Extensions for Wi-Fi Tags telemetry information and emergency notifications- Beginning with Release 4.1 of the Cisco UWN, Cisco has partnered with a variety of asset tag vendors to create an extensible specification for 802.11Wi-Fi based active asset tags. The Cisco Compatible Extensions Wi-Fi Tag specification defines a common transmission format that tag vendors can use to interoperate with the location-aware Cisco UWN. This includes a baseline feature set that encompasses telemetry, tag transmit power level, battery information, and advanced fields for emergency groups and chokepoints. The addition of a location appliance allows the location-aware UWN to take advantage of these newly introduced capabilities and benefits customers by providing the ability to “mix and match” compliant asset tags from different vendors in the same network. Complete details on the Cisco Compatible Extensions for Wi-Fi Tags program can be found at http://www.cisco.com/web/partners/pr46/pr147/ccx_wifi_tags.html.

Note At this time, chokepoint triggers and asset tags are compatible with one another only if they are supplied by the same vendor.

- Location notifications—The Cisco Location Appliance can dispatch location-based event notifications via e-mail, Syslog, SNMP traps, and SOAP/XML directly to specified destinations. These notifications can be triggered under the following conditions:
  - Location of a client or asset changes
  - Battery level of an RFID tag drops below a preset value
  - Client or tagged asset strays beyond set distances from pre-determined marker locations
  - Asset enters the proximity of a chokepoint
  - Client or tagged asset becomes missing
  - Asset tag signals that a detachment, tamper, or panic emergency has occurred

- SOAP/XML Location Application Programming Interface (API)—The Location Appliance API allows customers and partners to create customized location-based applications that interface with the Cisco Wireless Location Appliance. For further details, see SOAP/XML Application Programming Interface.

Accuracy and Precision

When discussing the performance of any positioning system, the metric that is usually the most familiar to use is *accuracy,* which typically refers to the quality of the information being received. *Location accuracy* refers specifically to the quantifiable error distance between the estimated location and the actual location of the mobile device.

However, in most real-world applications, any notion of location accuracy has little merit without the ability of the solution to repeatedly and reliably perform at this level. *Precision* is a direct measure of the reproducibility of the stated location accuracy. Any indication of location accuracy should therefore include an indication of the repeatability or confidence level of successful location detection, otherwise known as the *location precision*.

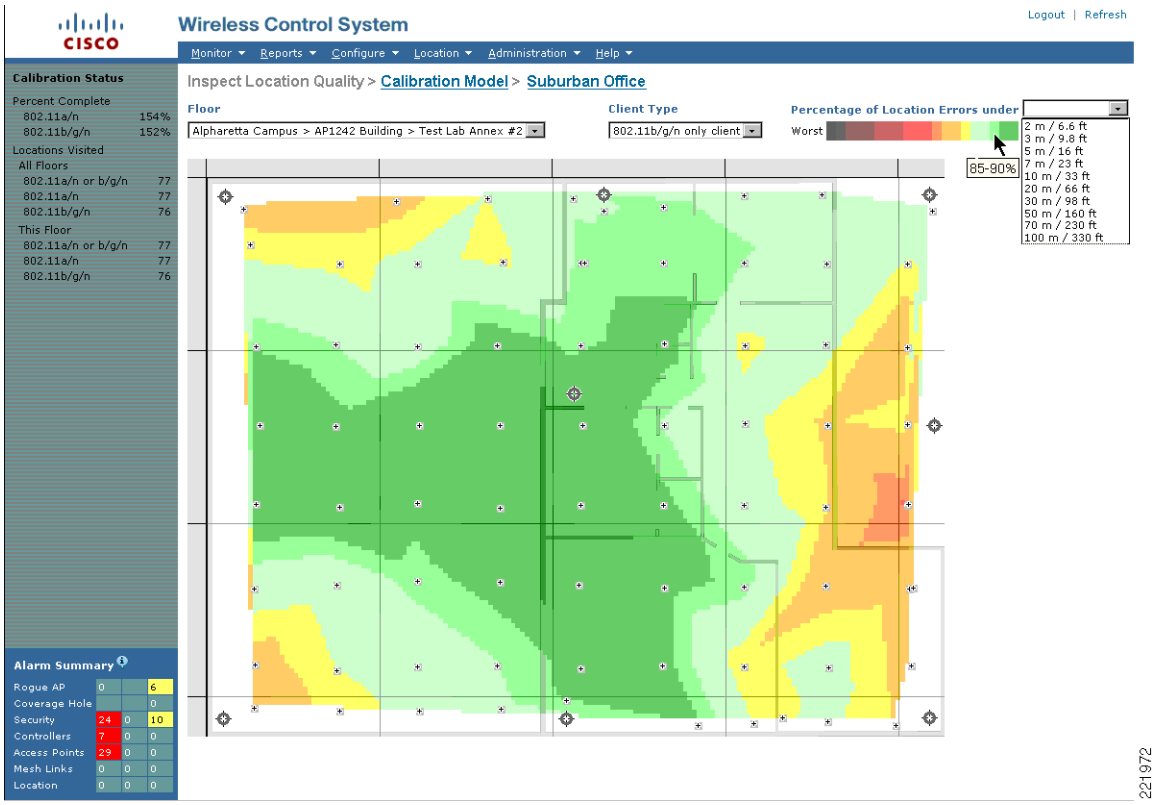
When deployed in accordance with the best practices described in this chapter as well as those contained within the documents referenced in Reference Publications, page 13-2, the location-aware Cisco UWN is capable of excellent accuracy and precision. The Cisco Wireless Location Appliance allows the system to deliver overall baseline performance of 10 meters accuracy with 90 percent precision. The use of chokepoint location capabilities allow the level of accuracy to be even further refined, in some cases to a resolution radius of a foot or less.

