Voice over Wireless LAN 4.1 Design Guide

Cisco Validated Design I

January 18, 2010

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

Text Part Number: OL-14684-01

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.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CONTENTS

CHAPTER 1

CHAPTER 2

CHAPTER 1

Voice over WLAN Introduction

About the Guide

Document Purpose and Audience

This guide is intended for systems design engineers who are responsible for designing, implementing, and operating the Cisco Voice over Wireless LAN (VoWLAN) solution.

Document Organization

This guide contains the following chapters:

Section	Description
This chapter	Provides an overview of the VoWLAN 4.1 solution.
Chapter 2, "WLAN Quality of Service."	Provides an overview of WLAN QoS and its implementation in the Cisco Unified Wireless Network.
Chapter 3, "Voice over WLAN Radio Frequency Design."	Provides an overview of the RF network requirements of VoWLAN deployments and a discussion of the RF deployment issues.
Chapter 4, "Voice over WLAN Security."	Provides an overview of WLAN Security as it applies to VoWLAN deployments.
Chapter 5, "Voice over WLAN Roaming."	Provides an overview of WLAN roaming fundamentals.
Chapter 6, "Voice over WLAN Campus Test Architecture."	Provides the configuration and design information for campus network design and configuration used in this design guide.
Chapter 7, "Voice over WLAN Unified Communications Test Architecture."	Provides configuration and design information for Unified Communications Architecture design and configuration used in this guide
Chapter 8, "Voice over WLAN Wireless LAN Controller Design and Configuration."	Provides configuration and design information for Cisco Unified Wireless Network design and configuration used in this guide
Chapter 9, "Voice over WLAN Troubleshooting and Management Tools."	Provides troubleshooting and management tools for the VoWLAN solution.

Section	Description
Chapter 10, "Cisco Unified IP Phone 7921 Implementation for Voice over WLAN."	Provides design and configuration information for the Cisco Unified Wireless IP Phone 7921G in the context of a VoWLAN environment.
Chapter 11, "Voice over WLAN Vocera Implementation."	Provides details for the Vocera Communication system used in this design guide.
Appendix A, "Deploying and Operating a Secure Voice over Wireless LAN Solution with Cisco Lifecycle Services."	Describes how to deploy and operating a secure voice over wireless LAN solution.

VoWLAN Solution Overview

The mobile user needs the same applications and services with the same accessibility, security, quality-of-service (QoS), and high availability delivered to wired users. Many users now enjoy the benefits of mobile access to their key enterprise applications through the Cisco Unified Wireless Network, but these applications are primarily based on data communications. Equally important within an enterprise is voice communication. The purpose of this design guide is to assist customers and systems engineers design, implement, and operate VoWLAN applications in an enterprise campus. To demonstrate these features this guide uses the Cisco 7921G VoWLAN Handset and Vocera B1000A badges, and builds upon the mobility, campus, unified communication, and location design guides from: http://www.cisco.com/en/US/netsol/ns742/networking_solutions_program_category_home.html

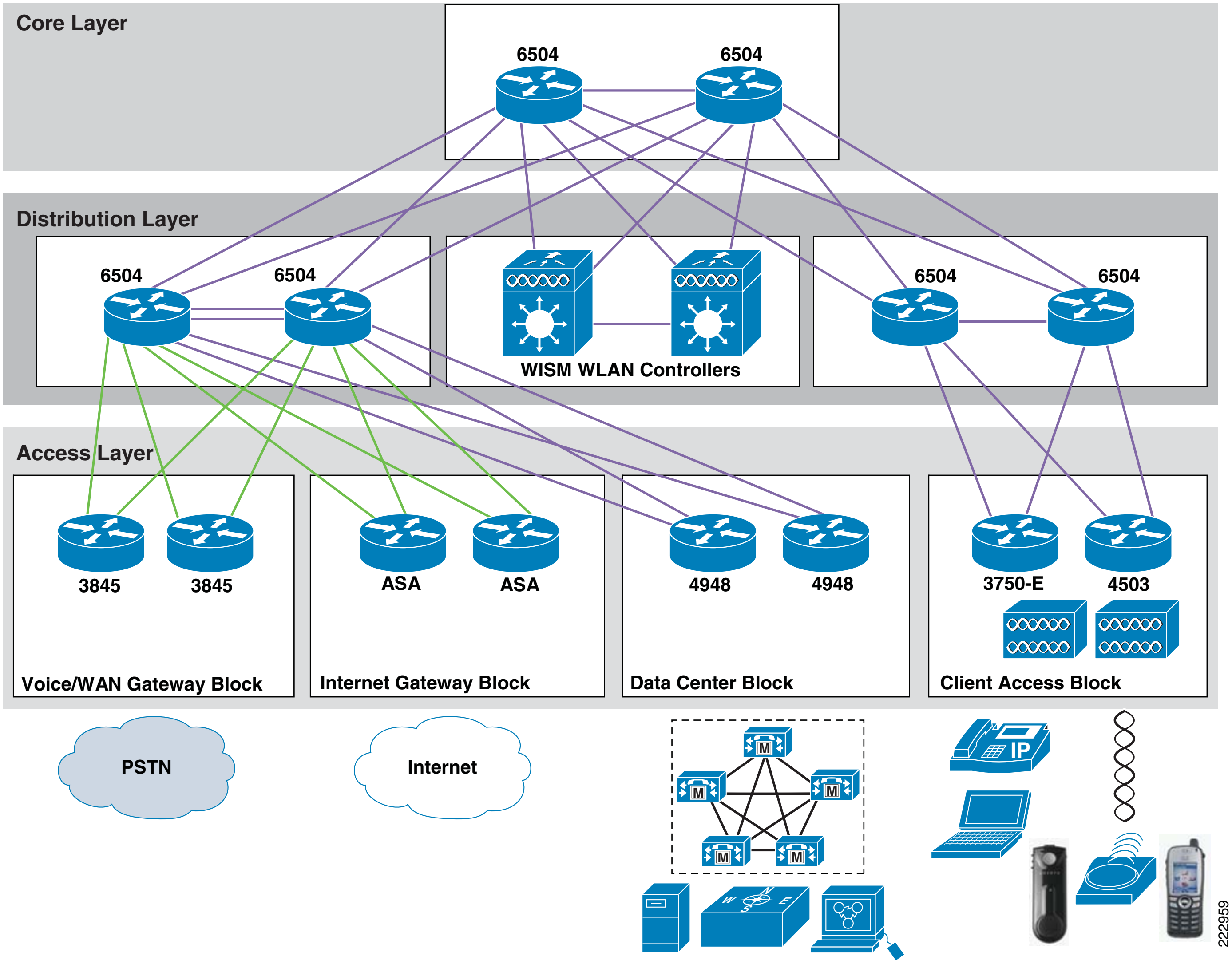
VoWLAN Solution Network Design Overview

The Cisco campus design (see Figure 1-1) is the platform used for testing and design of the VoWLAN solution. This Cisco campus design uses a typical hierarchical, access, distribution, core design. The following additional modules were included to this design for the VoWLAN solution:

- Services module to provide the Cisco Unified Wireless Network
- Data center module
- Voice WAN Gateway module
- Internet Gateway module

The VoWLAN solutions installed and tested for this design were the Cisco 7921G with the Cisco Unified Communications Manager, and the Vocera Communications System.

Figure 1-1 VoWLAN Solution Network Overview



Solution Benefits

Enterprises today are faster paced than ever before. Staying ahead of competition, success, and growth are dependent upon efficient employees, collaboration, and a timely business process. Today, we see that enterprises have a strong drive for efficiency, are looking to eliminate delays, and are dependent on team collaboration to support complex business processes. While maintaining a secure corporate data and voice infrastructure, enterprises are encouraging a mobile work style to get more done. Additionally, enterprises are not just streamlining processes through technology, but are also looking to increase their revenue and reduce costs with the latest technological trends.

Customer Requirements

The following are the customer requirements for deploying the VoWLAN solution:

- Reduce mobile cellular minutes—VoWLAN calls are free and employees would now use their VoWLAN handset on campus instead of their cell phone.
- Integrate Mobile and Enterprise Telephony systems—Mobile WiFi handsets can now be integrated with IP-PBX features and numbering plans and thus not have to return to their desk phone for certain features.
- No difficulty with cellular coverage since enterprises can deploy adequate access points to improve coverage.
- Provide mobile handsets for users that are not personal phones, in many enterprises it is inappropriate to be taking personal calls. A cell phones merges the personal and work phone into the same device, and despite the good will of the employee, many people do not feel that calling you on your cell phone is the same as calling you at work.
- In many industries the employee turn over makes the provision of a cell phones and expensing of cell phone calls difficult; therefore, the management of cell phone usage difficult. At the same time, communication with mobile employees is critical to business success. It is simpler and more cost efficient to provide a VoWLAN handset.
- Provide communications when other communications infrastructure is unavailable either due to emergency or lack of local services.

The need for a VoWLAN solution has grown because of the demand in different industry organizations as well. Industry organizations can take this solution and customize according to their needs. Two examples of industry organization that are looking to meet everyday requirements with VoWLAN are healthcare and retail organizations.

Healthcare

Many healthcare organizations today are burdened by multiple disjointed communication systems. A typical hospital may have several in-house phone systems, overhead paging systems, and pagers, and typically more than one data network. As the Forrestor 2006 survey –below- illustrates, these communication inefficiencies exacerbate staff shortages and impact care delivery. According to a study done by Forrester (2006):

- 65% of healthcare employees spend about 20-60 minutes / day just trying to reach staff.
- 66% search more than one channel to reach staff
- 84% said that time spent trying to reach staff impacts patient care. "Every minute engaged in tracking and locating others reduces a nurses availability for the patient."

Retail

Retail organizations can realize many benefits from deploying the VoWLAN solution, including:

- Improved customer service by freeing personnel from having to provide personalized service only from fixed locations
- Increased profits through operational efficiency and improved customer satisfaction
- Improved communication by giving phone services and voicemail to each store employee
- Improved responsiveness by making business applications, like inventory management, mobile with wireless phones

The Cisco VoWLAN solution can meet these requirements . Many businesses are turning to WLAN networking to give employees immediate access to the business applications and communication tools they need. By adding voice over IP capability to their wireless networks, they can further improve collaboration and responsiveness, and unlock the door to new cost savings. The Cisco wireless network is ready to support voice applications. VoWLAN allows businesses and other organizations to bring the mobility and flexibility of WLAN networking to their voice communications systems. With robust quality-of-service, diverse client support, and manageability, the solution enables the enterprise to take immediate advantage of IP communications to a campus workforce. The Cisco Enterprise Mobility solution streamlines business processes by providing anytime, anywhere access to critical information, and safeguarding information and network integrity in the new era of wireless threats. It delivers applications that transform business operations to deliver compelling benefits and are enabled on a simple, secure, and scalable unified platform for the lowest total cost of ownership. This VoWLAN solution is designed for businesses of all sizes that need to improve business processes, safeguard information and improve customer, partner and employee experience and loyalty.

Recommendations

During the research and development of this design guide, the following key findings were made:

- Planning, RF design, and site survey are critical parts of an optimal VoWLAN deployment.
- Auto-RF should be enabled in most cases for VoWLAN, but to allow Auto-RF to perform its role effectively, it requires a best practice RF design and site survey for VoWLAN. Just as in a static RF deployment, extra effort is required to maximize VoWLAN success.
- A simple choice between Auto-RF and no-Auto-RF is not required. There are a number of different options that may be a best fit for customers requirements. For example, there are the options when the Transmit Power Control (TPC) algorithms are run, and there are options upon the sensitivity settings for the Dynamic Channel Allocation (DCA), TPC, and Coverage Hole algorithms.
- Location and VoWLAN deployments are not incompatible. The required spacing of APs for VoWLAN deployment is very similar to that of a Location-Based Services (LBS) deployment. Additional APs may be required to meet the perimeter requirements of LBS. These additional APs are unlikely to add capacity to the WLAN system (particularly in the 2.4GHz band), and the additional APs are unlikely to have great impact upon the overall co-channel interference characteristics of the deployment.
- Depending on the shape of the WLAN deployment there may be little difference between a VoWLAN deployment and an LBS deployment, but is advisable to follow the LBS practice of ensuring there is perimeter placement of APs. This provides optimal location accuracy and likely assists in optimal Auto-RF behavior.
- The best strategy to address the co-channel issues that increase due to the higher density deployments of VoWLAN and LBS in 2.4GHz systems is to migrate as many devices as possible to the 5GHz spectrum which has more non-overlapping channels, and therefore less co-channel issues and higher capacity.

Table 1-1 lists the devices, roles, and releases of the products used in the VoWLAN 4.1 solution.

Table 1-1 Device and Roles

Device	Role	Software
6504	Campus Core	12.2(18)SXF9
6504	Campus Distribution	12.2(18)SXF9
6504	WLAN	12.2(18)SXF9
WiSM	WLAN	4.1.185
3845	Voice WAN gateway	12.4(15)T1
ASA	Internet gateway	7.2(2)
4948	Data center	12.2(25)EWA8
4503	Access	12.2(37)SG
3750-E	Access	12.2(37)SE1
2821	Branch Router	12.4(15)T1
MC7800	Unified CM	CM 6.0.1
7960	VoIP Handset	SCCP41.8-3-1S
7921G	VoWLAN Handset	CP7921G-1.0.4
MCS7800	Vocera Server	Vocera Server 4.0 [Build 1279] Vocera Telephony Server 4.0 [Build 1279]
B1000A	Vocera Badge	Vocera Badge V4.0 1273

CHAPTER 2

WLAN Quality of Service

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

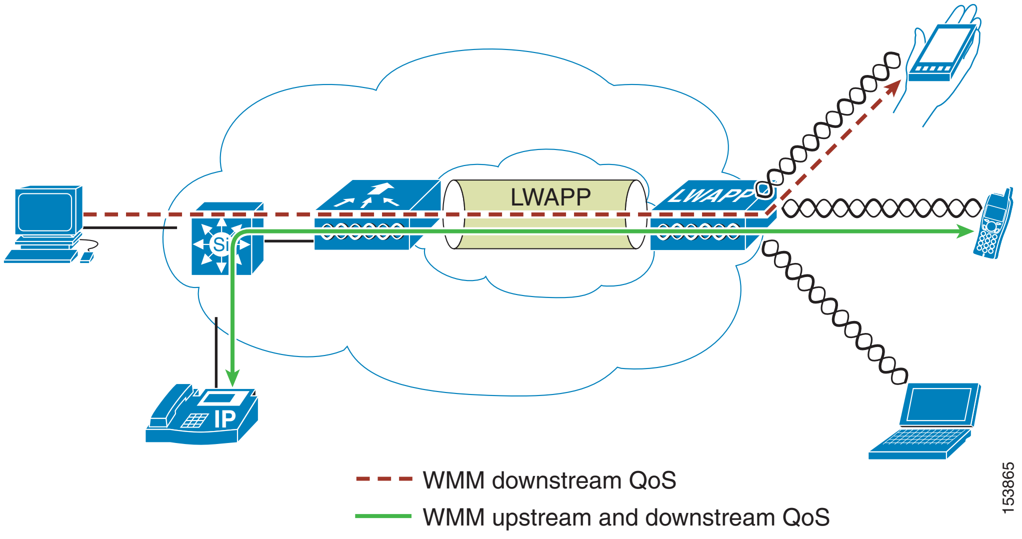
In the past, WLANs were mainly used to transport low-bandwidth, data-application traffic. Currently, with the expansion of WLANs into vertical (such as retail, finance, and education) and enterprise environments, WLANs are used to transport high-bandwidth data applications, in conjunction with time-sensitive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

Several vendors, including Cisco, have supported 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 Wi-Fi MultiMedia (WMM) and Cisco Compatible Extensions programs, ensuring the delivery of key features and interoperation through their certification programs.

Cisco Unified Wireless products support 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.

An example deployment of wireless QoS based on the Cisco Unified Wireless technology features is shown in Figure 2-1.

Figure 2-1 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 2-1.

Table 2-1 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 2-2 illustrates the definition of *radio upstream* and *radio downstream* QoS.

Figure 2-2 Upstream and Downstream QoS

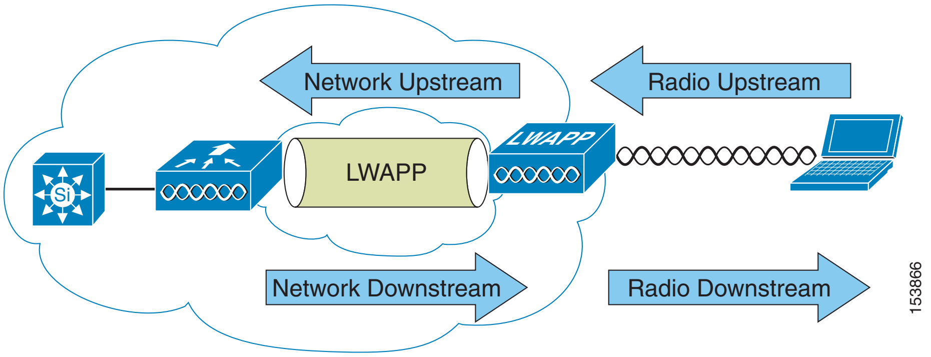


Figure 2-2 shows the following:

- *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 coordination function (EDCF). 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.

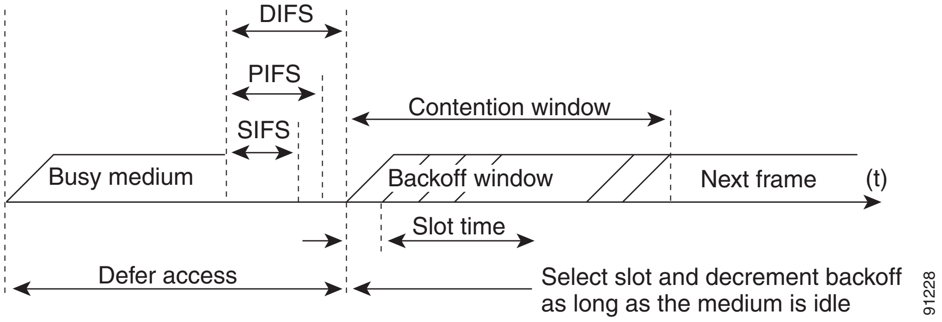
Interframe Spaces

802.11 currently defines three interframe spaces (IFS), as shown in Figure 2-3:

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

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 2-3 Interframe Spaces



Random Backoff

When a data frame using Distributed Coordination Function (DCF), shown in Figure 2-4, is ready to be sent, it goes through the following steps:

Step 1 Generates a random backoff number between 0 and a minimum contention window (CWmin).

Step 2 Waits until the channel is free for a DIFS interval.

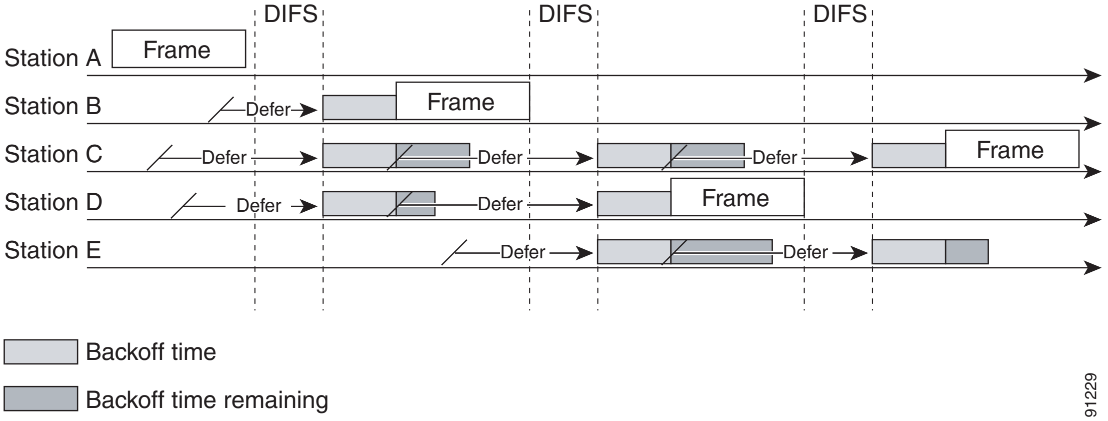
Step 3 If the channel is still free, begins to decrement the random backoff number, for every slot time (20 µs) that the channel remains free.

Step 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.

Step 5 If the channel remains free until the random backoff number reaches 0, the frame can be sent.

Figure 2-4 shows a simplified example of how the DCF process works. In this simplified DCF process, no acknowledgements are shown and no fragmentation occurs.

Figure 2-4 Distributed Coordination Function Example



The DCF steps illustrated in Figure 2-4 are as follows:

Step 1 Station A successfully sends a frame; three other stations also want to send frames but must defer to Station A traffic.

Step 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.

Step 3 The backoff counter of Station B reaches zero before Stations C and D, and therefore Station B begins transmitting its frame.

Step 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.

Step 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.

Step 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.

Step 7 The process continues as traffic arrives on different stations.

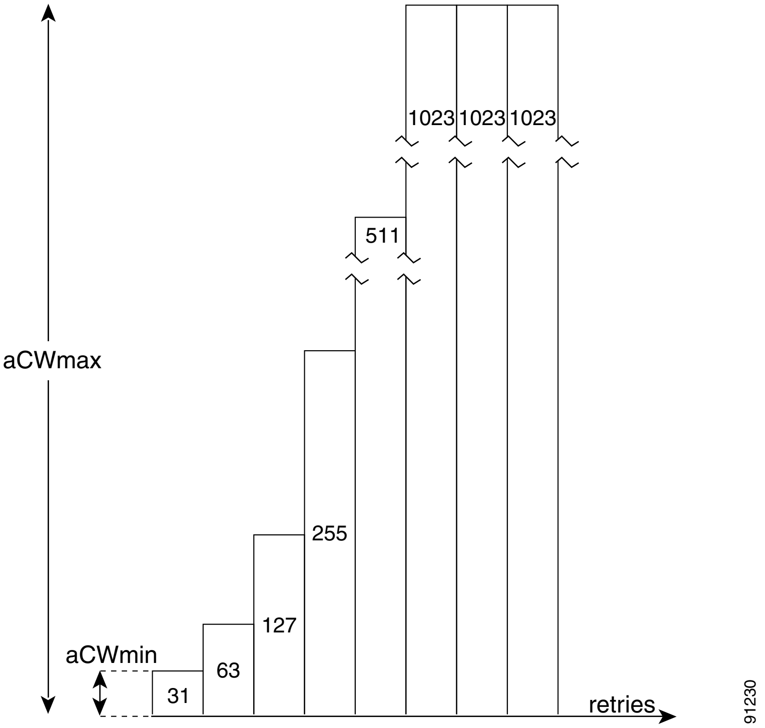
CWmin, CWmax, and Retries

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 2-5 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 2-5 Growth in Random Backoff Range with Retries



Wi-Fi MultiMedia

This section describes three Wi-Fi MultiMedia (WMM) implementation topics:

- WMM Access
- WMM Classification
- WMM Queues

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 EDCF 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 2-2.