These baseline performance levels can be reached using the design, calibration, and deployment tools included with the system. Included are predictive pre-deployment tools such as the *Location Planning* and *Location Readiness* tools, as well as post-deployment verification tools such as the *Location Inspector.*

The Location Planning tool provides recommendations for access point placement and density to create a WLAN deployment that supports location accuracy within the specifications of the location appliance. In software Release 4.1, support for irregularly-shaped polygonal buildings has been added to help organizations address the requirements of such structures. The Location Readiness tool allows network engineers to identify beforehand whether their currently planned access point deployment will support location accuracy within the specifications of the location appliance.

By using the Location Inspection tool shown in Figure 13-2, the system designer can evaluate post-calibration baseline accuracy and precision levels in their actual environment. After an accuracy level is selected, the Location Inspection tool displays, in color-coded format, the level of precision at any point from 0–5 percent all the way to a maximum of 95–100 percent. After viewing the output, the system architect can then work with the installation team to take the necessary steps to ensure that the system's performance is sufficient.

Figure 13-2 Post-Calibration Location Inspection



Using these tools, it is possible to both plan for the achievement of pre-determined performance goals and also verify that these performance targets are being met.

For those interested in a professional service offering that includes the tuning of location accuracy and much more, Cisco offers Wireless LAN Location Planning and Design professional services. This offering enlists the skills of specially-trained WLAN engineers to deliver an integrated solution that includes the services identified as essential for successful deployment of a secure location-based solution. For further information on Cisco Wireless LAN Location Planning and Design Professional Services, see the following URL: http://www.cisco.com/en/US/services/ps2961/ps6899/ps8306/services_overview0900aecd80648a4c.pdf.

Tracking Assets and Rogue Devices

The location-aware Cisco UWN can provide position tracking information for the following:

- *Standard WLAN clients* or *Wi-Fi 802.11 active RFID tags* that are associated or probing the location-aware UWN. These types of wireless LAN clients are displayed on the WCS location floor maps using a blue rectangular icon .
- *802.11 active RFID asset tags* communicating via layer two multicasts (including asset tags compatible with the Cisco Compatible Extensions for Wi-Fi tags specification). These asset tags are displayed on WCS floor maps as a yellow tag icon . In software Release 4.1 of the location-aware Cisco UWN, the *tag summary* icon is introduced to represent two or more tags whose predicted locations are at the same coordinates.

- *Rogue access points,* which are access points that are detected by the wireless LAN infrastructure and determined not to be members of the same mobility group or WLAN system. These are indicated on WCS location floor maps using a skull-and-crossbones within a black circle  .
- *Rogue clients,* which are clients associated to rogue access points. Rogue clients are displayed on the WCS location floor maps using a black rectangle icon with a skull-and-crossbones  .