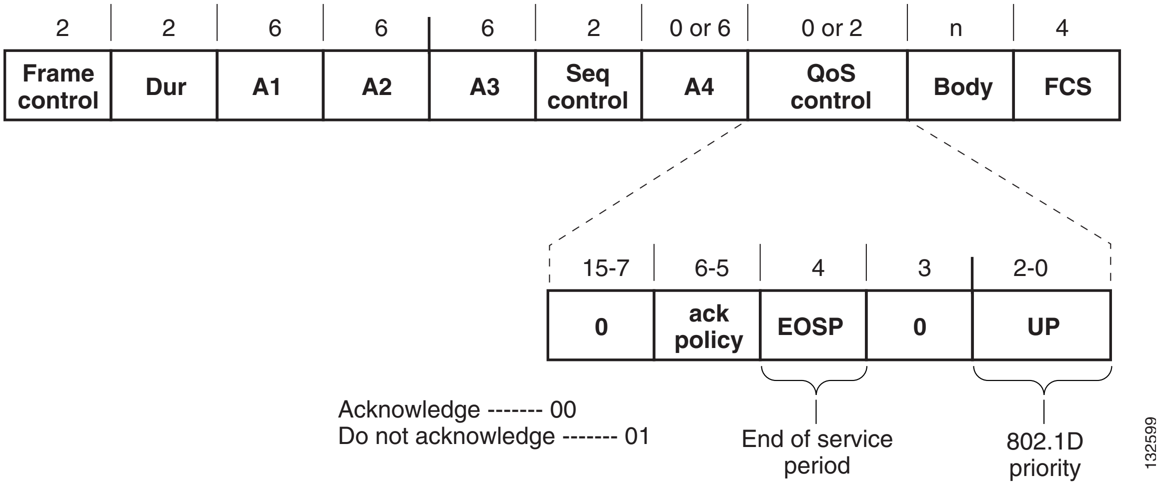
Table 2-2 Table 2 802.1P and WMM Classification

Priority	802.1P Priority	802.1P Designation	Access Category (AC)	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 2-6 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 2-6 WMM Frame Format



WMM Queues

Figure 2-7 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 coordination function (EDCF).

Figure 2-7 WMM Queues

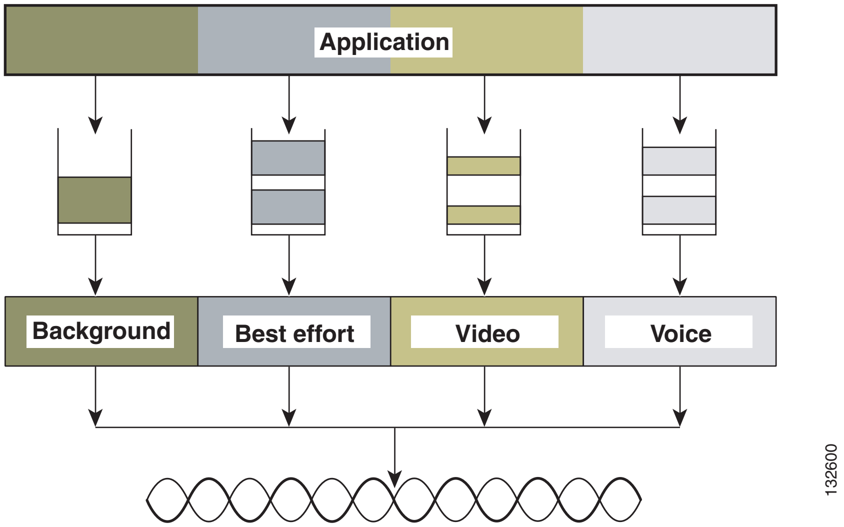
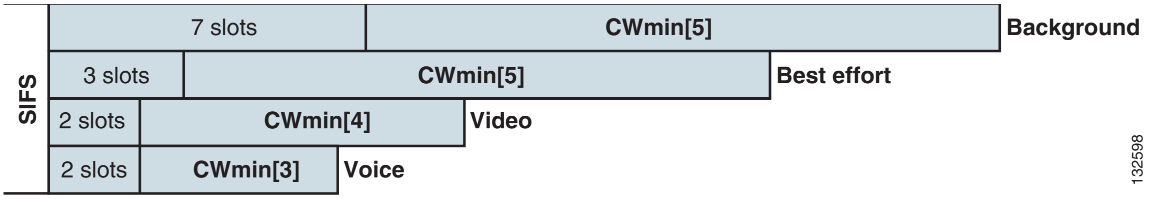


Figure 2-8 shows the principle behind EDCF where different interframe spacing and CWmin and CwMax values (for clarity CwMax is not shown) are applied per traffic classification. Different traffic types can wait different interface spaces before counting down their random backoff, and the CW value used 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.

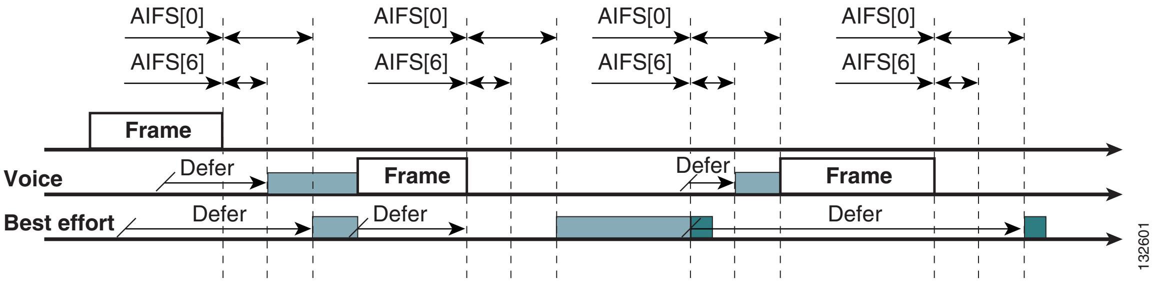
Figure 2-8 Access Category (AC) Timing



EDCF

The EDCF process is illustrated in Figure 2-9, using data from Figure 2-8.

Figure 2-9 EDCF Example



The EDCF 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 AC settings shown in Table 2-3 and Table 2-4 are, by default, the same for an 802.11a radio, and are based on formulas defined in WMM.

Note Table 2-3 refers to the parameter settings on a client, which are slightly different from the settings for an AP. This is because an AP is expected to have multiple clients and must send frames more often.

Table 2-3 WMM AP 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 2-3 WMM AP Parameters (continued)

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 2-4 WMM Client Parameters

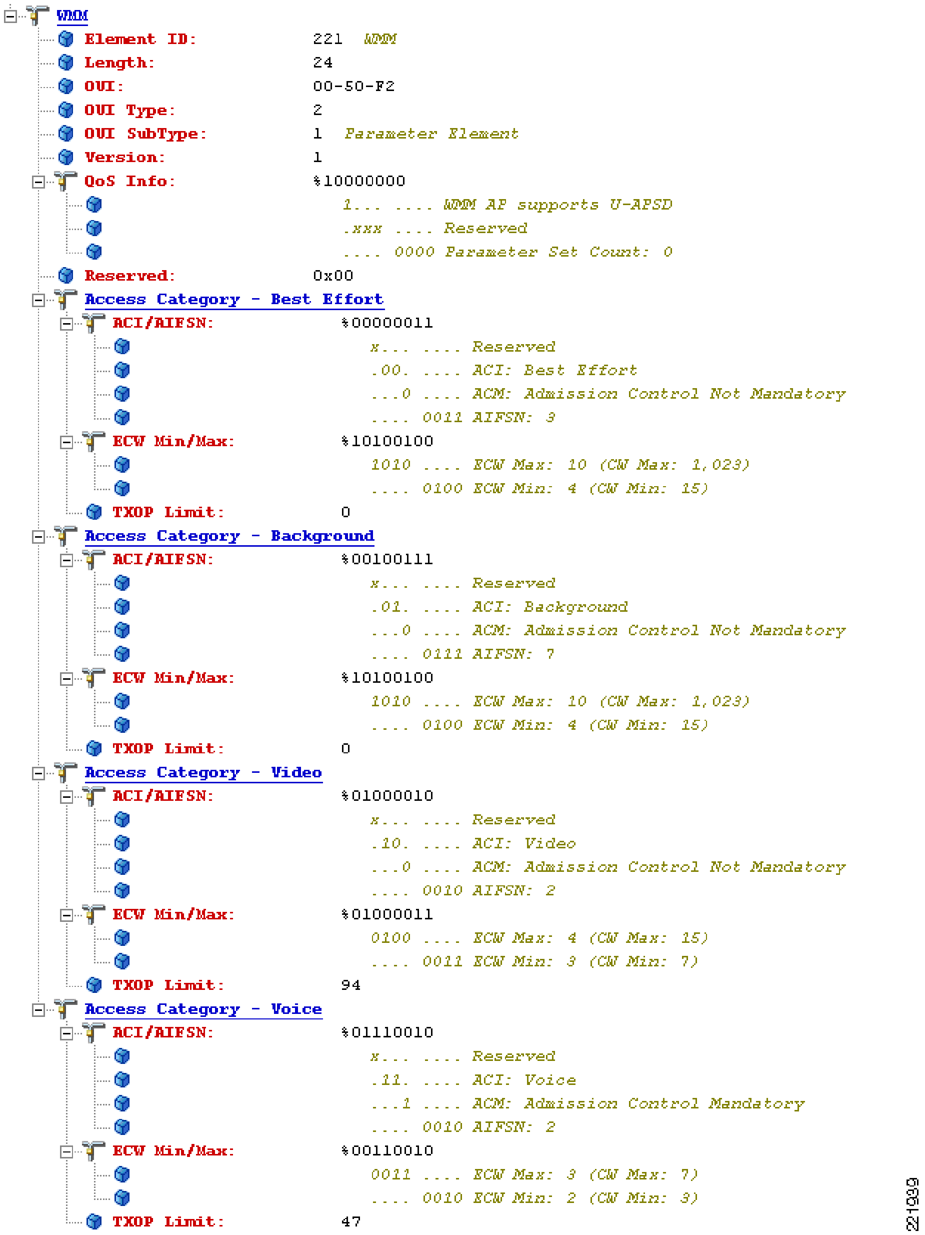
Access Category	CWmin	CWmax	AIFSN	TXOP Limit (802.11b	TXOP Limit (802.11a/g)
AC_BK	aCWmin	aCWmax	7	0	0
AC_BE	aCWmin	4*(aCQmin+1)-1	3	0	0
AC_VI	(aCWmin+1)/2-1	aCWmin	2	6.016 ms	3.008 ms
AC_VO	(aCWmin+1)/4-1	(aCWmin+1)/2-1	2	3.264 ms	1.504 ms

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 2-8.

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 2-10 shows the WMM information in a probe response. Apart from the WMM AC 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 2-10 Probe Response WMM Element Information



```
WMM
    Element ID:            221  WMM
    Length:                24
    OUI:                   00-50-F2
    OUI Type:              2
    OUI SubType:           1  Parameter Element
    Version:               1
    QoS Info:              %10000000
                              1... .... WMM AP supports U-APSD
                              .xxx .... Reserved
                              .... 0000 Parameter Set Count: 0
    Reserved:              0x00
    Access Category - Best Effort
        ACI/AIFSN:             %00000011
                                  x... .... Reserved
                                  .00. .... ACI: Best Effort
                                  ...0 .... ACM: Admission Control Not Mandatory
                                  .... 0011 AIFSN: 3
        ECW Min/Max:           %10100100
                                  1010 .... ECW Max: 10 (CW Max: 1,023)
                                  .... 0100 ECW Min: 4 (CW Min: 15)
        TXOP Limit:            0
    Access Category - Background
        ACI/AIFSN:             %00100111
                                  x... .... Reserved
                                  .01. .... ACI: Background
                                  ...0 .... ACM: Admission Control Not Mandatory
                                  .... 0111 AIFSN: 7
        ECW Min/Max:           %10100100
                                  1010 .... ECW Max: 10 (CW Max: 1,023)
                                  .... 0100 ECW Min: 4 (CW Min: 15)
        TXOP Limit:            0
    Access Category - Video
        ACI/AIFSN:             %01000010
                                  x... .... Reserved
                                  .10. .... ACI: Video
                                  ...0 .... ACM: Admission Control Not Mandatory
                                  .... 0010 AIFSN: 2
        ECW Min/Max:           %01000011
                                  0100 .... ECW Max: 4 (CW Max: 15)
                                  .... 0011 ECW Min: 3 (CW Min: 7)
        TXOP Limit:            94
    Access Category - Voice
        ACI/AIFSN:             %01110010
                                  x... .... Reserved
                                  .11. .... ACI: Voice
                                  ...1 .... ACM: Admission Control Mandatory
                                  .... 0010 AIFSN: 2
        ECW Min/Max:           %00110010
                                  0011 .... ECW Max: 3 (CW Max: 7)
                                  .... 0010 ECW Min: 2 (CW Min: 3)
        TXOP Limit:            47
```

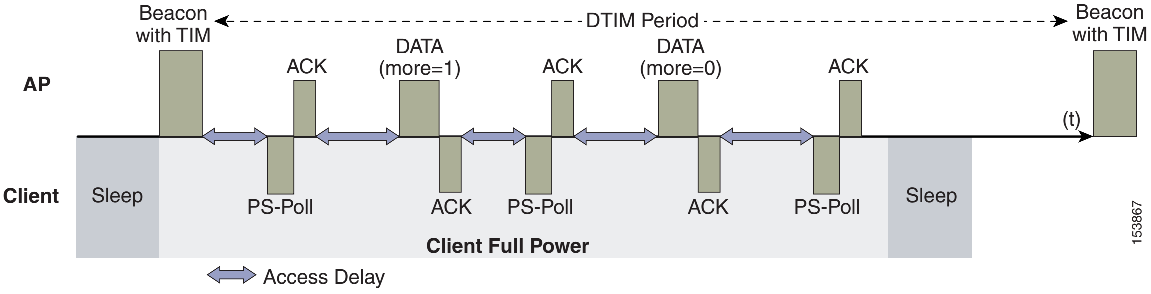
U-APSD

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 AC. 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 map (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 2-11 shows an example frame exchange for the standard 802.11 power save delivery process.

Figure 2-11 Standard Client Power-Save

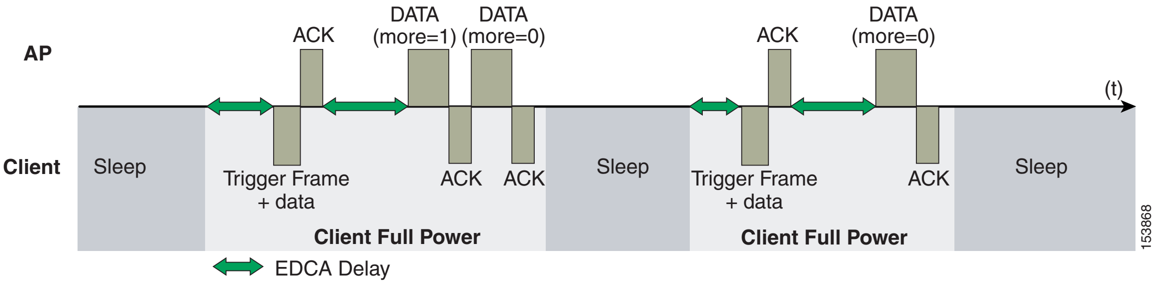


The client in power-save mode first detects that there is data waiting for it at the AP via the presence of the traffic indicator map (TIM) in the AP beacon. The client must power-save poll (PS-Poll) the AP to retrieve that data. If the data sent to the client requires more than one frame to be sent, 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 Cisco Unified Wireless IP Phone 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 Cisco Unified Wireless IP Phone 7921Gs on WLANs without U-APSD.

Figure 2-12 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 2-12 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 EDCF 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 ACs in EDCF. 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 EDCF 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 Cisco Unified Wireless IP Phone 7921G, which does have support for TSpec, the Cisco Unified Wireless IP Phone 7920 WVoIP handset does not support TSpec admission control.

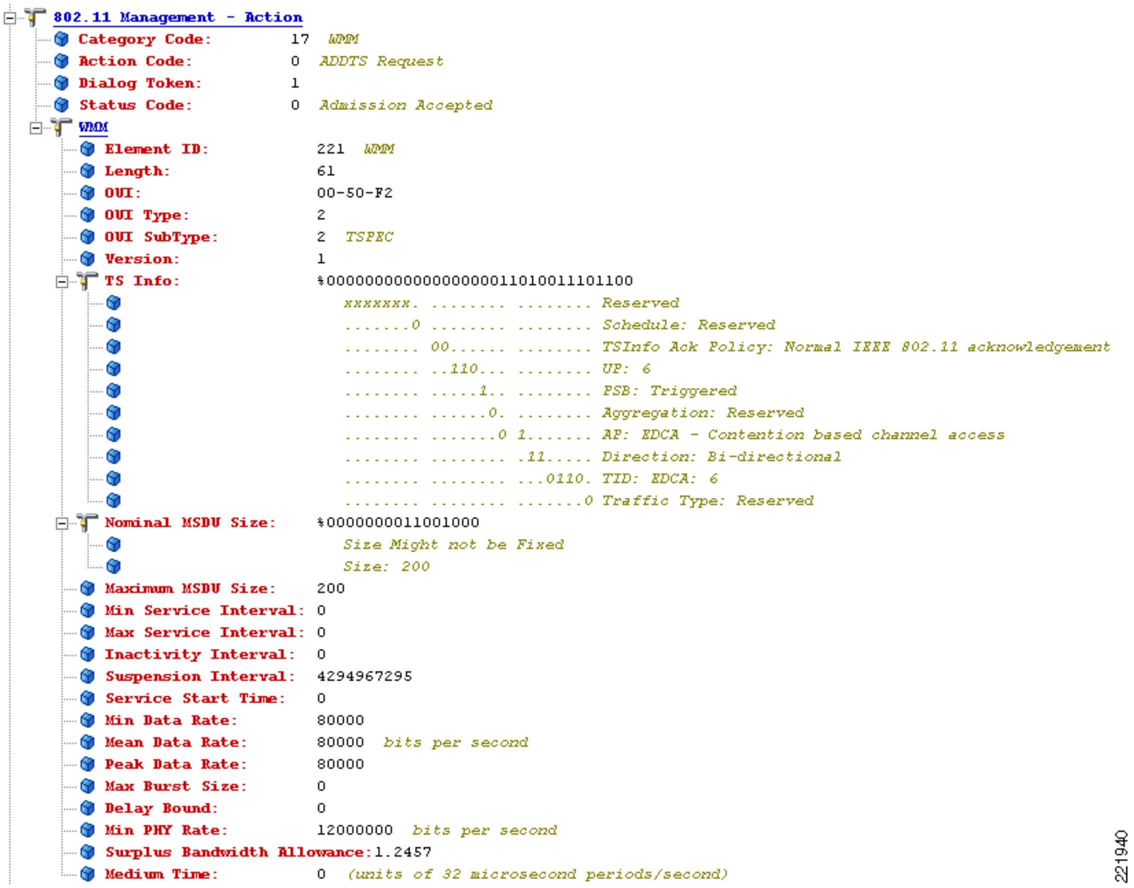
Add Traffic Stream

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.

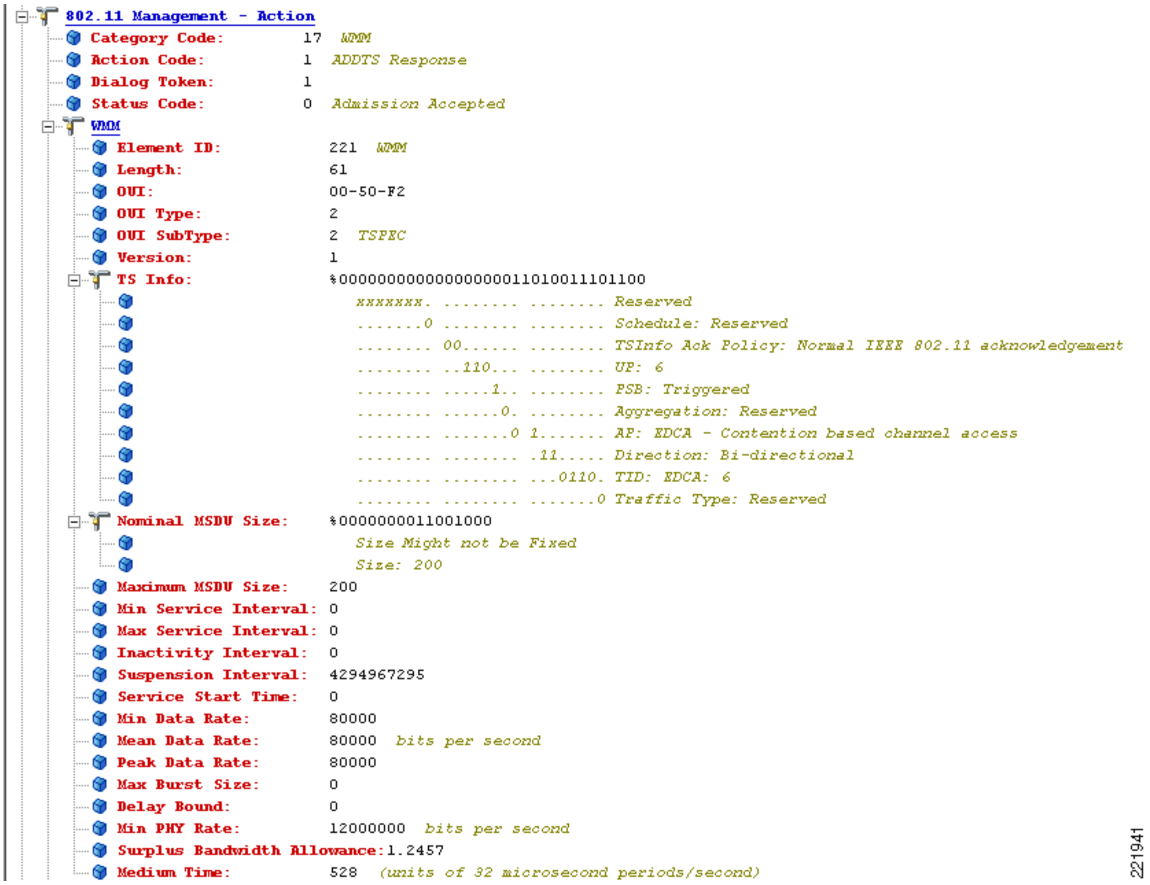
The ADDTS contains the TSpec element that describes the traffic request. See Figure 2-13 and Figure 2-14 for examples of an ADDTS request and response between a Cisco Unified Wireless IP Phone 7921G WLAN handset and a Cisco AP. Apart from key data describing the traffic requirements, such as data rates 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 2-13 ADDTS Request Decode



```
802.11 Management - Action
  Category Code:         17  WMM
  Action Code:           0   ADDTS Request
  Dialog Token:          1
  Status Code:           0   Admission Accepted
  WMM
    Element ID:            221  WMM
    Length:                61
    OUI:                   00-50-F2
    OUI Type:              2
    OUI SubType:           2  TSPEC
    Version:               1
    TS Info:               %00000000000000000011010011101100
                              xxxxxxx. ........ ........ Reserved
                              .......0 ........ ........ Schedule: Reserved
                              ........ 00...... ........ TSInfo Ack Policy: Normal IEEE 802.11 acknowledgement
                              ........ ..110... ........ UP: 6
                              ........ .....1.. ........ PSB: Triggered
                              ........ ......0. ........ Aggregation: Reserved
                              ........ .......0 1....... AP: EDCA - Contention based channel access
                              ........ ........ .11..... Direction: Bi-directional
                              ........ ........ ...0110. TID: EDCA: 6
                              ........ ........ .......0 Traffic Type: Reserved
    Nominal MSDU Size:     %0000000011001000
                              Size Might not be Fixed
                              Size: 200
    Maximum MSDU Size:     200
    Min Service Interval:  0
    Max Service Interval:  0
    Inactivity Interval:   0
    Suspension Interval:   4294967295
    Service Start Time:    0
    Min Data Rate:         80000
    Mean Data Rate:        80000  bits per second
    Peak Data Rate:        80000
    Max Burst Size:        0
    Delay Bound:           0
    Min PHY Rate:          12000000  bits per second
    Surplus Bandwidth Allowance:1.2457
    Medium Time:           0  (units of 32 microsecond periods/second)
```