The location-aware Cisco UWN also displays the location of any chokepoints that have been pre-defined to WCS and the location appliance. Chokepoints are indicated on WCS location floor maps using a blue star within a grey circle  . A concentric band of grey around the icon is used to give a relative indication of the chokepoint range that has been defined in WCS. Note that chokepoint range indication on WCS floor maps is for display purposes only. The actual chokepoint trigger's transmission power and range is configured using the vendor's specific utilities.

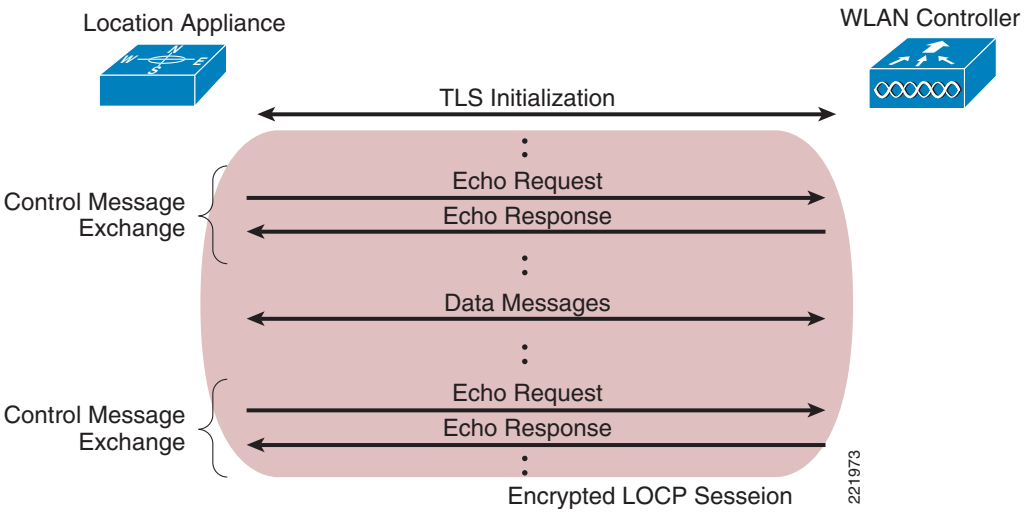
Note Comprehensive information regarding each class of device that can be tracked by the location-aware Cisco UWN is found in the "Location-Based Services Architecture" section of *Wi-Fi Location-Based Services 4.1 Design Guide*, which contains in-depth discussion and analysis and is available at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html.

Cisco Location Control Protocol

The Cisco Location Control Protocol (LOCP), introduced in software Release 4.1 of the Cisco UWN, represents a significant step forward in the support of new capabilities between the location appliance and other components of the Unified Wireless Network. In this release, LOCP augments the traditional SNMP polling of WLAN controllers and serves as the transport for the telemetry, chokepoint, and emergency notification features associated with the newly-introduced Cisco Compatible Extensions for Wi-Fi Tags program.

LOCP is a bi-directional protocol that can be run over a connection-oriented or connectionless transport and can be secured using Transport Layer Security (TLS). It provides for an ongoing exchange of control messages that allows either endpoint to determine whether its partner endpoint is still active, as shown in Figure 13-3, which illustrates a rudimentary LOCP packet exchange between the location appliance and a WLAN controller.

Figure 13-3 Location Appliance WLAN Controller LOCP Session



Cisco Unified Wireless Network software Release 4.1 represents the first phases of Cisco's LOCP implementation, making use of the new protocol to support the transport of information between the location appliance and WLAN controllers for the following:

- Cisco Compatible Extensions for Wi-Fi tag telemetry, such as:
  - Motion, temperature, pressure, humidity, distance, quantity, and status
  - Battery state and predicted remaining battery life
- High priority Cisco Compatible Extensions tag notification traffic, such as:
  - Emergency events (panic button, tag detached, tamper alert)
  - Chokepoint proximity
  - Vendor-specific tag information (used by third party location clients)

The mechanics behind how LOCP is used to provide these capabilities is just one aspect of the protocol that is examined in detail in "The Cisco Location Control Protocol (LOCP)" section of *Wi-Fi Location-Based Services 4.1 Design Guide*. In addition, design considerations surrounding the use of LOCP in the location-aware UWN can be found within the same white paper in the section entitled "Tag Telemetry and Emergency Notification Considerations".

Note Readers are reminded that in Release 4.1 of the Cisco UWN, LOCP augments but *does not replace* SNMP polling between the location appliance and WLAN controllers.