Figure 2-14 ADDTS Response Decode

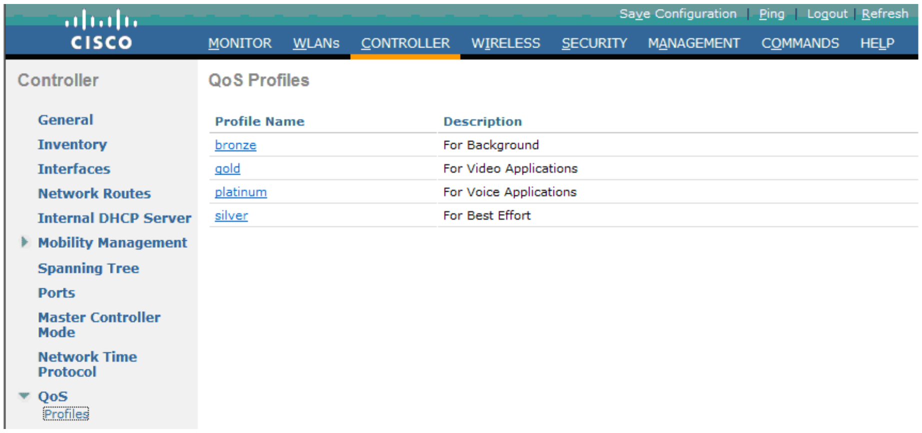


```
802.11 Management - Action
    Category Code:          17  WMM
    Action Code:            1  ADDTS Response
    Dialog Token:           1
    Status Code:            0  Admission Accepted
    WMM
        Element ID:             221  WMM
        Length:                 61
        OUI:                    00-50-F2
        OUI Type:               2
        OUI SubType:            2  TSPEC
        Version:                1
        TS Info:                %00000000000000000011010011101100
                                   xxxxxxx. ........ ........ Reserved
                                   .......0 ........ ........ Schedule: Reserved
                                   ........ 00...... ........ TSInfo Ack Policy: Normal IEEE 802.11 acknowledgement
                                   ........ ..110... ........ UP: 6
                                   ........ .....1.. ........ PSB: Triggered
                                   ........ ......0. ........ Aggregation: Reserved
                                   ........ .......0 1....... AP: EDCA - Contention based channel access
                                   ........ ........ .11..... Direction: Bi-directional
                                   ........ ........ ...0110. TID: EDCA: 6
                                   ........ ........ .......0 Traffic Type: Reserved
        Nominal MSDU Size:      %0000000011001000
                                   Size Might not be Fixed
                                   Size: 200
        Maximum MSDU Size:      200
        Min Service Interval:   0
        Max Service Interval:   0
        Inactivity Interval:    0
        Suspension Interval:    4294967295
        Service Start Time:     0
        Min Data Rate:          80000
        Mean Data Rate:         80000  bits per second
        Peak Data Rate:         80000
        Max Burst Size:         0
        Delay Bound:            0
        Min PHY Rate:           12000000  bits per second
        Surplus Bandwidth Allowance:1.2457
        Medium Time:            528  (units of 32 microsecond periods/second)
```

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 2-15.

Figure 2-15 QoS Profile Options

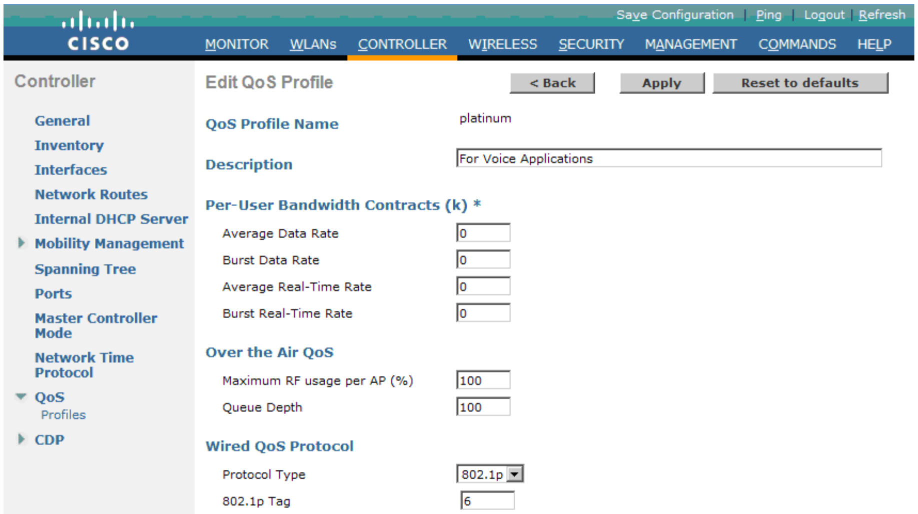


QoS Profiles

Profile Name	Description
bronze	For Background
gold	For Video Applications
platinum	For Voice Applications
silver	For Best Effort

Each of the profiles shown in Figure 2-16 allows the configuration of bandwidth contracts, RF usage control, and the maximum IEEE 802.1P classification allowed.

Figure 2-16 QoS Profile Settings



Edit QoS Profile

QoS Profile Name platinum

Description For Voice Applications

Per-User Bandwidth Contracts (k) *

Average Data Rate 0

Burst Data Rate 0

Average Real-Time Rate 0

Burst Real-Time Rate 0

Over the Air QoS

Maximum RF usage per AP (%) 100

Queue Depth 100

Wired QoS Protocol

Protocol Type 802.1p

802.1p Tag 6

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

For WLANs using a given profile, the IEEE 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 IEEE 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.

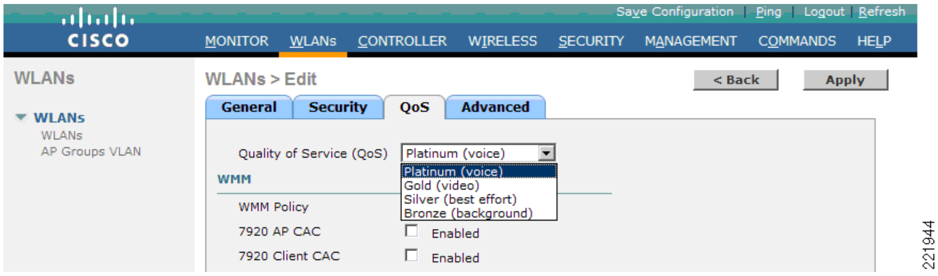
  The IEEE 802.1P classification sets the maximum CoS value that is admitted on a WLAN with that profile.

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 2-17. Each of the profiles (platinum, gold, silver, or bronze) is annotated with its typical use. In addition, a client can be assigned a QoS profile based on its 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 2-17 WLAN QoS Profile



WLANs > Edit

Quality of Service (QoS) Platinum (voice)

Platinum (voice)
Gold (video)
Silver (best effort)
Bronze (background)

WMM Policy

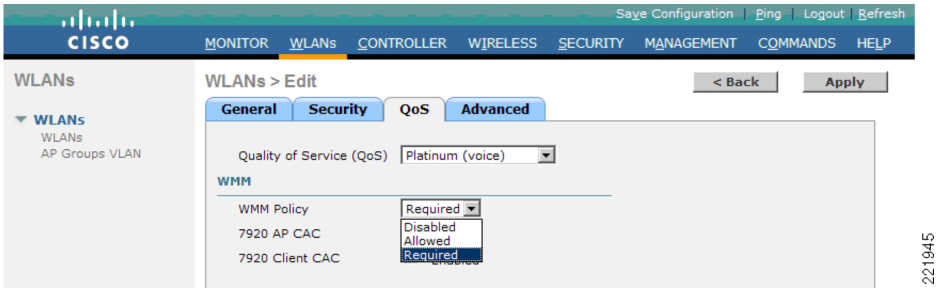
7920 AP CAC □ Enabled

7920 Client CAC □ Enabled

In addition to the QoS profiles, the WMM policy per WLAN can also be controlled, as shown in Figure 2-18. 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 2-18 WLAN WMM Policy



Quality of Service (QoS) Platinum (voice)

WMM Policy Required

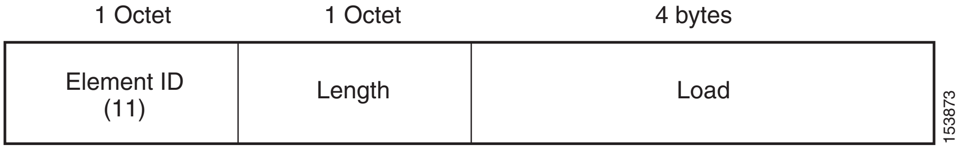
7920 AP CAC

7920 Client CAC

IP Phones

Figure 2-19 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 2-19 QBSS Information Element



1 Octet	1 Octet	4 bytes
Element ID (11)	Length	Load

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

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

The QBSS used depends on the WMM and Cisco Unified Wireless IP Phone 7920 settings on the WLAN.

Cisco Unified Wireless IP Phone 7920 support, shown in Figure 2-18, 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 Cisco Unified Wireless IP Phone 7920 and Cisco Unified Wireless IP Phone 7921G, use these advertised QoS parameters to determine the best AP with which to associate.

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

- Client CAC limit—The Cisco Unified Wireless IP Phone 7920 uses a call admission control setting that is set on the client. This supports legacy Cisco Unified Wireless IP Phone 7920 code-pre 2.01.
- AP CAC limit—The Cisco Unified Wireless IP Phone 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 (IEEE 802.11e standard) QBSS Load IE is sent out in the beacons and probe responses.

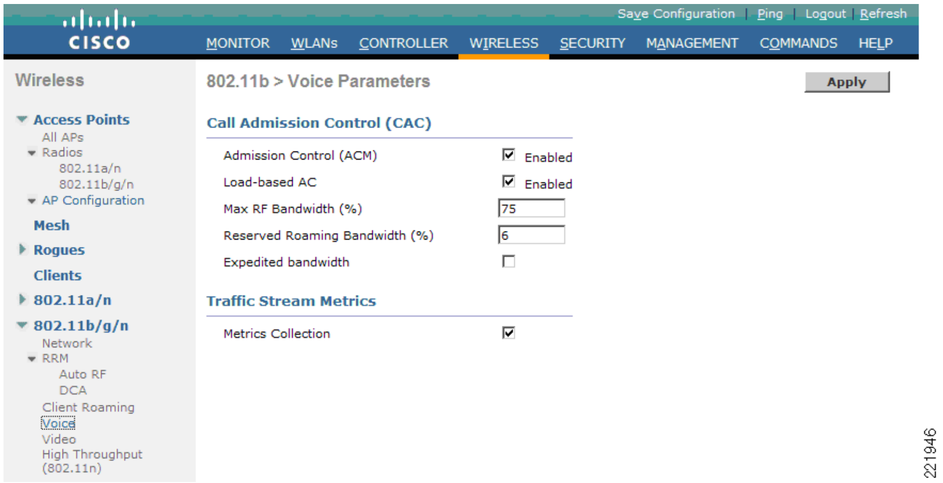
- If Cisco Unified Wireless IP Phone 7920 client CAC limit is to be supported, IE number 1 (the pre-standard QBSS IE) is sent out in the beacons and probe responses on the bg radios.
- If Cisco Unified Wireless IP Phone 7920 AP CAC limit is to be supported, the number 3 QBSS IE is sent in the beacons 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 2-20 shows a sample configuration screen for setting the voice parameters on the controller.

Figure 2-20 Voice Parameter Setting



802.11b > Voice Parameters

Call Admission Control (CAC)

Admission Control (ACM)	☑ Enabled
Load-based AC	☑ Enabled
Max RF Bandwidth (%)	75
Reserved Roaming Bandwidth (%)	6
Expedited bandwidth	☐

Traffic Stream Metrics

Metrics Collection	☑

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.

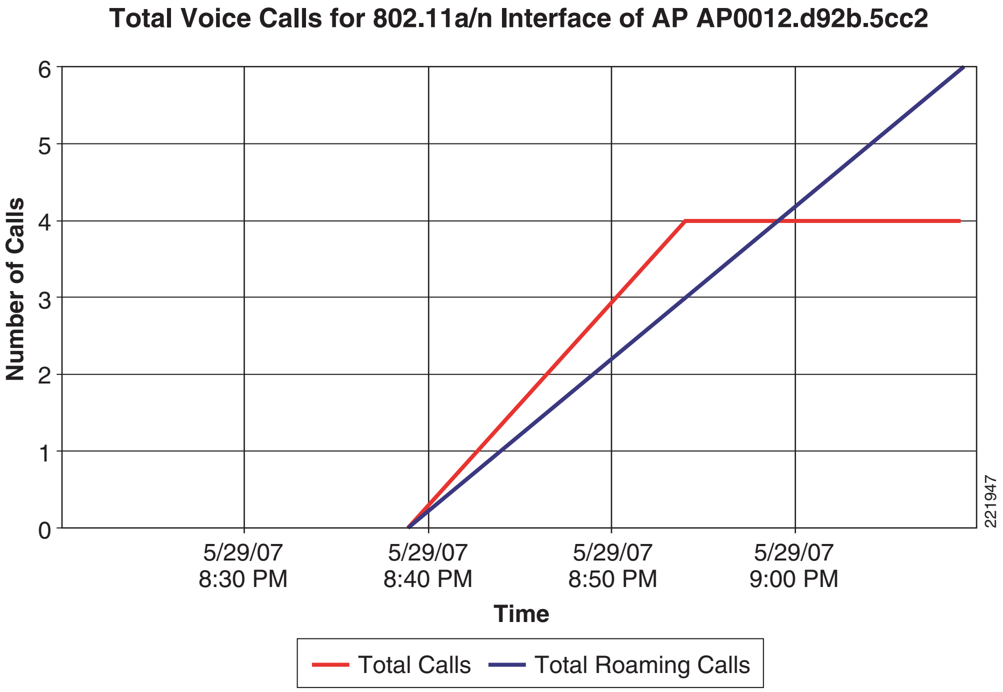
The reserved roaming bandwidth is how much capacity has been set aside to be able to respond to the ADDTS requests during association or re-association, which are VoWLAN clients with calls in progress that are trying to roam to that AP.

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 2-21 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 2-21 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 2-5 and Table 2-6 describe the impact on classification if access control is enabled and depending on whether a traffic stream has been established.

Table 2-5 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 2-6 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.

IEEE 802.11e, IEEE 802.1P, and DSCP Mapping

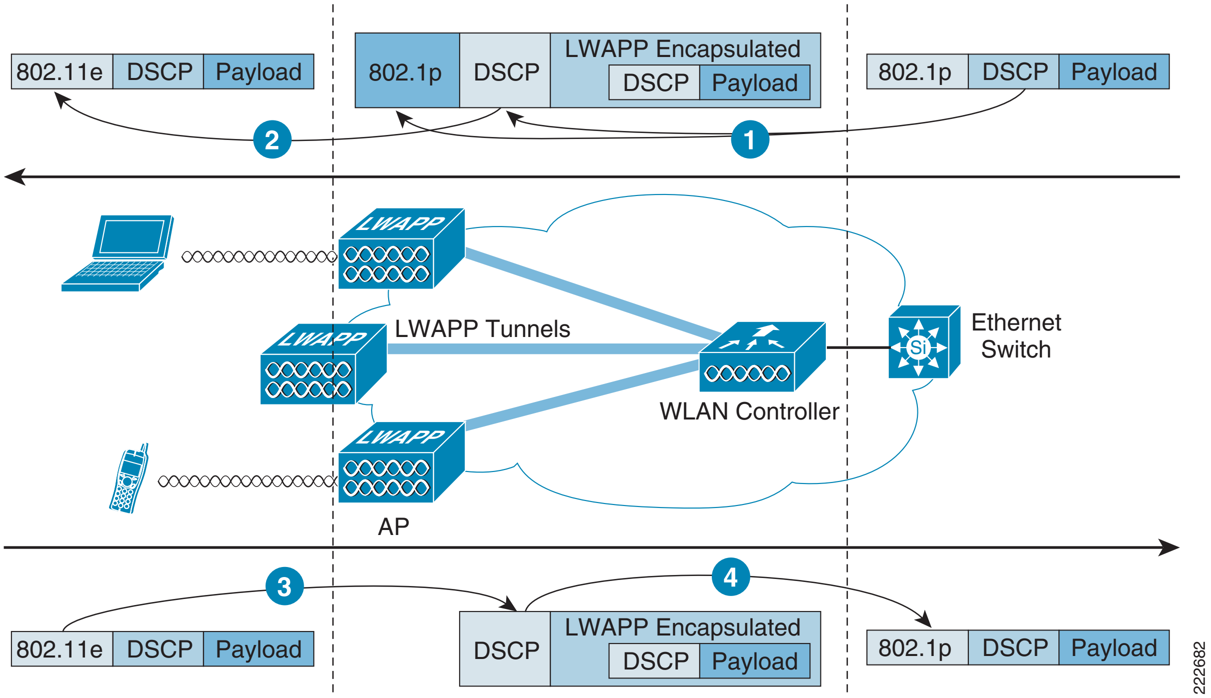
WLAN data in a Unified Wireless network is tunneled via LWAPP (IP UDP packets). To maintain the QoS classification that has been applied to WLAN frames, a process of mapping classifications to and from DSCP to CoS is required.

For example, when WMM classified traffic is sent by a WLAN client, it has an IEEE 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 2-22 shows a numbered example of the traffic classification flow for a WMM client, an AP, and a WLC.

Figure 2-22 WMM and IEEE 802.1P Relationship



In Figure 2-22, the following occurs:

Step 1 A frame with a 802.1p marking and a packet with an IP DSCP marking arrive at the WLC wired interface. The IP DSCP of the packet is used to determine the DSCP of the LWAPP packet leaving the WLC, and the 802.1p value of the frame depends on the QoS translation table (see Table 2-7), the QoS profile for the WLAN, and the Wired QoS Protocol configured for that QoS profile (Figure 2-16). If the Wired QoS Protocol is configured as "None", then no 802.1p value is set, but if the protocol is set to 802.1p, then the 802.1p used depends on the translation table capped at a maximum value of 802.1p table value shown in Figure 2-16.

Step 2 The IP DSCP of the LWAPP packet reaching the AP will translate to an 802.11e CoS marking based on Table 2-7.

Step 3 The 802.11e CoS marking of a frame arriving at the AP translates to an LWAPP DSCP value based on Table 2-7, capped at the maximum value for that QoS profile.

Step 4 The DSCP of the packet leaving the WLC will be equal to the DSCP of the packet that left the WLAN client, but the 802.1p value depends on the QoS translation table (Table 2-7), QoS profile for the WLAN, and the Wired QoS Protocol configured for that QoS profile (Figure 2-16). If the Wired QoS Protocol is configured as "None", then no 802.1p value is set, but if the protocol is set to 802.1p, then the 802.1p used depends on the translation table.

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 IEEE 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 Cisco Unified Wireless IP Phone 7920s 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 IEEE 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 2-7 are mapped to the appropriate QoS baseline DSCP values, rather than the IEEE values.

Table 2-7 Access Point QoS Translation Values

Access Point QoS Translation Values AVVID Traffic Type	AVVID IP DSCP	QoS Profile	AVVID 802.1p	IEEE 802.11e UP
Network control	56 (CS7)	Platinum	7	7
Inter-network control (CAPWAP control, 802.11 management)	48 (CS6)	Platinum	6	7
Voice	46 (EF)	Platinum	5	6
Interactive video	34 (AF41)	Gold	4	5
Streaming video	32 (CS4)	Gold	4	5
Mission critical	26 (AF31)	Gold	3	4
Call signaling	24 (CS3)	Gold	3	4
Transactional	18 (AF21)	Silver	2	3
Network management	16 (CS2)	Silver	2	3
Bulk data	10 (AF11)	Bronze	1	2

Table 2-7 Access Point QoS Translation Values (continued)

Best effort	0 (BE)	Silver	0	0
Scavenger	8 (CS1)	Bronze	0	1

In cases where the AP is translating CoS values, autonomous APs for example, the translation shown in Table 2-8 is used.

Table 2-8 WMM to AVVID Packet Re-Marking for APs when AVVID Priority Type Configured

Downstream L2 Packet Re-Marking[1]			Upstream L2 Packet Re-Marking		
Typical Application	**AVVID CoS**	**WMM UP**	**802.1d Designation**	**WMM UP**	**AVVID CoS**
Best Effort Data	0	0	BE	0	0
Medium Priority Data	1	2	BK	1	1
High Priority Data	2	3	-	2	1
Call Signaling	3	4	EE	3	2
Video Conferencing	4	5	CL	4	3
Voice Bearer	5	6	VI	5	4
Reserved	6	7	VO	6	5
Reserved	7	7	NC[2]	7	7

[1] In the downstream direction, the AP takes AVVID CoS markings on the wired interface and maps them to the UPs shown. In the upstream direction, the AP takes UPs received on the dot11 interface and maps them to AVVID CoS on the wired interface. Using this remapping results in the best match of WMM AC to AVVID CoS.

[2] The only network control traffic that should get mapped to CoS = 7 is spanning tree traffic that is used when WGBs are deployed or when outdoor bridges are deployed, connecting the LANs between 2 or more buildings. Even though 802.11 MAC management traffic is carried on UP=7 in autonomous APs, is it not bridged onto the wired port of the AP.

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 (IEEE 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 IEEE 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 IEEE 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.

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

Table 2-9 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 IEEE 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 IEEE 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 2-9 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 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 (to the AP and WLAN clients). 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 illustrates choosing to trust the CoS of settings of the WLC. 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, intending to have a more precise degree of control, might 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 IEEE 802.11 traffic directly. For WLANs that support WMM clients or Cisco Unified Wireless IP Phone 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 Unified Wireless IP Phone 7921G and 7920

The Cisco Unified Wireless IP Phone 7921G and the Cisco Unified Wireless IP Phone 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 implementation must 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—Refer to the following listing of whitepapers: http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/networking_solutions_white_papers_list.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

CHAPTER 3

Voice over WLAN Radio Frequency Design

The purpose of this chapter is to discuss, in general terms, the considerations in radio frequency (RF) planning and design for VoWLAN. Handset capabilities, local conditions, and regulations impose additional opportunities and constraints. This chapter illustrates the RF-related processes and considerations by presenting *typical* deployment scenarios.

General Voice AP Guidelines

The packet loss and jitter requirements of VoIP and the increased mobility of VoWLAN handset users place demands on connection quality, coverage, and user expectations that are beyond that a of a typical WLAN data deployment. While later generations of WLAN equipment and software might provide further VoWLAN improvements, RF planning, design, and implementation is the foundation of a successful VoWLAN deployment. A VoWLAN deployment without a solid RF foundation is the proverbial house built on sand. Correctly designing, planning, implementing, operating, and maintaining the WLAN RF environment is critical for a successful VoWLAN deployment. The processes, guides, heuristics, and tools used for a WLAN data deployment are unlikely to deliver a successful VoWLAN deployment. The general 7920 and 7921G VoWLAN guidelines are:

- The optimal VoWLAN network requires overlaps of 20 percent (2.4 GHz), and approximately 15 to 20 percent (5 GHz), where a WLAN Data design may use an AP cell overlap of 5 to 10 percent.
- The optimal VoWLAN cell boundary recommendation is -67 dBm

Note The RF characteristics of VoWLAN handsets do vary, and can greatly impact the WLAN design and capacity. If you are planning a deployment of a VoWLAN handset with RF deployment requirements that are at odds with those presented in this chapter, the handset guidelines should be followed. Although handset recommendations do vary, the general principles and issues discussed in this chapter still apply with some changes in cell sizes.

High Availability

One of the requirements of many systems—including VoWLAN—is for high availability (HA). In a VoWLAN deployment, the same HA strategies, as used in wired networks, can be applied to the wired components of the VoWLAN solution. One area unique to the VoWLAN availability is RF coverage HA—providing RF coverage that is not dependent upon a single WLAN radio. The primary mechanism for providing RF HA is *cell boundary overlap* as set out in the VoWLAN requirements. An overlap of 20 percent means that 80 percent of a given AP cell is also covered by other APs at the recommended signal levels, while in the other 20 percent of the cell VoWLAN calls may have degraded quality, but would still be available. The RF HA coverage is augmented by the Cisco Unified Wireless Network Coverage Hole algorithm which detects if WLAN clients are experiencing poor signal-to-noise ratio (SNR) values and causes the power of APs to increase as needed in order to rectify SNR issues.

Note In systems planning to rely on Coverage Hole algorithm, the planning needs to consider that if an AP is going to increase its power level to adjust for a hole, clients also need to increase their power to adjust for a hole. Therefore, the maximum power of the VoWLAN handset, which can be lower than the maximum power of an AP, needs to be considered in the AP power level used in the initial planning of the deployment. For example, if the VoWLAN handset has a maximum power of 40mW and the AP planning was based on an AP power of 40mW, increasing the AP power to cover an RF hole does not help a VoWLAN client in that hole. For the hole coverage to be effective, the RF planning needs to be based on an AP of 20mW or less.

Higher levels of overlap may be applied as required in order to increase the RF HA; however, increasing overlap requires that you consider the potential changes to your network operation due to the resulting increase in co-channel interference and the tuning of Auto-RF algorithms.

VoWLAN Call Capacity

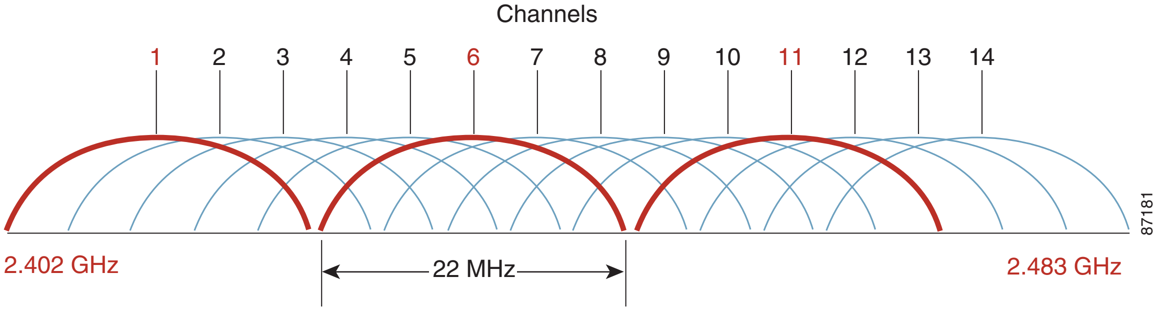
An important parameter in VoWLAN planning is *call capacity*—the number of simultaneous VoWLAN calls that can be supported in an area. This value can vary depending upon the RF environment, the VoWLAN handset features, and the WLAN system features. For example, the VoWLAN maximum capacity for a Cisco Unified IP Phone 7921G using a WLAN that provides optimized WLAN services (such as the Cisco Unified Wireless Network), the capacity is expected to be 14 simultaneous VoWLAN calls per 2.4 GHz channel and 20 simultaneous VoWLAN calls per 5 GHz channel. These capacity values are based on assuming no competing high priority WLAN traffic and *normal* background noise. Note that because the 5 GHz spectrum generally features less noise and interference, there can be greater capacity with the higher carrier frequency implementation. The additional non-overlapping channels available in the 5 GHz spectrum also provides a great deal more call capacity for a given area.

Note The call capacities are quoted per non-overlapping channel because the channel capacity is the limiting factor—not the number of access points (AP). This is explained in more detail in the following section. The purpose of providing these maximum call capacity figures is general planning purposes. The call capacity specified by the actual VoWLAN handset should be used for deployment since this is the supported capacity of that handset.

2.4 GHz Network Design

A total of 14 channels are defined in the IEEE 802.11b/g channel set. Each channel 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 U.S.), there are only three non-overlapping (and thus, non-interfering) channels: 1, 6, and 11—each with 25 MHz of separation. 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 non-overlapping channels. See Figure 3-1.

Figure 3-1 2.4GHz Channel Allocations



IEEE 802.11b provides rates of 1, 2, 5.5, and 11 Mbps. IEEE 802.11g provides data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps in the 2.4-GHz band, in the same spectrum as IEEE 802.11b. IEEE 802.11g is backward-compatible with IEEE 802.11b with a single AP providing WLAN access for both IEEE 802.11b and IEEE 802.11g clients.

Co-channel Interference Considerations

As mentioned in the preceding section, there are only three non-overlapping channels in U.S. 2.4 GHz spectrum. This presents a challenge when trying to deploy APs, and ensure that APs on the same channel cannot see the signal from an AP using the same channel. It is well known that the AP coverage radius changes with the client bit rates supported, and the boundary created by this RADIUS is often considered the AP's boundary.

The reality is somewhat more complicated because the AP influences the WLAN RF environment around it for a much greater distance than just the bit-rate boundary. This is because the RF energy from the AP, although too low to be demodulated in to a WLAN frame, is strong enough to cause an IEEE 802.11 radio to defer sending. In addition to the AP's influence of the RF environment, the clients associated with that AP extend the range of the RF energy associated with that AP's cell even further.

The IEEE 802.11 MAC is a Carrier Sense Multiple Access-Collision Avoidance (CSMA-CA) algorithm, and the Carrier Sense will perform a Clear Channel Assessment (CCA) before attempting to send an IEEE 802.11 Frame. If the CCA fails, it prevents the IEEE 802.11 radio to delay attempting transmission. The CCA mechanism is specified for each IEEE 802.11 physical layer; it is typically triggered either by a simple raw energy level, and physical layer convergence protocol (PLCP) header power levels, or carrier detection. The CCA of an IEEE 802.11 radio does not vary with the bit rates being used and is not, generally, user-configurable.

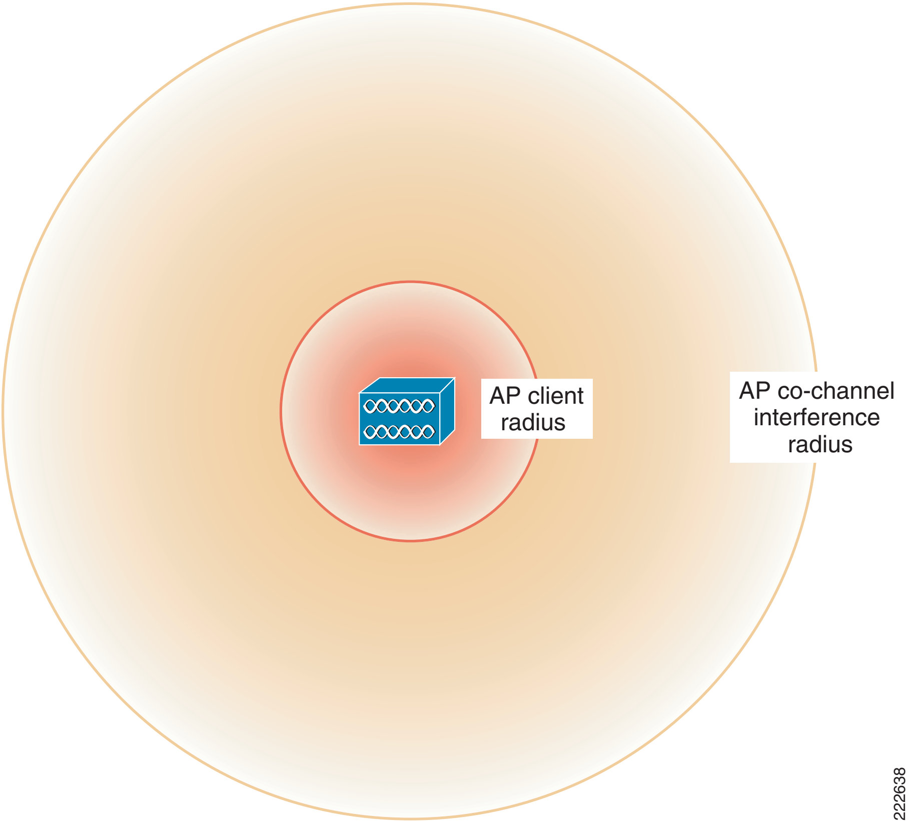
The impact of CCA deferrals on an AP WLAN from IEEE 802.11 radios that are not part of that AP WLAN is called *co-channel interference*. As co-channel interference results in delays in sending frames, it causes increased jitter and delay experienced by VoWLAN calls. Although WLAN QoS prioritizes WLAN traffic, this occurs after the CCA and therefore prioritization does not overcome the jitter and delay introduced by CCA.

The guidance for the Cisco Unified IP Phone 7921G VoWLAN handset is for a power level boundary of -67 dBm, and a separation between adjacent AP channels of -86 dBm. The -67 dBm requirement is to minimize packet loss, and the -86 dBm requirement is to minimize co-channel interference from other AP cells on the same channel. Figure 3-2 shows an example of the two boundaries created by the -67 dBm and -86 dBm requirements, based on standard RF loss formulas for an open office environment. This RF environment that would give an AP a client radius of 43 feet gives an AP co-channel interference radius of 150 feet using standard antenna gain (2 dB) and an AP output power of 16 dBm (40mW). Different RF environments, AP powers, and antennas will result in different client and co-channel interference radii, but the principles discussed in this chapter will generally hold.

Note The recommended cell boundary for the *Vocera* badge is at -65 dBm and therefore would yield slightly different results from those below.

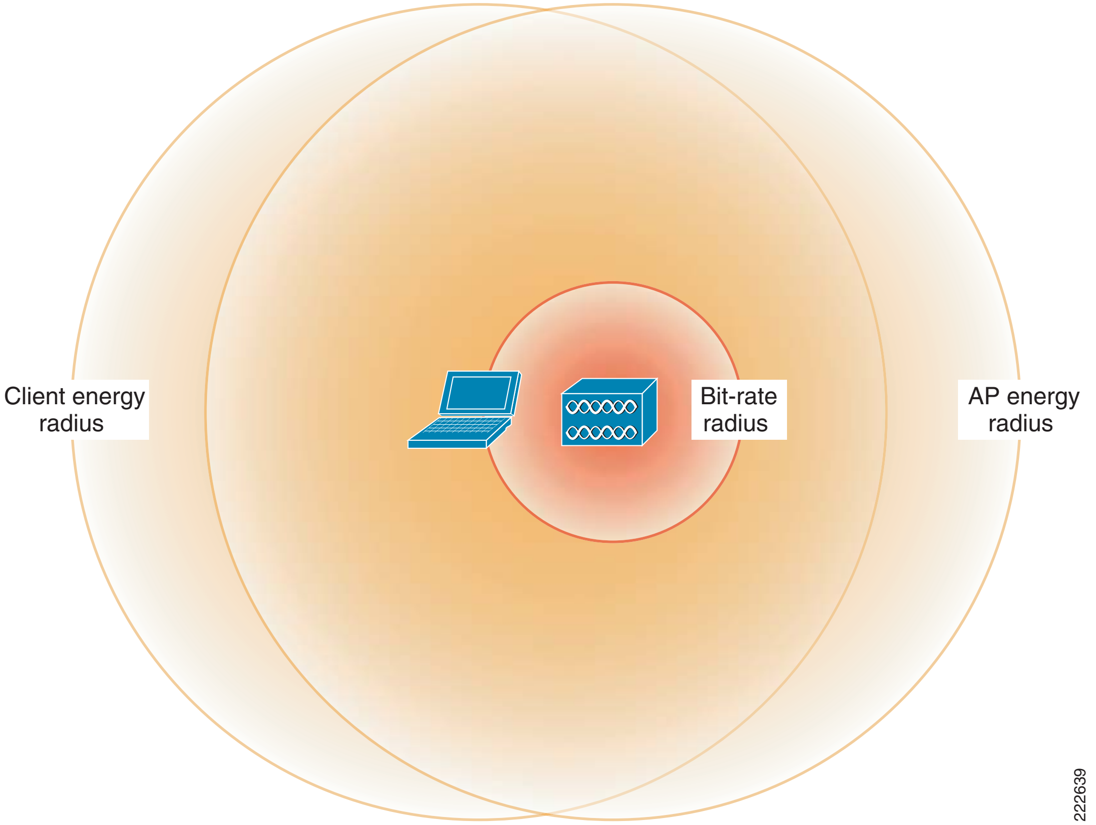
Note The output power chosen for the AP must align with the VoWLAN handset capabilities and deployment requirements. For example the Cisco Unified Wireless IP Phone 7921G has a maximum output power of 40 mW. An AP power greater than 40 mW should not be used for a Cisco Unified Wireless IP Phone 7921G deployment. In circumstances where the Cisco Unified Wireless Network Hole Coverage mechanism is expected to provide VoWLAN coverage in event of an AP outage, an AP power of less than 40 mW (using the Cisco Unified Wireless IP Phone 7921G as an example) should be used for AP planning to allow the APs covering an RF hole to be operating in a range suitable for the VoWLAN handset. One additional advantage of using a lower AP transmit power is a proportional decrease in the co-channel interference radii. Our example of 40 mW transmit power gives a co-channel radius of the 150 feet and a client radius of 43 feet. Decreasing the power to 20 mW reduces the co-channel radius to 130 feet and the client radius to 38 feet, and also reduces the co-channel interference proportional to the co-channel interference generated by an AP.

Figure 3-2 Bit Rate and Co-channel Interference Boundaries of an AP



The RF co-channel interference radius of an AP is not the whole picture because a WLAN client is just as capable as an AP of producing co-channel interference as illustrated in Figure 3-3.

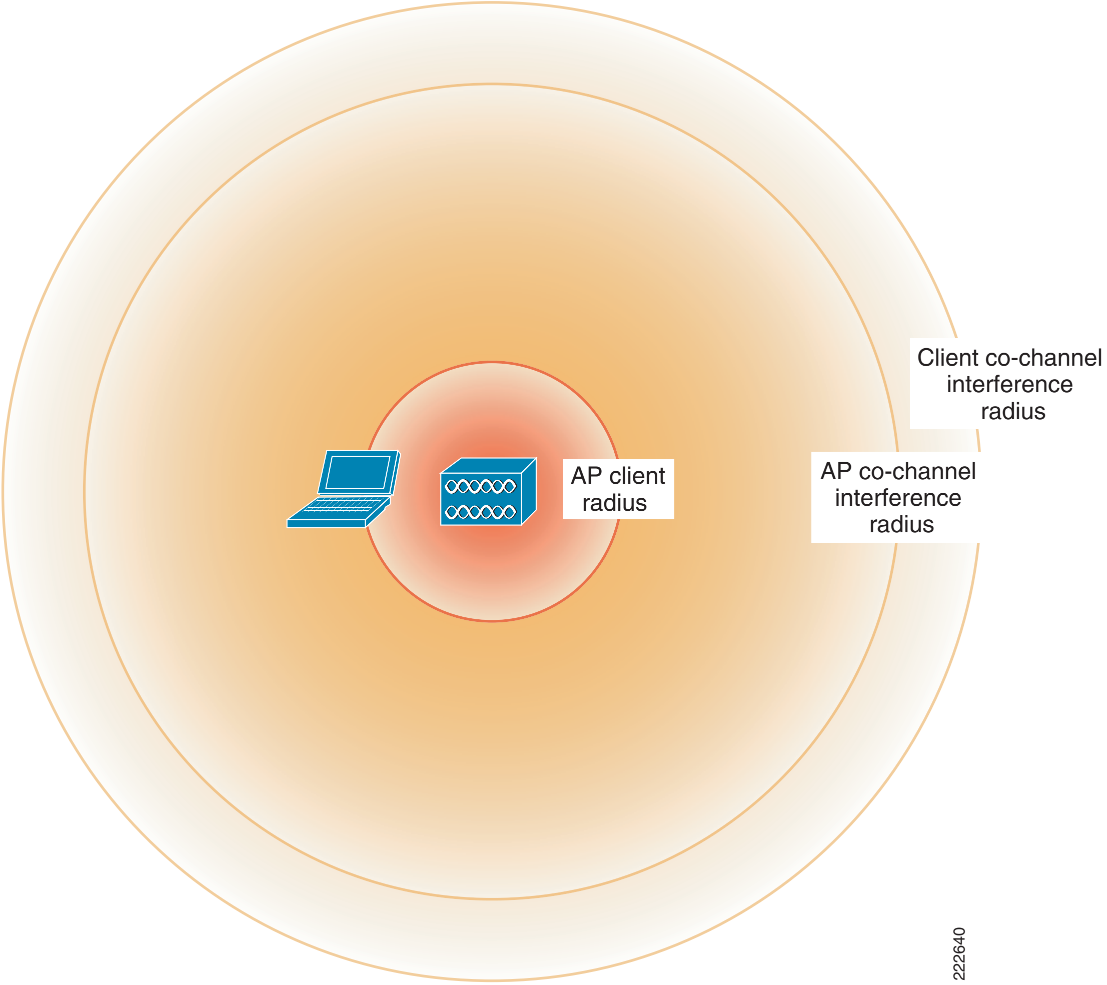
Figure 3-3 Single Client Co-channel Interference Radius



Given that a client or clients might be anywhere on the bit-rate radius perimeter, the client co-channel interference radius is better illustrated by Figure 3-4. Given the 43 foot bit-rate radius and 150 foot AP co-channel interference radius of the previous calculations the new client co-channel interference radius is 193 feet.

Note The 193 feet would represent close to a worst case because the WLAN client is not normally in an equivalent location to an AP and would likely suffer greater signal attenuation due to obstacles.

Figure 3-4 Complete Client Co-channel Interference Radius


Client co-channel interference radius
AP client radius
AP co-channel interference radius
222640

Bit Rate Impact on Co-channel Interference

The AP client radius in our example results in a nominal bit rate for the Cisco Unified IP Wireless IP Phone 7921G of approximately 24 Mbps or greater, depending upon noise. The AP client radius can be extended further by decreasing by supporting lower bit rates. This is not recommended for the following reasons:

- Lowering the bit rate extends the AP client radius, but also increases the client co-channel interference radius, increasing the area that only has the VoWLAN call capacity of a single AP.
- The lower bit rates reduce the overall call cell capacity, as lower bit rate packets consume more time, and transmit less packets.

VoWLAN call quality is sensitive to data-rate shifting. The decision to a data-rate shift is normally the result of being unable to send at the date rate previously used which is determined by sending multiple times without receiving an acknowledgement for that frame. This increases the delay and jitter experienced by a VoWLAN call.

20 Percent Cell Overlap

The recommended AP cell overlap for VoWLAN deployments at 2.4GHz, is 20 percent. The purpose of the 20 percent overlap is to ensure that a VoWLAN handset can detect and connect to alternative APs, when it is close to the cell boundary. This should allow a VoWLAN client to change AP associations with a minimum of interruption to a call, by minimizing the amount of data rate shifting and retransmission at a cell boundary for a given VoWLAN client. This 20 percent overlap requirement means that APs are spaced closer together than the two-times-70 feet distance suggested by the cell boundary. The area of overlap between two circles of radius equals 1 is given by:

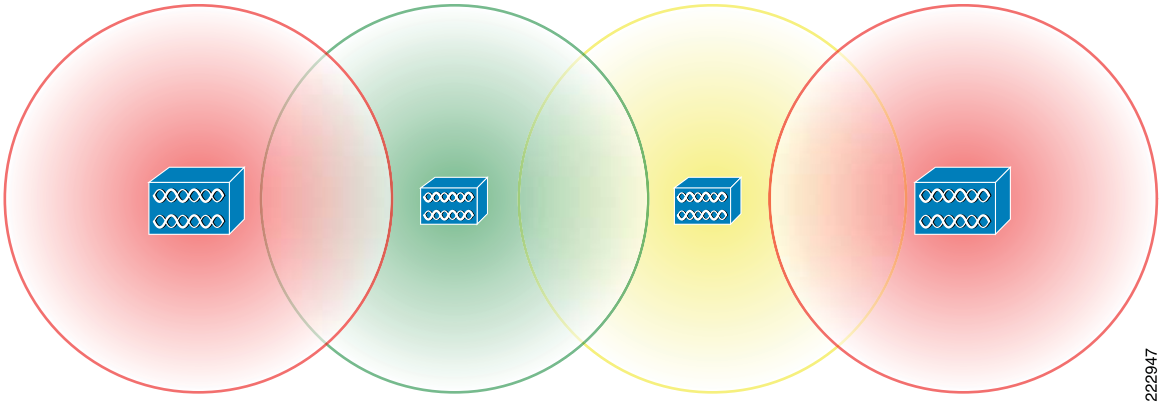
This calculation is taken from http://mathworld.wolfram.com/Circle-CircleIntersection.html

In this equation, *d* is the distance between the centers of each circle. Solving for an area of 20 percent gives a *d* value of 1.374 for a standard radius of 1, or 59 feet between APs for our 67 dBm boundary.

Note Other common *d* values are 10 percent (1.611), 15 percent (1.486), 25 percent (1.269), and 30 percent (1.198)

Figure 3-5 illustrates this AP overlap, where the colors, red, green, and yellow represent channels 1, 6, and 11 respectively.