Installation and Configuration

Installing and Configuring the Location Appliance and WCS

Detailed procedures for installing and configuring the Cisco Wireless Location Appliance and WCS may be found using the references mentioned in the "Installation and Configuration" section of *Wi-Fi Location-Based Services 4.1 Design Guide*.

Configuration of the parameters listed under the WCS Location Server > Administration menu are discussed in the document entitled *Cisco Location Appliance Configuration Guide: Editing Location Server Properties* at the following URL: http://www.cisco.com/en/US/docs/wireless/location/2700/3.0/configuration/guide/lacg30.html.

However, there are additional ramifications associated with making changes to the factory defaults that need to be carefully considered. This and other valuable information that a designer of a location-enabled wireless LAN should consider can be found in the "Installation and Configuration" section in *Wi-Fi Location-Based Services 4.1 Design Guide,* including the following:

- History parameters
  - History archive period
  - History data pruning
- Advanced parameters
  - Absent data cleanup interval
  - DB disk memory
  - Run Java GC
  - Defragment database
  - DB free size
- Location parameters
  - Enable calculation time
  - Relative RSSI discard time
  - Absolute RSSI discard time
  - RSSI cutoff
  - Chokepoint Usage
  - Chokepoint Out of Range Timeout
- Notification parameters
- LOCP parameters
- Location appliance dual Ethernet operation
- Location appliance time synchronization
- Cisco Compatible Extensions location measurement
- Setting location appliance passwords
- Proper shutdown (quiescing) of the location appliance

Deployment Best Practices

Location-Aware WLAN Design Considerations

In the past decade, the design best practices for enterprise-ready wireless LANs have evolved from coverage-centric and minimum access point models to those where coverage uniformity and proper cell-to-cell overlap are the predominant requirements. This has been driven by increased interest in deploying new wireless applications that are typically not as tolerant as traditional data-only deployments toward large amounts of dropped packets and roaming delays.

In a similar fashion, the deployment of location-aware WLAN applications requires modification to traditional approaches. This includes the design of "greenfield" location-aware installations as well as the augmentation or retrofitting of existing deployments. For location tracking to function optimally, the correct number of access points along with proper access point placement is a key requirement.

The "Deployment Best Practices" section of *Wi-Fi Location-Based Services 4.1 Design Guide* discusses in great detail several best-practice recommendations for location-aware WLAN deployments, such as the following:

- Minimum received signal thresholds—For mobile devices to be tracked properly, it is highly recommended that access points report mobile device RSSI to their respective controllers at levels meeting or exceeding the *RSSI cutoff* value that is configured in WCS. A minimum of three access points (and preferably four or more for optimum accuracy) should be reporting this level of signal strength or better for any device being localized. Mobile device RSSI reported below this level is eligible for discard by the location appliance.
- Correct access point placement—Proper placement of access points is critical if the system is expected to fully deliver on its performance potential. In many office wireless LANs, access points are distributed throughout interior spaces, providing more than adequate coverage to surrounding work areas. These locations are usually selected on the basis of coverage, WLAN bandwidth, channel re-use, cell-to-cell overlap, security, aesthetics, and deployment feasibility. In a location-aware WLAN design, however, access points must not be located based solely on these criteria but must strike a balance between them and location placement requirements. Although there is no single rule that consistently yields the proper access point density for every environment, the signal threshold and placement suggestions made in the "Deployment Best Practices" section of *Wi-Fi Location-Based Services 4.1 Design Guide* should be followed as a starting point of any location-aware design. Among these recommendations is the adherence to an inter-access point separation of 50 to 70 feet.
- Validating location performance—Although adherence to design and deployment best practices provides the necessary foundation for success, tools that provide corrective feedback to the designer (as well as the installer) play a major role in optimizing performance. The use of predictive tools such as the Location Planning and the Location Readiness tools can identify performance shortcomings early when they are most easily (and most cost-effectively) addressed. Post-deployment tools such as Location Inspection can offer a comprehensive "reality-check" of an entire calibration area by comparing known calibration positions to predictions and calculating the degree of location error. When location accuracy does not conform to specifications, the *location debug* feature can be enabled to allow for more in-depth investigation. This feature displays the access points that contributed to the location calculations for a specific tracked device, the signal strength of these devices, as well as a timestamp of when the signal strength measurement was last received. Newly added in software Release 4.1 of the Cisco UWN, the use of *location test points* allows for impromptu location accuracy checks to be performed by comparing predicted location against the actual physical position of devices bearing selected MAC addresses.