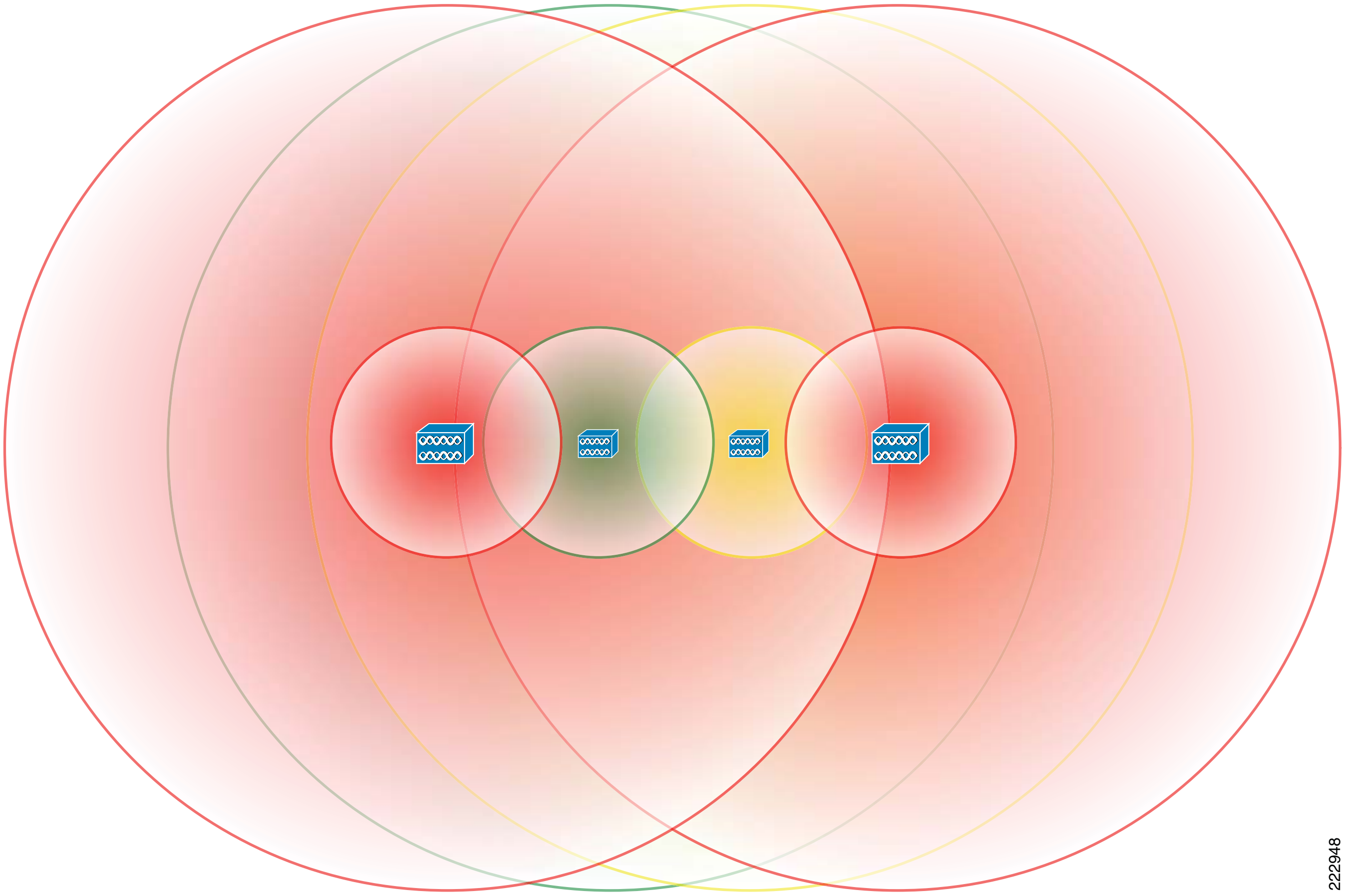
Figure 3-5 APs with 20 Percent Overlap



Co-channel Interference and 20 Percent AP Cell Overlap

Figure 3-6 shows the APs with 20 percent overlap and their co-channel interference boundaries. The co-channel interference boundary for one of the APs using channel 1 (red) overlaps with an AP using the same channel. In this situation, co-channel interference will occur in a 2.4 GHz VoWLAN deployment.

Figure 3-6 AP with 20 Percent Overlap and Co-channel Interference Boundaries



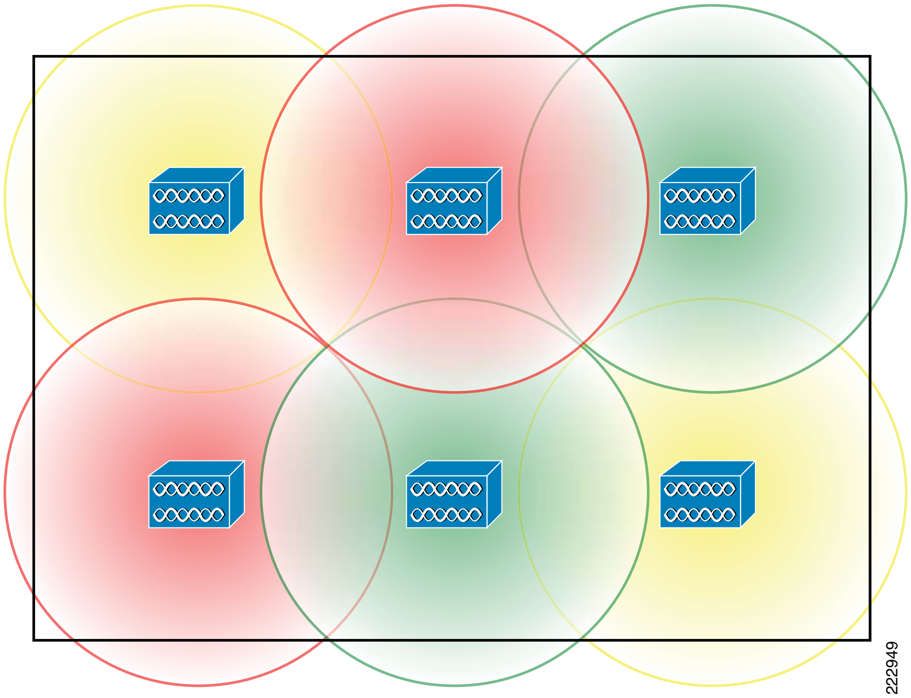
It should be noted that the combined effect of the 20 percent overlap requirement for reliable roaming between AP cells and the impact of co-channel interference is a reduced per VoWLAN call capacity over a given area.

Note It is not an effective strategy to reduce the overlap in order to reduce co-channel interference. As users satisfaction can be greatly affected by poor roaming performance. In contrast, call capacity can be addressed in planning and design.

Existing WLAN data deployments (initially using lower-power cell-boundaries and less overlap) that are changed to match recommended power boundaries and overlap for VoWLAN or Location might experience application issues for timing-sensitive applications. It is difficult to predict which applications might be affected by the WLAN changes, because the actual effect depends on the application implementation. Generally, custom applications (requiring keepalive timeouts) are most likely to be affected and should be validated in the new environment to ensure that their timers require no adjustment.

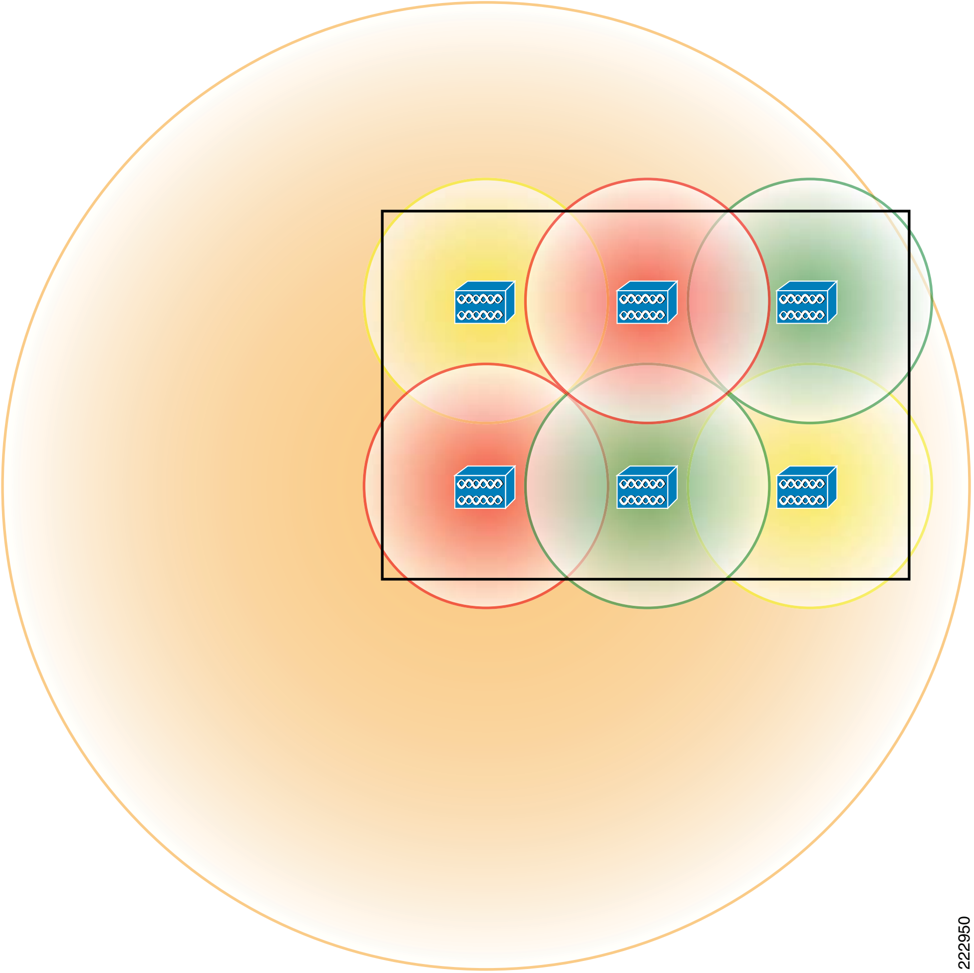
For the sake of comparison, a WLAN data deployment is illustrated in Figure 3-7. This example features an AP client radius of 110 feet, -a 75 dBm client power boundary-, and a 10 percent overlap. The increased client radius and reduced overlap is possible because WLAN data clients are generally more tolerant of packet loss and jitter.

Figure 3-7 WLAN Data Single Floor Data Example



Note The co-channel radius is larger for the WLAN Data example. See Figure 3-8. The energy detect levels are the same, but the AP client radius 67 feet larger. This means that the capacity of the single floor will still be the equivalent of three channels, even though 6 APs are used.

Figure 3-8 Single Floor WLAN Data with Co-channel Radius



Example Deployments

The AP layout within a building depends greatly upon the building construction and shape, as well as the WLAN coverage requirements in that building. Due to differing effects of implementation-specific variables, there is not a single recommended deployment for the number of APs that should be deployed nor a single solution for determining the effect of co-channel interference. Therefore, we illustrate the design process with examples to illustrate deployment options. In the subsequent descriptions, we focus upon the following examples:

- Example Single Floor Building Deployment
- Example Multi-Floor Building

Example Single Floor Building Deployment

Figure 3-9 shows a simple rectangular building example, based upon a standard size building floor at the Cisco San Jose Campus (285 feet x 185 feet). As we can see from Figure 3-9, 20 APs are required to give complete coverage. A WLAN data deployment with the same AP boundary and plan may have been able to use only 15 APs, as shown in Figure 3-10, but this has small coverage gaps. One of the characteristics of VoWLAN deployments is that users are more mobile and find coverage gaps that were not found by WLAN data clients. As a result, a 20 AP deployment is needed. A detail that has not been shown in Figure 3-9 and Figure 3-10 is the location of building exits. It is critical to have coverage around the building exits, if not between buildings. Employees will step outside for many reasons and expect VoWLAN calls to be maintained. One of the issues of Figure 3-10 is that the coverage gaps would occur at building exits.

Figure 3-9 Single Floor Deployment with 20 APs

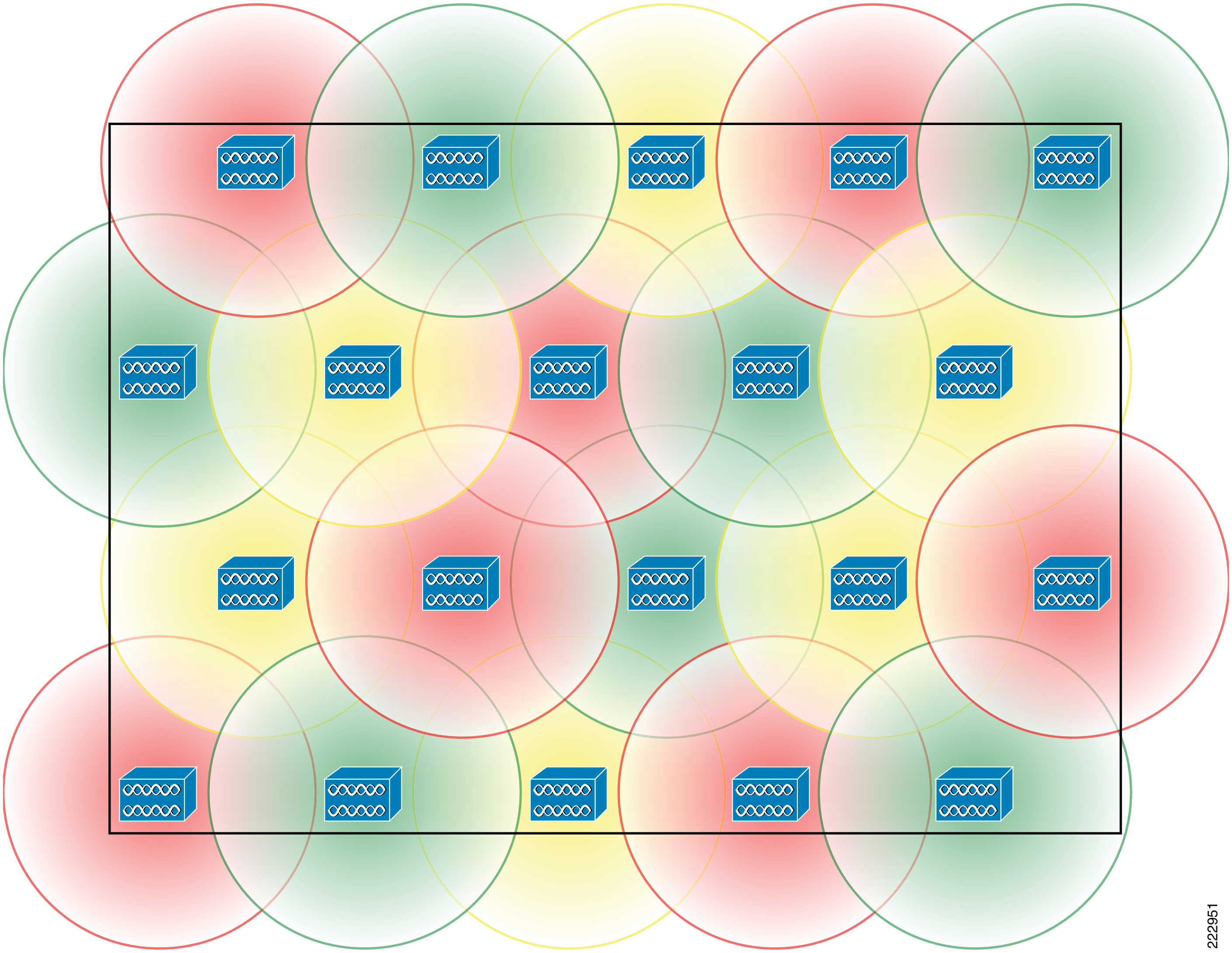


Figure 3-10 Single Floor Deployment with 15 APs

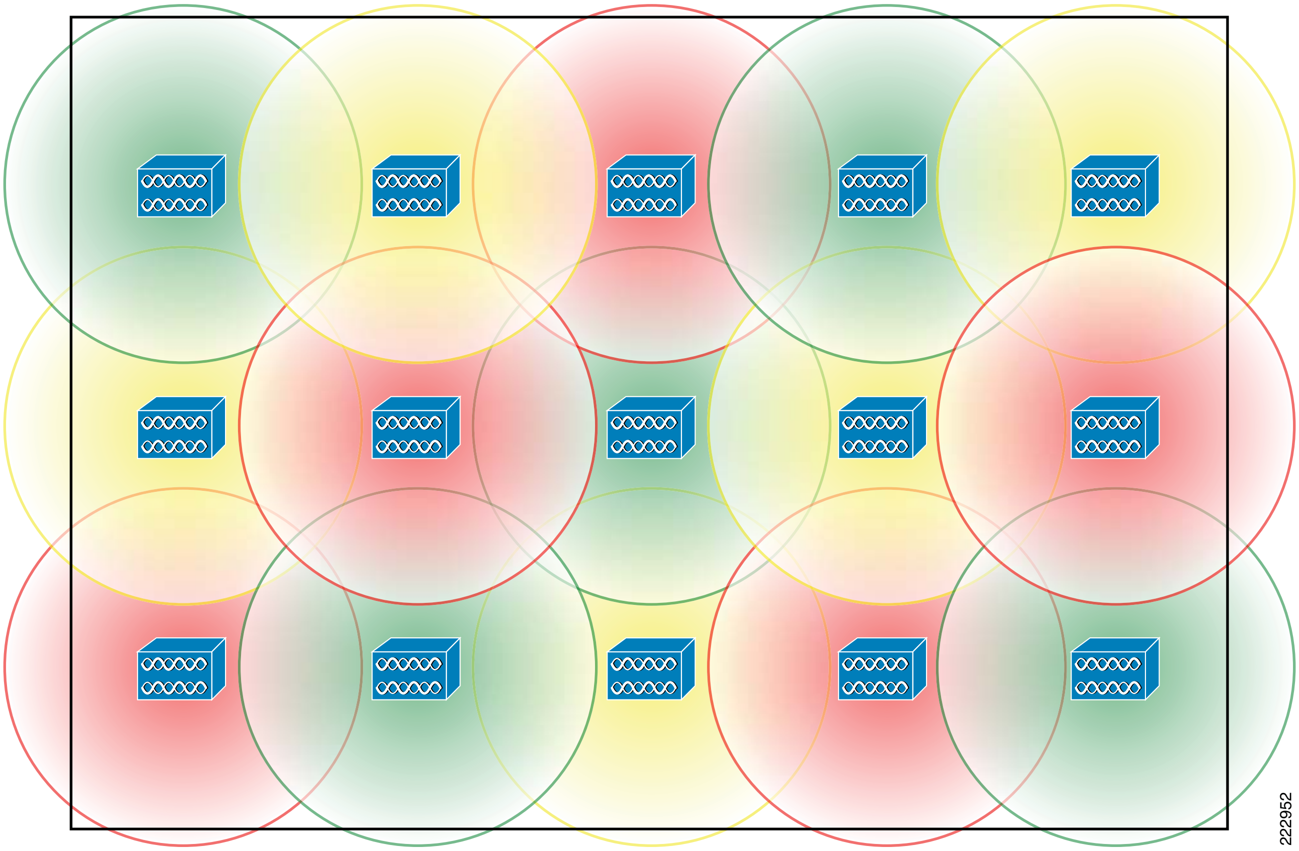
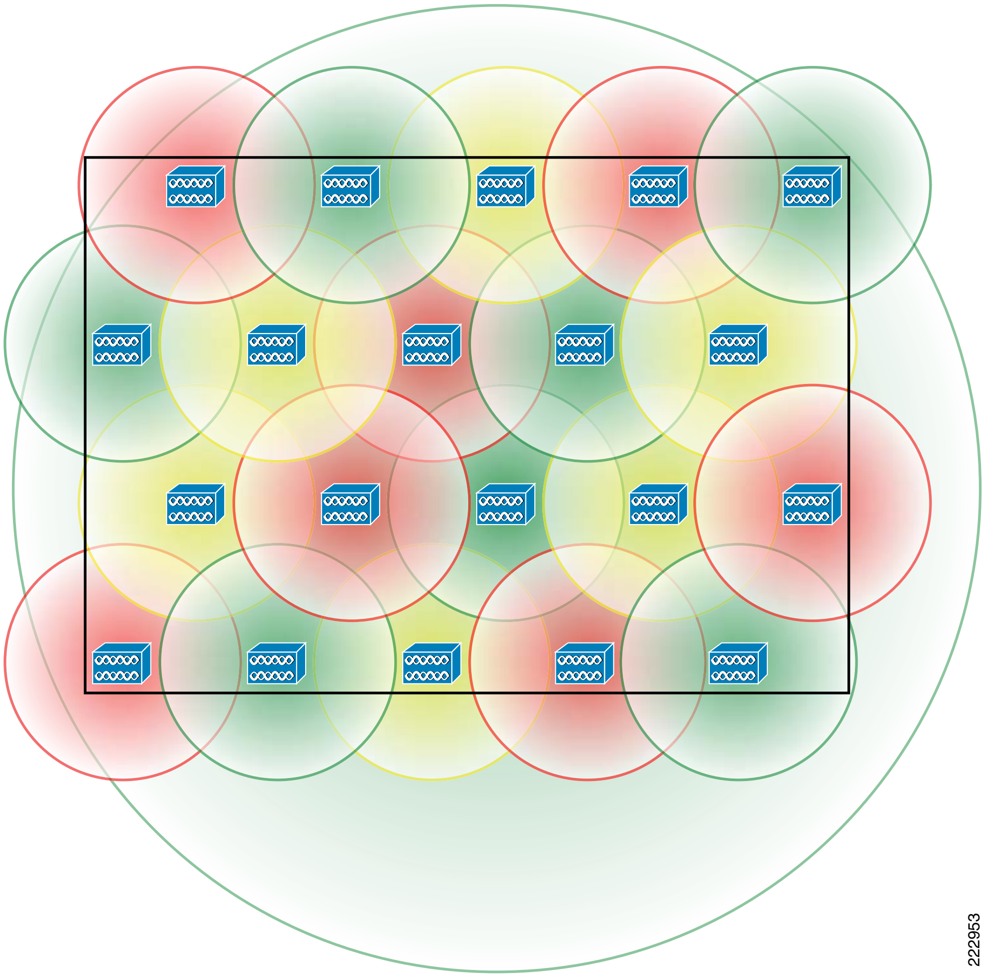


Figure 3-11 shows the co-channel interference radius of an example AP. As can be seen from the figure, the co-channel interference radius extends for the entire building. This means that the APs using channel 1 (red) are effectively sharing some channel capacity. The seven channel 1 APs have increased the coverage over single AP by seven times, but has not increased the capacity by the same ratio and might not increase the capacity significantly in comparison with single AP. The same is true for the APs on other channels. Due to co-channel interference the call capacity of the floor is equivalent to something above the capacity of 3 independent APs, but not approaching the capacity of 20 APs. This is the primary reason for addressing VoWLAN call capacity in terms on the number of calls per channel, rather than the number of calls per AP. Channel capacity is the limiting factor.