- Minimizing excessive co-channel interference—In many cases, location-based services are added or retrofitted to an existing wireless design, some of which encompass VoWLAN handheld devices (such as the Cisco 792x). When designing a location-aware solution to be used in conjunction with latency-sensitive devices, special care needs to be taken to ensure that excessive co-channel interference is not introduced into the environment. In cases such as this, the needs of an optimal location-aware design must be carefully balanced against the requirements of a properly designed wireless voice infrastructure.
- Avoiding location display "jitter"—At times, devices appear to move on location displays even though they are known to physically be at rest. This can be due to a variety of factors, including the movement of surrounding objects in the environment and slight changes in the orientation of the client and the client's antenna system over time. *Location smoothing* is used to assist in counteracting this phenomena and stabilize location jitter for clients that are not in constant motion.
- Multi-domain design considerations—The Cisco Wireless Location Appliance can provide simultaneous tracking for up to 2500 total devices, which includes WLAN clients, asset tags, rogue access points, and rogue clients. In most cases, a single location appliance and WCS management system should suffice for the majority of applications. However, in larger networks, it may be necessary to use either a single WCS server with multiple location appliances or multiple WCS servers with one or more location appliances.
- Antenna considerations—A discussion of supported antenna combinations for use with the location-aware Cisco UWN, tips on third-party antennas, and antenna orientation best practices. This section includes information on the newly-introduced (in Release 4.1 of the Cisco UWN) antenna vertical height and azimuth capability, which allows the vertical height and x-axis angular offset of access point antennas to be specified in WCS when placing access points on WCS floor maps.
- Site calibration—Post-deployment location calibration can be performed if location accuracy using one of the included calibration models is lower than expected or if the target environment is complex and not well represented by one of the included models. During this calibration, an 802.11 wireless client device is used to take RSSI measurements in the environment. The measured RSSI is then used by the location appliance to fine-tune the path loss model assigned to the environment, which typically leads to improved accuracy and precision. This section contains important tips on performing site calibrations, calibration validity, choosing a calibration client, and improving overall calibration performance. The benefits of performing calibrations using clients compatible with the Cisco Compatible Extensions for WLAN clients specification version 2 or higher are also discussed in detail in this section.

RFID Tag Considerations

The majority of RFID tags currently produced commercially are *passive* RFID tags, consisting basically of a micro-circuit and an antenna. They are referred to as passive tags because they are actively communicating only when they are within the electromagnetic field of a passive RFID tag reader or *interrogator.*

Another type of common RFID tag in the current marketplace is known as the *active* RFID tag, which usually contains a battery that directly powers RF communication. This onboard power source allows an active RFID tag to transmit information about itself at great range, either by constantly *beaconing* this information to a RFID tag reader or by transmitting only when it is prompted to do so. Active tags are usually larger in size and can contain substantially more information (because of higher amounts of memory) than do pure passive tag designs.

The "RFID Tag Considerations" section of *Wi-Fi Location-Based Services 4.1 Design Guide* provides readers who are new to RFID with a foundation in both active and passive tag technologies. Among other areas, this section comprehensively discusses the following:

- Passive RFID technology-Passive and semi-passive RFID tags
- Active RFID technology-Beaconing, transponder, and 802.11 (Wi-Fi) RFID tags
- Multimode RFID technology-A relatively new category offering multiple tag technologies in a single device.
- Chokepoint triggers-Proximity communication devices (often referred to simply as "chokepoints") that trigger tags to alter their configuration or behavior when the tag enters their area of operation.
- Using RFID tags with the Location Appliance-Compatible RFID tags, enabling asset tag tracking, configuring asset tags, and using 802.11b tags on 802.11g networks
- Tag telemetry and notification considerations-Provides initial best practice recommendations and other valuable information pertinent to the design of solutions dependent on telemetry and emergency notification functions.
- Chokepoint design considerations- Provides best practice recommendations and other information pertinent to the design of solutions augmenting the location capabilities of the Cisco UWN with chokepoint-based proximity localization.

SOAP/XML Application Programming Interface

To facilitate the deployment of location-based applications in the enterprise, the Cisco Wireless Location Appliance is equipped with a SOAP/XML API. Applications can make use of the location information contained within the location appliance by importing components via the API such as entire network maps including buildings, floors, access points, chokepoints, coverage areas, and device lists. Actionable data can also be imported, such as recent and historical location as well as statistical device information. Location-based alarms and notifications can be triggered in applications through area boundary definitions, chokepoint proximity, tag emergency or missing status, tag battery status, allowed areas, and allowed distances. All these capabilities allow the SOAP/XML API interface to the Cisco Wireless Location Appliance API to be used for integration with external software applications such as location-enabled asset management, enterprise-resource-planning (ERP) tools, and workflow automation systems.

From a high-level perspective, a third-party application system can use the SOAP/XML API to participate as a member of a location-aware system consisting of the following four basic components:

- Location client—The primary role of the location client is to serve as the interface to the location and asset information contained on the location server.
- Control client—The primary role of the control client is to populate the server with information about the physical environment (network designs, floors maps, calibration models, access point locations, and so on) as well as the network elements that should be monitored.
- Location server— The location server provides general location services for the Cisco UWN and is responsible for running the algorithms that predict device location.
- WLAN system—All the monitored mobile devices (tags, mobile stations, rogue clients, and access points) as well as supporting devices (such as chokepoint triggers) that serve as key components of the wireless network, as well as the embedded software contained within WLAN controllers.

An in-depth examination of a location client implementation by a Cisco Technology Partner can be found in the document entitled *Design Considerations for Cisco – PanGo Asset Tracking*, which is located at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/pango/PanGoEx.html.

The location appliance API is available and licensable to the Cisco development community along with tools to facilitate solution development. Integration support is available via the Cisco Developer Services Program. For complete details on this program, see the following URL: http://www.cisco.com/go/developersupport.

GLOSSARY

A

AAA Authentication, Authorization, and Accounting.

ACS Cisco Access Control Server.

AES Advanced Encryption Standard.

AP Access point.

B

BSSID Basic service set identifier.

C

CAM Clean Access Manager.

CCMP Counter Mode with Cipher Block Chaining Message Authentication Code Protocol.

CCX Cisco Compatible Extensions.

CKIP Cisco Key Integrity Protocol.

CMIC Cisco Message Integrity Check.

CSA Cisco Security Agent.

CSSC Cisco Secure Services Client.Cisco Key Integrity Protocol (CKIP) and Cisco Message Integrity Check (CMIC).

D

DoS Denial of service.

E

EAP Extensible Authentication Protocol.

EAP-FAST EAP-Flexible Authentication via Secured Tunnel.

EAP-TLS EAP-Transport Layer Security.

EIRP Effective Isotropic Radiated Power.

ESSID Extended service set identifier, commonly referred to as an SSID.

F

FWSM Firewall Services Module.

I

IDS Intrusion detection system.

IPS Intrusion prevention system.

L

LAP LWAPP Access Point.

LBS Location-based service

LWAPP Lightweight Access Point Protocol.

M

MAP Mesh AP

MFP Management frame protection.

MIC Message integrity check.

N

NAC Network Admission Control.

O

OFDM Orthogonal Frequency Division Multiplexing.

P

PEAP GTC Protected EAP Generic Token Card.

PEAP MSCHAP Protected EAP Microsoft Challenge Handshake Authentication Protocol.

PKI Public Key Infrastructure.

R

RADIUS Remote Authentication Dial-In User Service.

RF Radio frequency.

RFID Radio frequency.Radio-frequency identification.

RLDP Rogue Location Discovery Protocol.

RSSI Received signal strength indication.

S

SNR Signal-to-noise ratio.

SSID IEEE Extended Service Set Identifier.

SSO Single sign-on.

SVI Switched virtual interfaces.

T

TKIP Temporal Key Integrity Protocol.

TLS Transport Layer Security.

W

WCS Wireless Control System.

WEP Wired Equivalent Privacy.

Wi-Fi Wi-Fi is the brand of the Wi-Fi Alliance, which certifies interoperability of products and services based on IEEE 802.11 technology.

WiSM Wireless Services Module.

WLAN Wireless LAN.

WLC Wireless LAN Controller.

WLCM Wireless LAN Controller Module.

WLSM Wireless LAN Services Module.

WMM Wi-Fi Multimedia

WPA Wi-Fi Protected Access.