Figure 3-11 Single Floor Co-channel Interference

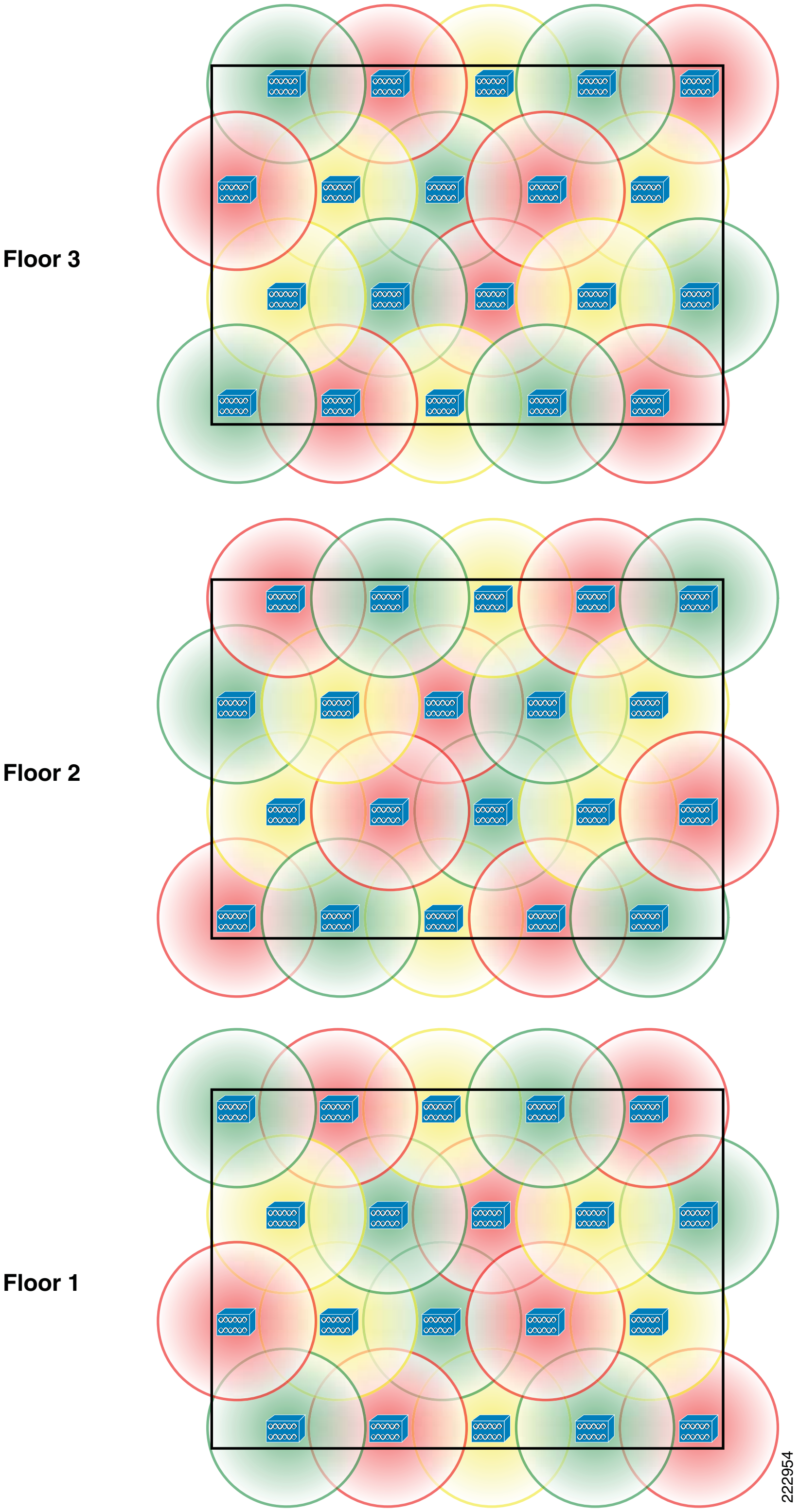


Example Multi-Floor Building

In a multi-floor building, RF energy can travel between floors and, as part of RF planning, the channels are staggered from floor-to-floor to minimize the co-channel interference between floors, as show in Figure 3-12.

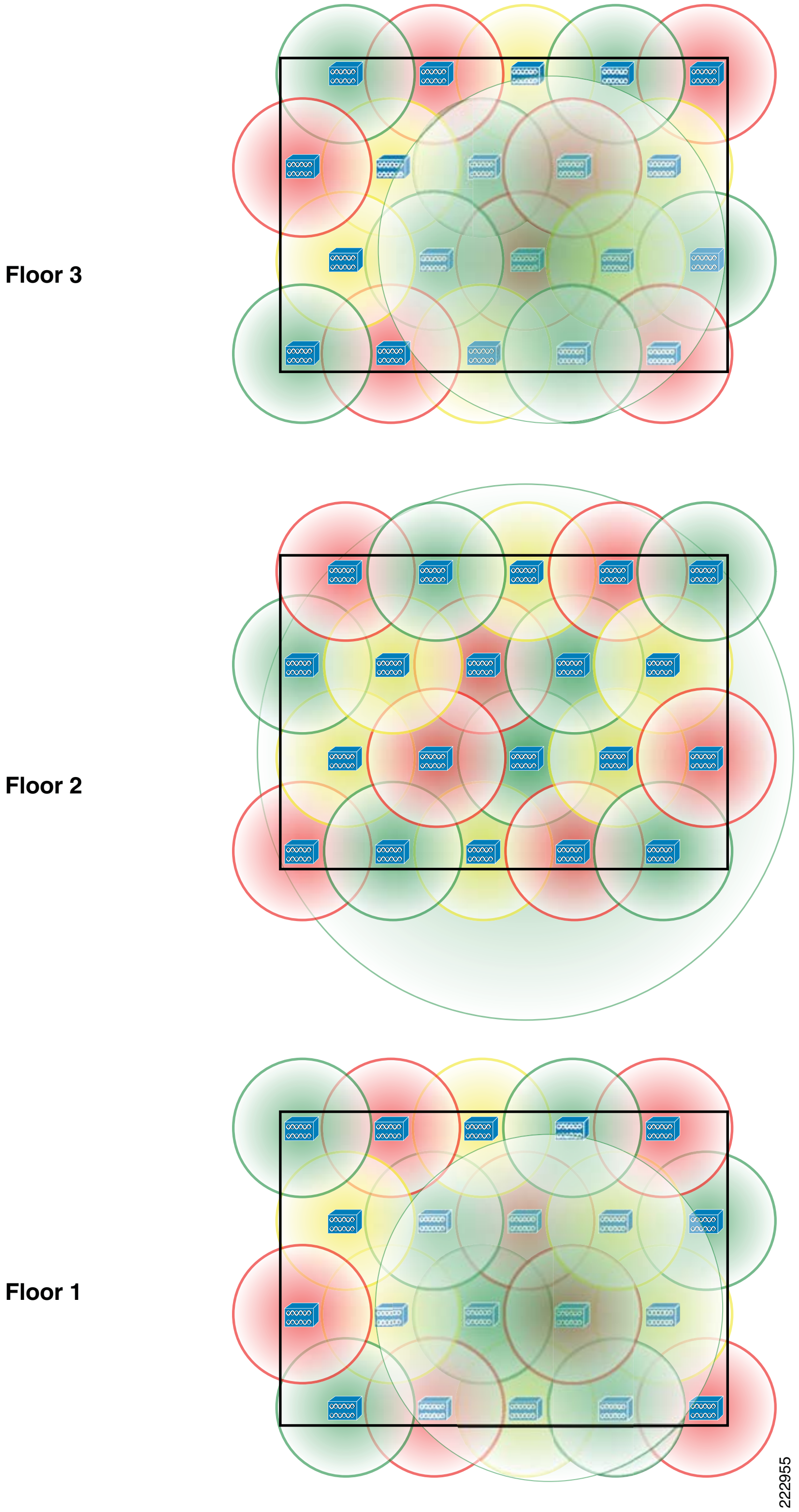
Note Figure 3-12 and Figure 3-13 do not represent a recommended channel implementation and are provided only to illustrate this description.

Figure 3-12 Multi-floor Channel Assignments



As the signal path between the floors is different from that on the same floor (there is often a piece of reinforced concrete in the between floor path), this must be taken into account when considering the co-channel interference radius of an AP. If we use a typical between floor loss of 7 dB, the co-channel interference radius of an AP between floors is reduced to 120 feet. Figure 3-13 shows an example of the co-channel interference radius of APs on different floors. Where floor 2 is the same layout as our single floor example earlier, and floor 1 and floor 3 shows the co-channel interference radius on the floors above and below. As can be seen from Figure 3-13, the co-channel interference between floors is still significant and it is reasonable to assume that the capacity across the three floors may be the equivalent of six or seven APs, but is not close to that of the 60 APs that have been deployed.

Figure 3-13 Multi-floor Building Showing Co-channel Interference



Location-based Services Design Considerations

The signal level requirements of IEEE 802.11 location-based services are similar to those on VoWLAN, but the AP placement requirements are different. For example, our AP placements shown in Figure 3-9 illustrate APs positioned close to what would be required in a Location-based Service (LBS) deployment. In this environment, there are many APs deployed on the perimeter—as well as at the core of the building. An additional column of APs (four) might be required. The VoWLAN AP count and the Location AP count may not always be this similar. The AP placement requirements of LBS may result in the addition of more APs—depending on the shape and size of the building. The addition of more APs for LBS will introduce an additional level of co-channel interference due to the additional IEEE 802.11 management traffic associated with additional AP; however, given the existing co-channel interference, the difference is not likely to be significant. The key point, as with the VoWLAN deployment, is that the addition of extra APs does not contribute to additional capacity in the 2.4GHz band due to co-channel interference.

The Importance of Auto-RF

As developed in the preceding sections, the VoWLAN call capacity is constrained by the effect of co-channel interference in the 2.4GHz band. This constraint should be considered in the planning, design and operation of the VoWLAN network. In our examples we determined that the call capacity of our deployment is the equivalent of three times the capacity of a single AP. These estimates assume that Auto-RF in being used, and that an AP will change channels to minimize interference and provide an optimal channel plan. Unfortunately, there is only so much Auto-RF can do to address the effects of co-channel interference in the 2.4 GHz channel because the limiting factor in the 2.4 GHz band is the three, non-overlapping channels. Auto-RF can tune AP power levels that might reduce co-channel interference by reducing power levels, but this power level adjustment must be balanced against the signal-level and coverage requirements of the VoWLAN deployment. Auto-RF is discussed further in a subsequent chapter of this document. The best mechanism to achieve greater capacity and a greater return on the investment of deployed APs is to use the 5 GHz band of IEEE 802.11a.

5 GHz Network Design

This section describes the following considerations for implementing a 5 GHz VoWLAN deployment:

- IEEE 802.11a Physical Layer, page 3-17
- IEEE 802.11a Channels, page 3-18
- IEEE 802.11a Operating Frequencies and Data Rates, page 3-18
- IEEE 802.11a and VoWLAN Deployments, page 3-19

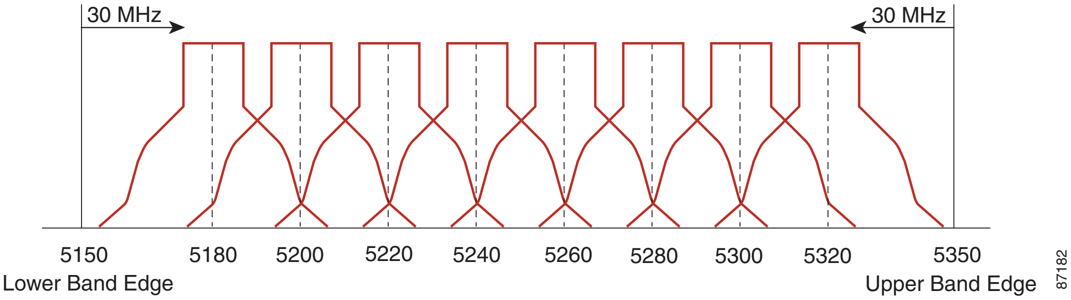
IEEE 802.11a Physical Layer

IEEE 802.11a defines requirements for the physical layer (of the OSI model), operating in the 5 GHz UNII frequency band, with data rates ranging from 6 Mbps to 54 Mbps. It uses Orthogonal Frequency Division Multiplexing (OFDM), which is a multi-carrier system (52 sub-carriers are used, modulated with BPSK, QPSK, QAM or 64-QAM to provide different data rates). OFDM allows sub-carrier channels to overlap, providing a high spectral efficiency. The modulation technique used by OFDM is more efficient than spread spectrum techniques used with IEEE 802.11b; it is the same as is used in 802.11g.

IEEE 802.11a Channels

The basic IEEE 802.11a channels are shown in Figure 3-14. This shows the center frequency of the channels. The spectrum of each channel is 10 MHz on either side of the dotted line (20 MHz total), with 5 MHz of separation between channels spectrum.

Figure 3-14 5 GHz Channel Set



For the U.S.-based IEEE 802.11a standard, the 5 GHz unlicensed band covers 300 MHz of spectrum and supports 23 channels. As a result, the 5 GHz band is actually a conglomeration of three bands in the U.S.: 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).

IEEE 802.11a Operating Frequencies and Data Rates

Operating in the unlicensed portion of the 5 GHz radio band, IEEE 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 IEEE 802.11a standard operates in a different frequency range, it is not compatible with existing IEEE 802.11b or IEEE 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.

IEEE 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 compared to 2.4GHz network, for a given power and gain. However it has up to 23 non-overlapping frequency channels (depending on the geographic area) as compared to the three non-overlapping channels for the 2.4GHz band, which 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 IEEE 802.11a operates is divided into several sub-bands. Each of the Unlicensed National Information Infrastructure (UNII) bands presented in Table 3-1 were originally intended for different uses, but all can now be used for indoor IEEE 802.11a deployments with applicable power restrictions. Originally, the FCC defined what is known as the UNII-1, UNII-2, and UNII-3 bands, each consisting of four channels. The channels are spaced 20 MHz apart with an RF spectrum bandwidth of 20 MHz, thereby providing four non-overlapping channels.

Table 3-1 Operating Frequency Range for IEEE 802.11a

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

There are different limitations imposed on each of the UNII bands. Depending on the band, restrictions include transmit power, antenna gain, antenna styles, and usage. The UNII-1 band is designated for indoor operation, and initially required devices to use permanently attached antennas. The UNII-2 band was designated for indoor or outdoor operation, and permitted the use of external antennas. The UNII-3 band, originally intended for outdoor bridge products that use external antennas, can now be used for indoor or outdoor IEEE 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, 140 and 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. Table 3-1 shows the various channels in the UNII-1, -2, and -3 bands, along with the additional 11 new channels.

Note The 1100 AP does not have an 802.11A radio and the 1000 series AP does not support DFS channels.

IEEE 802.11a and VoWLAN Deployments

Although there are 23 non-overlapping channels in the 5 GHz band, it is generally recommended to use the lower four channels and upper four channels of the 5 GHz spectrum as the base for VoWLAN, as they do not have a DFS and TPC requirements. Then add to the base of eight channels by determining which other channels are unlikely to be affected by DFS and TPC. The timing requirements of DFS and

TPC can adversely affect VoWLAN call quality. If your region or location is such that you are certain DFS and TPC will not be triggered, then the use of specific channels should not be an issue. If you are not certain, you should investigate. The Cisco Spectrum Expert analyzer is a good tool for starting this assessment to determine whether there are any 5 GHz signals in the area that would trigger DFS and TCP. Note that these channels must also be supported by the WLAN clients (data and VoWLAN). It is simpler to stay with the eight non-DFS channels, but every additional channel that can be safely deployed increases the capacity of the design. In addition to avoiding the DFS and TPC channels, it is also recommended that adjacent channels be avoided in the AP channel lay out—to avoid interference from the sidebands in each channel. The channel spacing and channel mask characteristics are such that the sidebands produced by an IEEE 802.11a client might interfere with the adjacent channels. It is best to avoid this potential issue in the AP layout. The general power levels and AP separation recommendations use in this guide for VoWLAN in the 5 GHz implementation are the same as the 2.4 GHz implementation: a power level boundary of ~67 dBm and a separation between adjacent AP channels of -86 dBm. Given the lower noise floor in the 5 GHz bands, the overlap recommendation may be reduced to 15 percent. A 20 percent or higher overlap can still be used if desired. It provides a higher availability design and takes into account that the use of the 5GHz spectrum is increasing; therefore, the noise floor can be expected to rise.

The range in the 5 GHz band is different to that in the 2.4 GHz band. However, when using the recommended power levels and typical antennas in our example, we obtained distances similar to those used in the 2.4 GHz example. Therefore, the same AP locations and overlap have been used for both the 2.4 GHz and 5 GHz bands. The primary difference between the two deployments is the additional capacity available due to the additional non-overlapping channels. This difference is sufficient for the 5 GHz band to be recommended for VoWLAN deployments.

Note The TPC mechanism discussed above is different from the TPC algorithm that is part of Auto-RF.

An Example Single Floor Building

Figure 3-15. shows an AP layout using the eight different channels and designed to maximize the distance between re-used channels. However, in most cases, more channels should be available. Because the 2.4GHz and 5 GHz AP client radius and co-channel interference radii are fundamentally the same in this example, the multiple floor examples need not be repeated here. The major difference between the two bands is the increase in capacity that is made available by the added channels associated with the 5 GHz band. The more channels that can be found for use in the 5 GHz band, the closer the capacity of the system can correlate to the number of APs deployed.

Figure 3-15 5 GHz Single Floor Layout

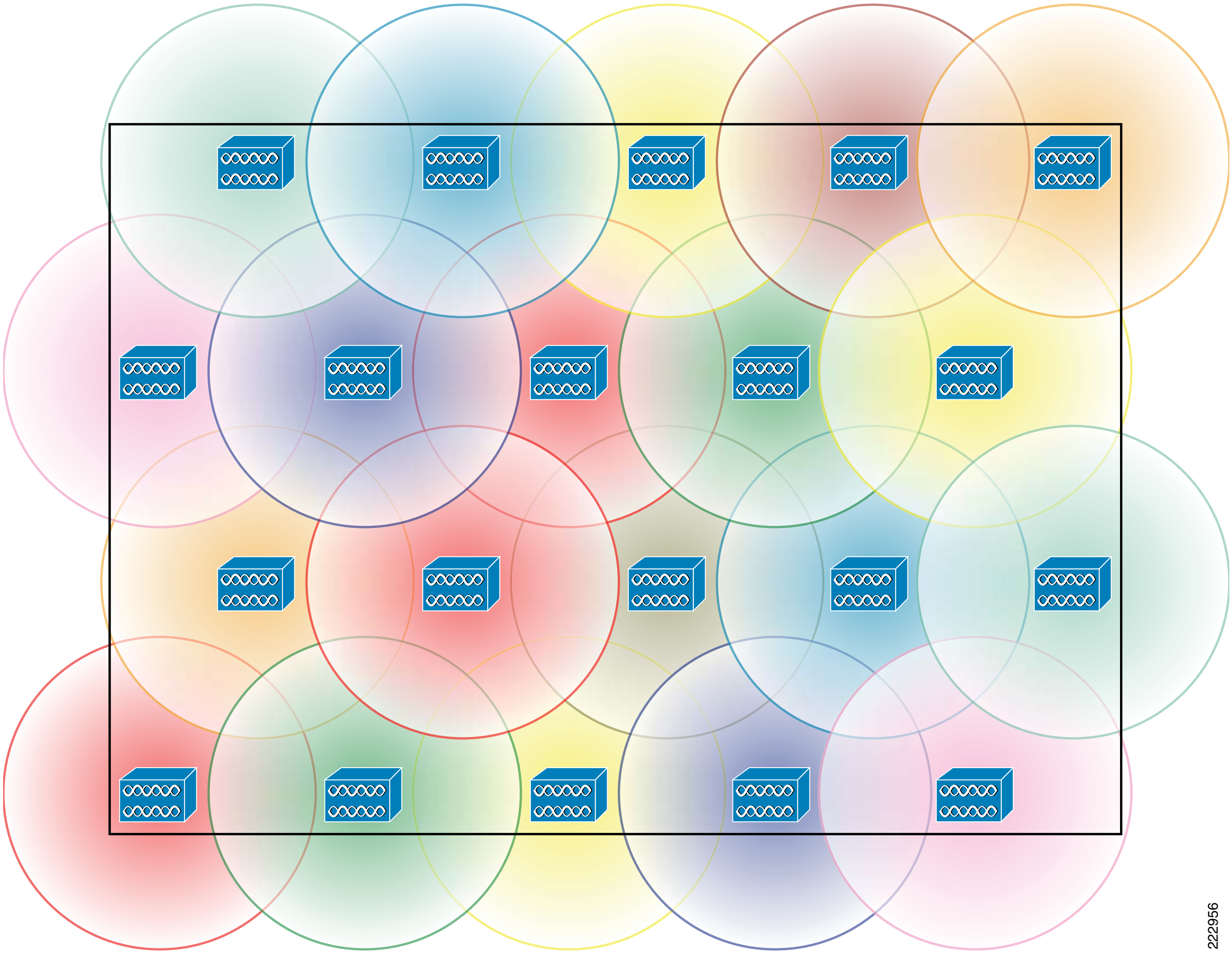
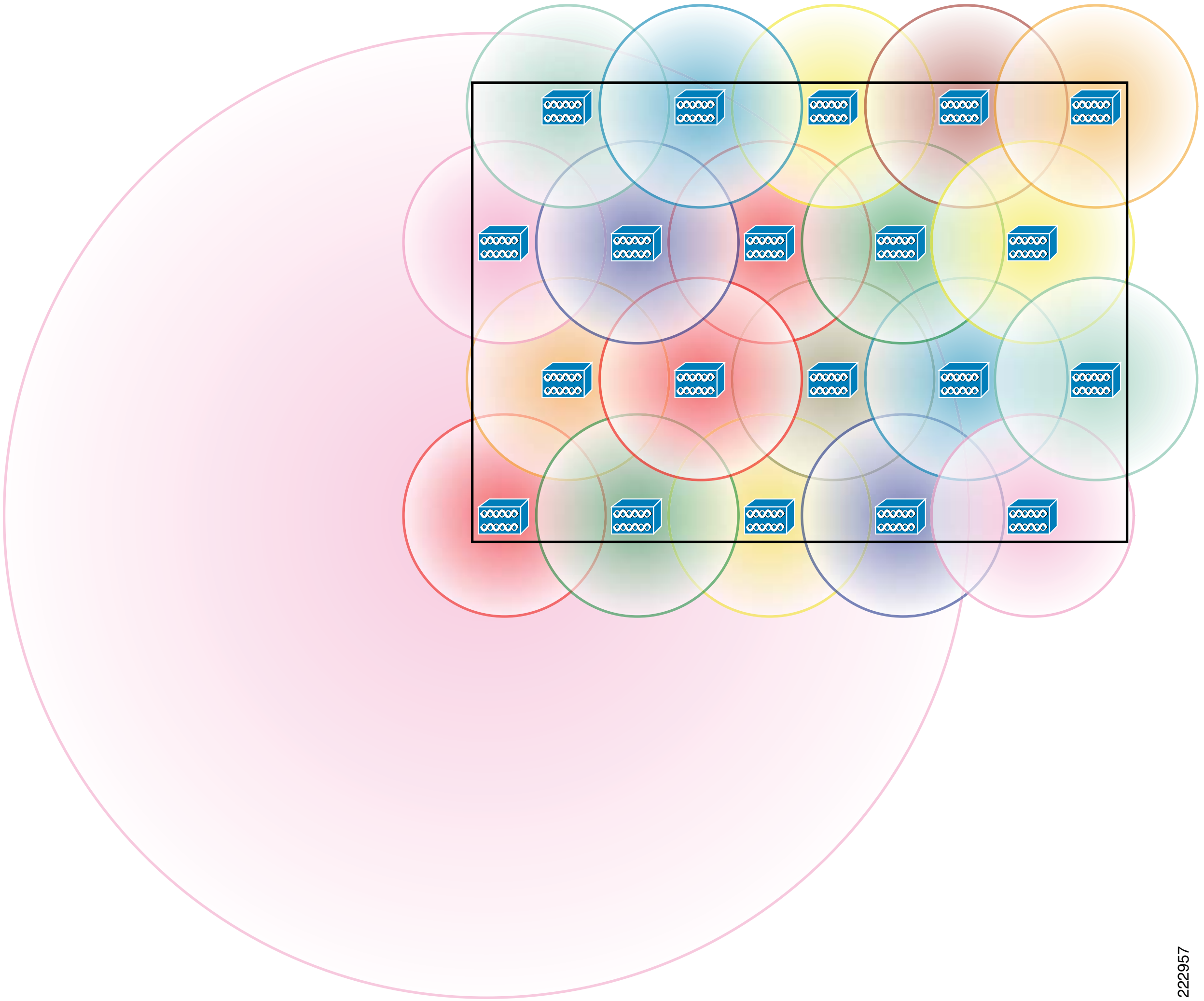


Figure 3-16 illustrates an example of the same AP layout as Figure 3-15 combined with the co-channel interference radius of a single AP. This illustrates that even though the co-channel interference is smaller, and the number of channels available is greater, co-channel interference is sufficiently large to affect overall call capacity on the floor. It would be very difficult to attempt to calculate the amount of co-channel interference across the entire floor, given that there are 20 APs and eight channels in use. It is safe to say, given that there are eight channels in use, that the VoWLAN call capacity of the floor would be equivalent eight times the call capacity of a single AP.

Figure 3-16 5 GHz Single Floor Layout with Co-channel Radius

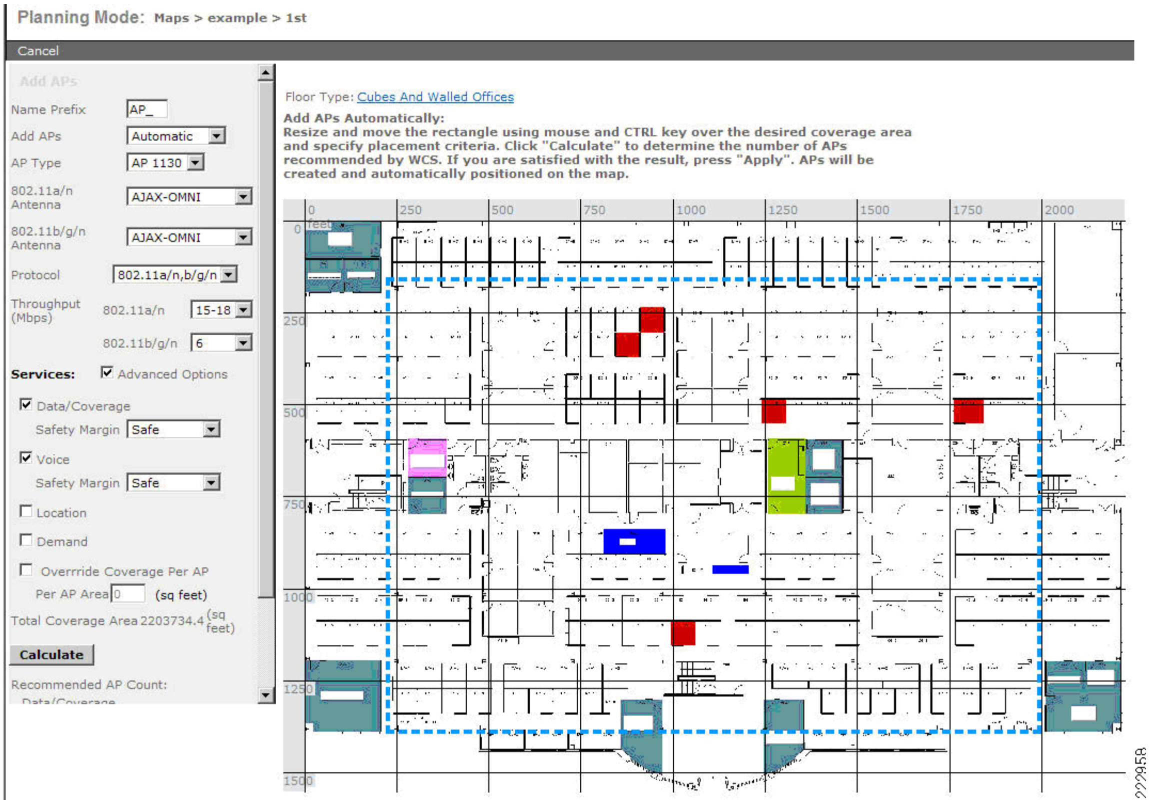


Planning Tools

The examples shown in this chapter use simple drawing tools and do not address the complex physical construction and building layout that must be considered in WLAN planning. We recommend that WLAN planning tools be used to plan the WLAN layout. These tools will assist in both ordering and placing equipment in an optimum. As with any project, the cost of fixing errors increases by orders of magnitude in a project. An error missed in planning can be 10 times more costly to fix in the implementation stage and 100 times more costly to fix in the operation stage. Investments in planning and planning tools generally pay for themselves many times over.

The Cisco Unified Wireless Network Wireless Control System (WCS) provides a WLAN planning tool, as do third-party vendors such as *AirMagnet*. Figure 3-17 depicts an example of the WCS planning page that uses the same floor plans that would be later used by the WCS to automatically lay out APs based on common WLAN deployment models.

Figure 3-17   Example WCS Planning Page



Planning Mode: **Maps > example > 1st**

Cancel

Add APs

Name Prefix: AP_

Add APs: Automatic

AP Type: AP 1130

802.11a/n Antenna: AJAX-OMNI

802.11b/g/n Antenna: AJAX-OMNI

Protocol: 802.11a/n,b/g/n

Throughput (Mbps): 802.11a/n 15-18

802.11b/g/n 6

Services: ☑ Advanced Options

☑ Data/Coverage

Safety Margin: Safe

☑ Voice

Safety Margin: Safe

□ Location

□ Demand

□ Overrride Coverage Per AP

Per AP Area 0 (sq feet)

Total Coverage Area 2203734.4 (sq feet)

Calculate

Recommended AP Count:

Data/Coverage

Floor Type: Cubes And Walled Offices

Add APs Automatically:
Resize and move the rectangle using mouse and CTRL key over the desired coverage area and specify placement criteria. Click "Calculate" to determine the number of APs recommended by WCS. If you are satisfied with the result, press "Apply". APs will be created and automatically positioned on the map.

CHAPTER 4

Voice over WLAN Security

The security of a wireless LAN (WLAN) system is always a critical consideration in every WLAN deployment. Control of the WLAN access relies on the principles of Authentication, Authorization, and Accounting (AAA), augmented by encryption to ensure privacy. This chapter focuses on the authentication and encryption aspects of WLAN security, as they relate to VoWLAN deployments. For a more complete and system view of WLAN security, refer to the following guides:

- *Secure Wireless Design Guide*—
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/secwlandg10/secwire_1_0_book.html
- *Mobility Design Guide*—
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html

WLAN Security Overview

WLAN traffic is visible to any WLAN device within radio frequency (RF) range, and is a shared access medium. This creates a number of security challenges:

- How do you provide privacy for users of your WLAN, from non-users?
- How to provide privacy for users of your WLAN from each other?
- How to support privacy of multicast and broadcast traffic?
- How to identify which user is which on the WLAN?

Each generation of WLAN security have addressed these challenges in slightly different ways. But the key mechanisms are based on the same strategies used to secure communication over an untrusted medium(i.e., Authentication, Authorization and Accounting (AAA) , and encryption). The original 802.11 standard defined an encryption mechanism, Wired Equivalent Privacy (WEP), but did not define a AAA mechanism. The level of authentication offered in the 802.11 standard was at a group level, everyone in the group had to have the same encryption key. This key was used to encrypt unicast and multicast traffic. WLAN security solutions have augmented this group authentication by authenticating the client’s MAC address. This is not considered a significant improvement in security as:

- It does not provide any additional per user privacy; the WEP key is still shared by all users.
- Offers a weak level of authentication as the 802.11 MAC addresses are sent unencrypted; the MAC address identifies the WLAN client and not the users.

- MAC address authentication can be difficult to administer for large groups of users, as the database of client MAC addresses must be maintained. The management for WEP keys is difficult, if a WEP needs to be changed all devices must be updated.

802.1X/EAP and Dynamic WEP

In order to provide an enterprise-level WLAN security, Cisco introduced the 802.1X/EAP authentication mechanisms to provide mutual authentication of WLANs and WLAN clients. During the authentication process, a unique per-user per session shared key is also derived and a portion of this key is used as per-session WEP encryption key. The Extensible Authentication Protocol (EAP) mechanism used by Cisco was called LEAP Lightweight Extensible Authentication Protocol (LEAP), which allowed users to perform an MSCHAPv2 authentication against a RADIUS server. Additional EAP mechanisms such as PEAP and EAP-TLS followed LEAP, all providing mechanism for dynamic WEP key generation. However, LEAP is considered the best suited of these for VoWLAN handsets as it requires fewer network transactions for authentication and has lower CPU requirements than the other EAP mechanisms.

Note EAP-FAST, if available, is the recommended EAP type for use of VoWLAN deployments. For more information about EAP-FAST, refer to EAP-FAST, page 4-3.

WEP

While the introduction of a dynamic WEP mechanism was a great improvement upon static WEP key implementations, weakness found in the WEP encryption mechanism means that the security of both static and dynamic WEP are compromised. Dynamic WEP is still the superior security mechanism to static WEP, but the security weaknesses in WEP are such that WEP, either static or dynamic, should not be relied upon to secure a WLAN network.

LEAP

LEAP has been found to have security weakness where weak passwords can be derived through analysis of the LEAP authentication transactions. The security weakness of LEAP is such that it should only be used where the use of strong passwords, a 10-character or higher random string, can be enforced. This means that LEAP may be suitable for VoWLAN handsets as they typically can have a strong passwords policy enforced, as the network administrator would control the handset’s passwords. LEAP may be unsuitable for WLAN PCs, as LEAP would typical use the Windows password and these passwords are generally user-generated and a strong password policy can be difficult to enforce.

Note Although LEAP is considered secure for VoWLAN handsets when correctly deployed, it is recommended that a different EAP supplicant, such as EAP-FAST, be used if available.

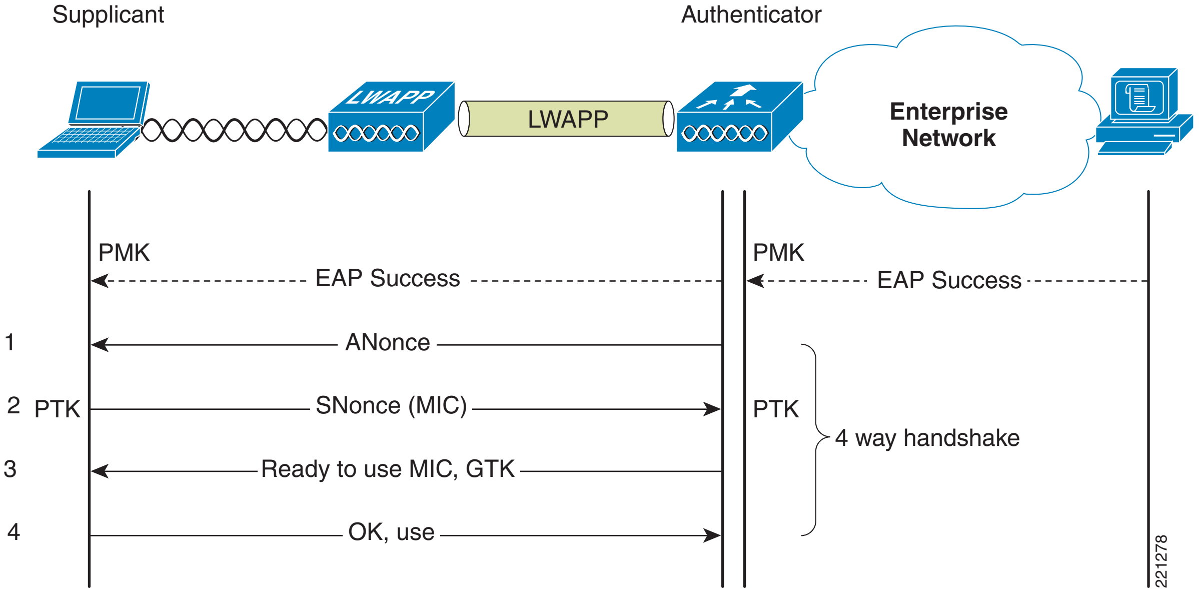
EAP-FAST

The recommended replacement for LEAP is EAP-Flexible Authentication via Secure Tunneling (EAP-FAST). The EAP-FAST protocol was specifically design to take into account the limited processing power of application specific devices (ASDs) such as VoWLAN handsets. It is designed to provide the same tunneling protection as a tunneled authentication protocol such as PEAP, without requiring the Public Key Infrastructure (PKI) overhead associated with setting up the TLS tunnel used in PEAP. As a tunneled protocol EAP-FAST is capable of supporting multiple inner authentication mechanism such as MSCHAPv2 or GTC, the supported inner authentication mechanism depends upon the client implementation.

WPA

The weaknesses in WEP and the demand for a solution drove the Wi-Fi Alliance (http://www.wi-fi.org/) to develop WLAN security improvements, based on an 802.11i draft. These improvements are defined as Wi-Fi Protected Access (WPA). WPA addressed the main weakness in WEP encryption by replacing it with the Temporal Key Integrity Protocol (TKIP) which reuses the core encryption engine of WEP (RC4). The reuse of RC4 allowed TKIP to be implemented in the majority of systems through a firmware upgrade, rather than requiring a hardware upgrade. In addition to TKIP, WPA implemented one other major improvement to WEP encryption, an additional message integrity check (MIC) mechanism. In addition to the encryption and message integrity improvements WPA introduced cryptographic improvements where the key shared between the WLAN client and the WLAN AP is not used directly for encryption, but instead it is used as the basis for a 4-way cryptographic handshake, that derives the encryption key, and passes the multicast (group) key. This 4-way handshake is used in both WPA-Personal and WPA-Enterprise. Figure 4-1 shows the basic 4-way handshake mechanism used in WPA-Enterprise. The difference between the WPA-Enterprise behavior and the WPA-Personal behavior is that the 4-way handshake with WPA-Enterprise uses a key derived during the EAP authentication as the base key of the 4-way. Whereas WPA-Personal 4-way handshake users a shared key configured in the WLAN client, Supplicant, and the WLC Authenticator (see Figure 4-1).

Figure 4-1 4-Way Handshake



The keys used for encryption are derived from the PMK that has been mutually derived during the EAP authentication. 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:

Step 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 generates an supplicant nonce (SNonce), which is a random number generated by the supplicant).

  b. The supplicant derives a pair-wise temporal key (PTK) from the ANonce and SNonce (supplicant nonce, which is a random number generated by the client/supplicant).

Step 2 The supplicant sends an EAPOL-Key frame containing an SNonce, the RSN information element from the (re)association request frame, and a MIC (generated from the PMK).

  a. The authenticator derives the PTK from the ANonce and SNonce and validates the MIC in the EAPOL-Key frame.

Step 3 If the validation is successful, the authenticator sends an EAPOL-Key frame containing the group temporal key (GTK), the multicast, and the broadcast encryption key.

  a. Upon validating the MIC from this frame, the supplicant installs its PTK and the GTK.

Step 4 The supplicant sends an EAPOL-Key frame to confirm that the temporal keys are installed.

  a. Upon validating the MIC from this frame, the authenticator installs the PTK for this client.

At this point the supplicant and authenticator have verified that they both have a matching PMK, and both share the same PTK and GTK.

WPA-Personal

WPA-personal uses the same cryptographic tools, as WPA-Enterprise but uses a shared key to authenticate WLAN clients. This shared key is the key that used in the 4-way handshake that creates the encryption key for that session. The shared key mechanism of authentication used in WPA-Personal does not provide a per-user or per device authentication, every device and every AP that is part of that WLAN uses the same shared key. The key used for encryption is unique per user and per session thanks to the randomizing that occurs during the 4-way handshake, but the shared key used to authenticate is the same for everyone. The primary advantage of WPA-personal in a VoWLAN deployment is that it does not require the use of a AAA server, and this can be an advantage in branch deployments.

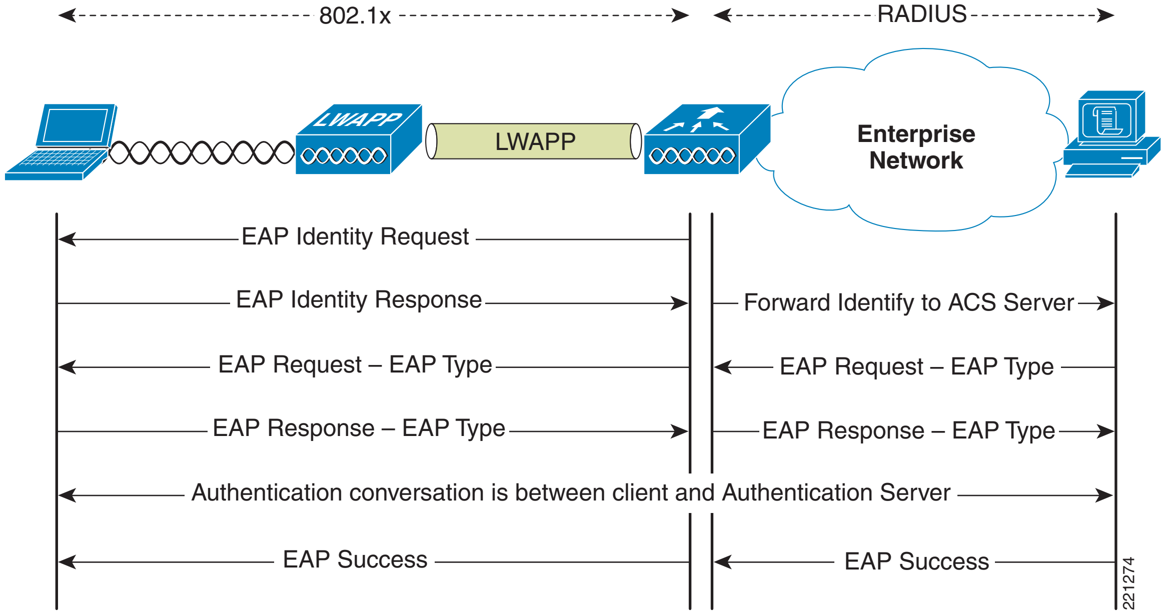
Note Strong keys should be used as there are tools available that can successfully perform a dictionary attack on WPA-personal.

WPA-Enterprise

WPA-enterprise uses the base WPA frame protection features, and cryptographic features as WPA-personal, but adds 802.1X/EAP-based authentication to the certification. In WPA-enterprise the shared key that is used to generate the cryptographic key through 4-way handshake is derived during the EAP Authentication. The EAP authentication process provides the AAA features missing in

WPA-personal, allowing each user/device to be individually authenticated, a policy based on the authentication ID applied (authorization), and the collection of statistics based on authentication ID (accounting). Figure 4-2 shows an example of EAP protocol flow.

Figure 4-2 EAP Protocol Flow



WPA-Enterprise vs WPA-Personal

Generally, the use of WPA-enterprise is preferred over WPA-personal in enterprise deployments; therefore, the naming convention, WPA-personal is targeted more at the home users. Shared key security systems do not provide the AAA features required for the enterprise, and can introduce operational issues due to the overhead in updating the shared keys if a WLAN client is lost, stolen, or as part of a regular key rotation regime. The reward for successfully cracking, guessing, or stealing the shared key is very high, as it the key for all users. In some deployments WPA personal may be used for VoWLAN deployments, as the enterprise security requirement for AAA need to be balanced against the VoWLAN handset requirements, and characteristics. Voice systems have very high availability requirements, and these may be difficult to achieve in branch and remote environments, when there is a dependency upon a centralized authentication system. This could be addressed by distributing authentication databases to branches through local AAA servers or the embedded AAA services of a WLC; or by deploying a VoWLAN system that does not rely on centralized authentication, such as WPA-personal. The security requirements of VoWLAN also need to be considered in light of the access given to the VoWLAN handsets (i.e., the VoWLAN handset need not be given access to the entire enterprise network) is able to make and receive phone calls, and have limited application access. In addition, a handset such as a Cisco 7921G has application level AAA performed by the UC Manager where the handset is authenticated, authorized, and accounting information is collected.

WPA2

The security features developed in WPA were based on the recommendations of the 802.11i workgroup that was tasked with replacing original security features defined in the 802.11 standard. The market demands for a replacement for WEP, where WPA was released prior to the ratification of the 802.11i standard. There are also slight differences between WPA and the related sections of the 802.11i standard; these differences should be transparent to users. The sections from the 802.11i standard used by WPA primarily addresses the need for a securing the WLAN while maintaining sufficient backward compatibility with WEP for the deployed hardware to be upgraded, though software and firmware changes. While the security changes from 802.11i adopted by WPA are important, the key component in 802.11i was the incorporation of the Advanced Encryption Standard (AES) into WLAN security this would align its encryption mechanism with the new industry standard for encryption. The underlying mechanism of AES-Counter Mode CBC-MAC (AES-Counter Mode describes the encryption mechanism, and CBC-MAC describes frame protection mechanism) is very different to those of WPA and WEP, and generally requires hardware upgrades to be supported. The hardware requirements to support AES encryption in WPA2 mean that migration from WPA is dependent upon a hardware refreshes. In many cases, updating the network infrastructure is an easier task than updating the WLAN client infrastructure and a complete migration to WPA2 is dependent upon a generational change in the WLAN client infrastructure. The desire to migrate from WPA to WPA2 is also tempered by the knowledge that currently there are no known serious security exposures in WPA.

WPA2-Personal

WPA2-Personal uses the same shared key and 4-way handshake of WPA, but uses the AES-Counter Mode CBC-MAC Protocol to encrypt and protect frames.

WPA2-Enterprise

WPA2-Enterprise uses the same 802.1X/EAP authentication and 4-way handshake of WPA, but uses the AES-Counter Mode CBC-MAC Protocol to encrypt and protect frames.

EAP Timing

The EAP authentication mechanism, its supporting infrastructure and protocols, has to make some assumptions about what is a reasonable amount of time to wait for a WLAN client during the EAP authentication process. These assumptions are based on the typical timing from PC clients, and may not be valid for lower CPU devices such as VoWLAN handsets. For example, an EAP timer adjustment is recommended when using EAP-FAST authentication for the 7921G phone. If not implemented the 7921G is likely to fail authentication even though its credentials are correct.

To adjust the EAP request timeout to 20: [WiSM]]-slot3-1) config advanced eap request-timeout 20 show advanced eap command:

```
EAP-Identity-Request Timeout (seconds)........... 1
EAP-Identity-Request Max Retries................. 20
EAP Key-Index for Dynamic WEP.................... 0
EAP Max-Login Ignore Identity Response....... enable
EAP-Request Timeout (seconds).................... 20
EAP-Request Max Retries.......................... 2
```

Note Only adjust the EAP timers on the advice of the VoWLAN handset vendor, or when following recommendation from Cisco TAC.

Network Segmentation

The VoIP network shares the base network infrastructure of an enterprise network, but should be separated whenever possible from the general purpose data network. The topic of segmenting and securing the VoIP network is beyond the scope of this design guide, but the VoWLAN network should be separated from the WLAN data network. This can be done in the Cisco Unified Wireless Network, through the assignment of a VoWLAN interface on the WLC, which is a type of VLAN separation. This should be sufficient to provide integration into the large enterprise VoIP segmentation scheme, whether that be VLAN segmentation, IP address segmentation, or VRF segmentation.

CHAPTER 5

Voice over WLAN Roaming

At its most basic level, *roaming* in an enterprise IEEE 802.11 network occurs when an IEEE 802.11 client changes its access point (AP) association from one AP to another AP within the same WLAN.

Roaming is a client decision. The client is responsible for deciding it needs to roam, and then detecting, evaluating, and roaming to an alternative AP.

Note Roaming is a client decision. WLAN standards bodies (such as the IEEE) and industry bodies (such as the Wi-Fi Alliance) do not specify when a client should roam, or how the client determines to which alternative AP it should roam. Each vendor's roaming algorithms are proprietary and are not generally published.

Client Roaming Decision

IEEE 802.11 clients typically decide to roam when the connection to the current AP becomes degraded. Roaming necessarily has some impact on client traffic because a client scans other IEEE 802.11 channels for alternative APs, reassociates, and authenticates to the new AP. Prior to roaming, a client may take some actions to improve its current connection without necessitating a roam:

- *Data retries*—The IEEE 802.11 MAC specifies a reliable transport. Every unicast frame sent between a wireless client and an AP is acknowledged at the MAC layer. The IEEE 802.11 standard specifies the protocol used to retry the transmission of data frames for which an acknowledgment was not successfully received.
- *Data rate shifting*—IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g each support a variety of possible data rates. The data rates supported for a given frequency band (such as 2.4GHz or 5GHZ) are configured on the WCS/WLC and are pushed down to the APs using that frequency band. Each AP in a given WLAN then advertises the supported data rates in its beacons. When a client or AP detects that a wireless connection is becoming degraded, it can change to a lower supported transmission rate (lower transmission rates generally provide superior transmission reliability).

Although the roaming algorithms differ for each vendor or driver version (and potentially for different device-types from a single vendor), there are some common situations that typically cause a roam to occur:

- *Maximum data retry count is exceeded*—Excessive numbers of data retries are a common roam trigger.
- *Low received signal strength indicator (RSSI)*—A client device can decide to roam when the receive signal strength drops below a threshold. This roam trigger does not require active client traffic in order to induce a roam.

- *Low signal to noise ratio (SNR)*—A client device can decide to roam when the difference between the receive signal strength and the noise floor drops below a threshold. This roam trigger does not require active client traffic in order to induce a roam.
- *Proprietary load balancing schemes*—Some wireless implementations have schemes where clients roam in order to more evenly balance client traffic across multiple APs. This is one case where the roam may be triggered by a decision in the WLAN infrastructure and communicated to the client via vendor-specific protocols.

Cisco Compatible Extensions Client Roam Triggers

WLAN controllers (WLC) are configured with a default set of RF roaming parameters that are used to set the RF thresholds adopted by the client to decide when to roam. The default parameters can be overridden by defining a custom set. These Cisco Compatible Extensions parameters are defined on the WLC once per IEEE 802.11 frequency band (2.4GHz or 5GHz).

WLAN clients running Cisco Compatible Extensions version 4 or later are able to use the following parameters (which are communicated to the client via the *enhanced neighbor list* feature described in "Cisco Compatible Extensions Channel Scanning" section on page 5-3):

- *Scan threshold*—The minimum RSSI that is allowed before the client should roam to a better AP. When the RSSI drops below the specified value, the client must be able to roam to a better AP within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.
- *Transition time*—The maximum time allowed for the client to detect a suitable neighboring AP to roam to and to complete the roam, whenever the RSSI from the client's associated AP is below the scan threshold. The scan threshold and transition time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a WLAN network that supports roaming simply by ensuring a certain minimum overlap distance between APs.
- *Minimum RSSI field*—A value for the minimum RSSI required for the client to associate to an AP.
- *Hysteresis*—A value to indicate how much greater the signal strength of a neighboring AP must be in order for the client to roam to that AP. This parameter is intended to reduce the amount of roaming between APs if the client is physically located on or near the border between two APs.

Roaming Selection of a New AP

Channel Scanning

Wireless clients learn about available APs by scanning other IEEE 802.11 channels for available APs on the same WLAN/SSID. Scanning other IEEE 802.11 channels can be performed actively or passively as follows:

- *Active scan*—Active scanning occurs when the client changes its IEEE 802.11 radio to the channel being scanned, broadcasts a probe request, and then waits to hear any probe responses (or periodic beacons) from APs on that channel (with a matching SSID). The IEEE 802.11 standards do not specify how long the client should wait, but 10 ms is a representative period. The probe-request frames used in an active scan are one of two types:

  - *Directed probe*—The client sends a probe request with a specific destination SSID; only APs with a matching SSID will reply with a probe response
  - *Broadcast probe*—The client sends a *broadcast* SSID (actually a null SSID) in the probe request; all APs receiving the probe-request will respond, with a probe-response for each SSID they support.
- *Passive scan*—Passive scanning is performed by simply changing the clients IEEE 802.11 radio to the channel being scanned and waiting for a periodic beacon from any APs on that channel. By default, APs send beacons every 100 ms. Because it may take 100 ms to hear a periodic beacon broadcast, most clients prefer an active scan.

During a channel scan, the client is unable to transmit or receive client data traffic. There are a number of approaches clients take to minimize this impact to client data traffic:

- *Background scanning*—Clients may scan available channels before they need to roam. This allows them to build-up knowledge of the RF environment and available APs so they may roam faster if it becomes necessary. Impact to client traffic can be minimized by only scanning when the client is not actively transmitting data, or by periodically scanning only a single alternate channel at a time (scanning a single channel incurs minimal data loss)
- *On-roam scanning*—In contrast with background, on-roam scanning occurs after a roam has been determined necessary. Each vendor/device may implement its own algorithms to minimize the roam latency and the impact to data traffic. For example, some clients might only scan the non-overlapping channels.

Typical Scanning Behavior

Although most client roaming algorithms are proprietary, it is possible to generalize the typical behavior.

Typical wireless client roam behavior consists of the following activities:

- *On-roam scanning*—This ensures clients have the most up-to-date information at the time of the roam.
- *Active scan*—An active scan is preferred over a passive scan, due to lower latency when roaming.

There are some informational attributes that may be used to dynamically alter the roam algorithm:

- *Client data type*—For example, voice call in progress
- *Background scan information*—Obtained during routine periodic background scans

Ways in which attributes can be used to alter the scan algorithm include:

- *Scan a subset of channels*—For example, information from the background scan can be used to determine which channels are being used by APs in the vicinity.
- *Terminate the scan early*—For example, if a voice call is in progress, the first acceptable AP might be used instead of waiting to discover all APs on all channels.
- *Change scan timers*—For example, if a voice call is in progress, the time spent waiting for probe responses might be shortened during an active scan.

Cisco Compatible Extensions Channel Scanning

While WLAN clients ultimately determine when to associate (or reassociate) to an AP, Cisco APs provide information to clients to facilitate AP selection by providing information (such as channel load in its beacons and probe responses) or by providing a list of neighboring APs.

WLC software release 4.0 and later support the following Cisco Compatible Extensions, Layer-2 client-roaming enhancements:

- *AP assisted roaming*—This feature helps clients save scanning time. Whenever a Cisco Compatible Extensions v2 client associates with an AP, it sends an information packet to the new AP listing the characteristics of its previous AP. The AP uses this information to build a list of previous APs, which it sends (via unicast) to clients immediately after association to reduce roaming time. The AP list contains the channels, BSSIDs of neighbor APs that support the client's current SSID(s), and time elapsed since disassociation.
- *Enhanced neighbor list*—The enhanced neighbor list is an enhanced version of the neighbor list which is sent as part of the Cisco Compatible Extensions v2 AP Assisted Roaming feature. It is always provided unsolicited by the AP to the client immediately following a successful association or reassociation. As the AP periodically checks to ensure its neighbor list is up to date, it may also send an unsolicited update to the corresponding clients. The enhanced neighbor list may include, for each AP, the RF parameters discussed in the "Cisco Compatible Extensions Client Roam Triggers" section on page 5-2. In addition, it may include, for each AP in the list, additional information about AP timing parameters, information about the AP support for the clients subnet, and the strength and SNR of the last transmission from the client received by the AP.
- *Enhanced neighbor list request (E2E)*—The *End-2-End* (E2E) specification is a Cisco and Intel joint program that defines new protocols and interfaces to improve the overall voice and roaming experience. It applies only to Intel clients in a Cisco Compatible Extensions environment. Specifically, it enables Intel clients to request a neighbor list at will. When this occurs, the AP forwards the request to the WLC. The WLC receives the request and replies with the current Cisco Compatible Extensions roaming sublist of neighbors for the AP to which the client is associated.

Note To see whether a particular client supports E2E, click **Wireless** > **Clients** on the WLC GUI, click the **Detail** link for the desired client, and look at the E2E *Version* field under *Client Properties*.

- *Directed roam request*—This feature enables the WLC to send directed roam requests to the client in situations when the WLC can better service the client on an AP different from the one to which the client is associated. In this case, the WLC sends the client a list of the *best* APs that it can join. The client can either honor or ignore the directed roam request. Non-Cisco Compatible Extensions clients and clients running Cisco Compatible Extensions v3 or prior must not take any action. No configuration is required for this feature.

WLC software release 4.0 supports Cisco Compatible Extensions versions 1 through 4. Cisco Compatible Extensions support is enabled automatically for every WLAN on the WLC and cannot be disabled. The WLC stores the Cisco Compatible Extensions version of the client in its client database and uses it to generate and respond to Cisco Compatible Extensions frames appropriately. Clients must support Cisco Compatible Extensions v4 (or Cisco Compatible Extensions v2 for AP-assisted roaming) in order to utilize these roaming enhancements.

Note AP 1030s in Remote Edge AP (REAP) mode, and hybrid-REAP APs in H-REAP locally switched mode do not support Cisco Compatible Extensions Layer 2 roaming.

Evaluating the List of Potential Roam Targets

Once the wireless client has a list of potential APs to which it can roam, the client will use a client-specific algorithm to choose a specific AP to which it will roam. Factors that may be considered include:

- Receive signal strength indicator (RSSI)
- Signal to noise ratio (SNR)
- Number of clients on the AP
- Transmit and receive bandwidth being used by the AP
- RF channel load information from beacon and probe responses sent by the AP (see Chapter 2, "WLAN Quality of Service" for more information).

Reauthenticating to a New AP

When a wireless client initially joins a WLAN it must authenticate before being granted access to the network. This section describes the following considerations and processes:

- Authentication Types, page 5-5
- Reauthenticating When Roaming, page 5-6

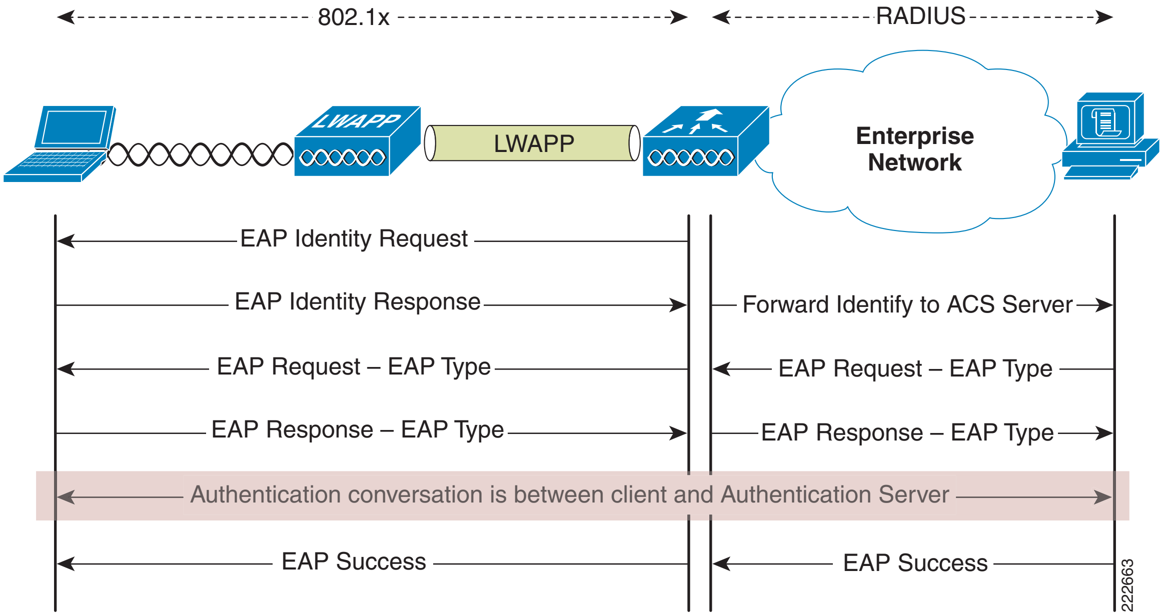
Note Detailed security information including WLAN authentication details is available in the CVD *Secure Wireless Design Guide*.

Authentication Types

Authentication schemes for WLAN access include the following:

- *Open Authentication*—This is null authentication, any client is permitted to access the WLAN.
- *Wired Equivalent Privacy (WEP) Shared Key (Static WEP)*—Static WEP requires sender and receiver to have the same pre-provisioned key in order to decode messages from each other
- *Wi-Fi Protected Access (WPA)-Personal and WPA2-Personal*—A shared key, which is not the encryption key, is configured on both the WLAN and the WLAN client, and this key is used in the WPA 4-way handshake to generate a per-session encryption key.
- *IEEE 802.1X/Extensible Authentication Protocol (EAP) Authentication used in WPA-Enterprise or WPA2-Enterprise*—Depending on the customer requirements, various EAP authentication protocols such as Protected EAP (PEAP), EAP-Transport Layer Security (EAP-TLS), and EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) can be used in secure wireless deployments. Regardless of the protocol, they all currently use IEEE 802.1X, EAP, and Remote Authentication Dial-In User Service (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. Figure 5-1 shows the basic flow of an IEEE 802.1X/EAP authentication.

Figure 5-1 EAP Protocol Flow



In Figure 5-1, the section labeled *Authentication conversation is between client and Authentication Server* (highlighted in red) depicts the step when authentication of the client by the authentication—Authentication, Authorization, and Accounting (AAA)/RADIUS—server occurs. This authentication involves multiple packets being relayed by the WLC from the client to the AAA/RADIUS server and back again. This portion of the authentication also requires CPU-intensive cryptographic processing at both the client and the AAA/Radius server. This part of the authentication is where latency can easily exceed one second and is the focus of the fast roaming algorithms discussed in the following section.

Reauthenticating When Roaming

Roaming with Open Authentication/Static WEP

When a client roams using open authentication (no keys) or using shared keys, authentication adds little roam latency, This is because no additional packets need to be exchanged between the client and the AAA server.

Roaming with IEEE 802.1X/EAP Authentication

When a client roams using IEEE 802.1X with Dynamic WEP WPA-Enterprise or WPA2-Enterprise, an IEEE 802.1X authentication generally must occur with an AAA/RADIUS server. As discussed above, authenticating with an AAA/RADIUS server can take more than one second. A one-second interruption to latency sensitive applications such as VoIP when roaming is unacceptable and therefore fast secure roaming algorithms have been developed to reduce the roam latency.

Fast Secure Roaming

Fast roaming algorithms include Cisco Centralized Key Management (CCKM) and Proactive Key Caching (PKC). CCKM and PKC allow a WLAN client to roam to a new AP and re-establish a new session key—known as the Pairwise Transient Key (PTK)—between the client and AP without requiring a full IEEE 802.1X/EAP reauthentication to a AAA/RADIUS server.

Both CCKM and PKC are Layer-2 roaming algorithms in that they to not consider any Layer-3 issues such address IP address changes. In the Cisco Unified Wireless Network, clients are allocated IP addresses from subnets that originate at the WLC—not the AP. In this way, it is possible to group large numbers of WLAN clients for a given SSID into the same Layer-2 subnet. This maximizes the scope of the Layer-2 domain—and the Fast Secure Roaming domain. Additionally, multiple-WLC deployments support client roaming across APs managed by WLCs in the same mobility group on the same or different subnets. This roaming is transparent to the client because the session is sustained and a tunnel between the WLCs allows the client to continue using the same DHCP-assigned or client-assigned IP address as long as the session remains active.

Fast Secure Roaming with Cisco Centralized Key Management

CCKM is a Cisco standard supported by Cisco Compatible Extensions clients to provide fast secure roaming.

CCKM requires support in the client. Cisco Compatible Extensions provides client-side specifications for support of many client functions, including fast secure roaming. Table 5-1 summarizes the EAP types supported in each version of Cisco Compatible Extensions.

Table 5-1 Cisco Compatible Extension EAP Support

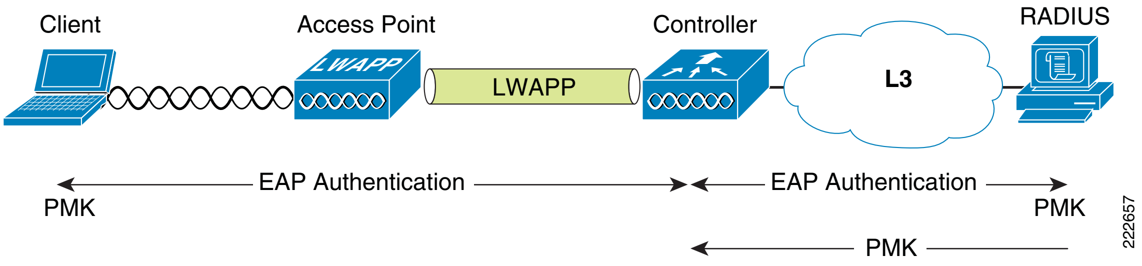
Cisco Compatible Extensions Version	EAP Types Supported
Cisco Compatible Extensions v2	CCKM with LEAP
Cisco Compatible Extensions v3	CCKM with LEAP, EAP-FAST
Cisco Compatible Extensions v4	CCKM with EAP, EAP-FAST, EAP-TLS and LEAP

CCKM establishes a key hierarchy upon initial WLAN client authentication and uses that hierarchy to quickly establish a new key when the client roams. The following sections describe the initial establishment and roam phases.

CCKM Roaming—Initial Key Hierarchy Establishment

The initial key hierarchy establishment process is illustrated in Figure 5-2 through Figure 5-5. In WPA-Enterprise and WPA2-Enterprise, the outcome of a successful EAP authentication (the protocol portion highlighted in red in Figure 5-1) is a Pairwise Master Key (PMK). Figure 5-2 shows the establishment of this PMK at the client and the AAA/RADIUS server, and the subsequent forwarding of of the PMK to the WLC.

Figure 5-2 CCKM Initial Key (Part 1 of 4)

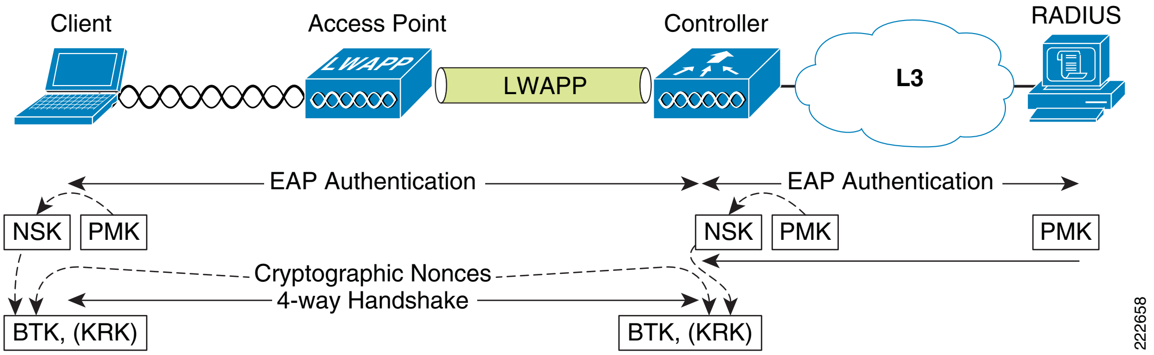


The WLC and the client both derive a Network Session Key (NSK) from the PMK. After the NSK is established, the WPA-prescribed 4-way handshake is performed between the client and the WLC. At the conclusion of the 4-way handshake, a Base Transient Key (BTK) and Key Request Key (KRK) are established. See Figure 5-3.

For more detail on the 4-way handshake, see the CVD *Secure Wireless Design Guide*.

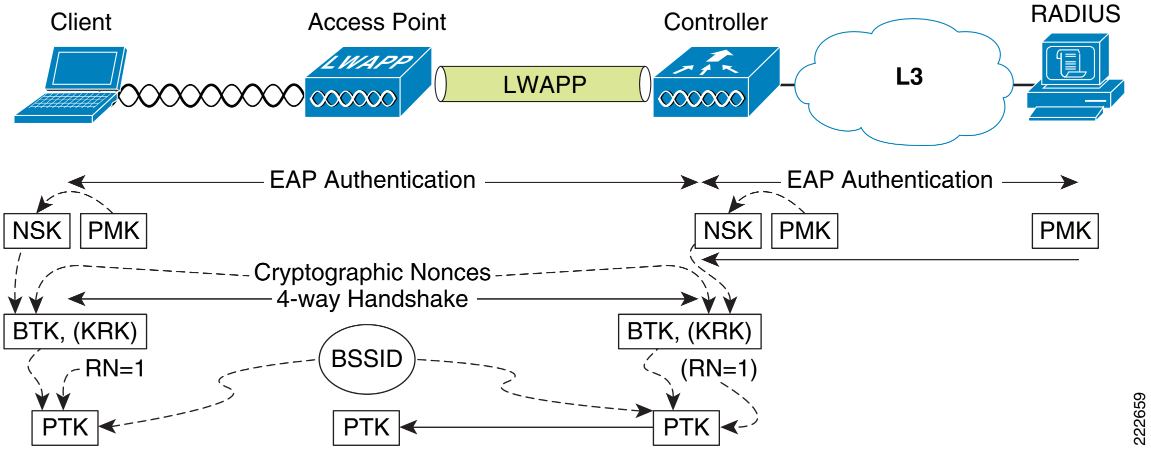
WPA and WPA2 differ only slightly from CCKM at this point. WPA/WPA2 uses the PMK directly (instead of deriving a NSK), and after the 4-way handshake establishes a Pairwise Transient Key (PTK) thus concluding the establishment of the WPA/WPA2 unicast key.

Figure 5-3 CCKM Initial Key (Part 2 of 4)



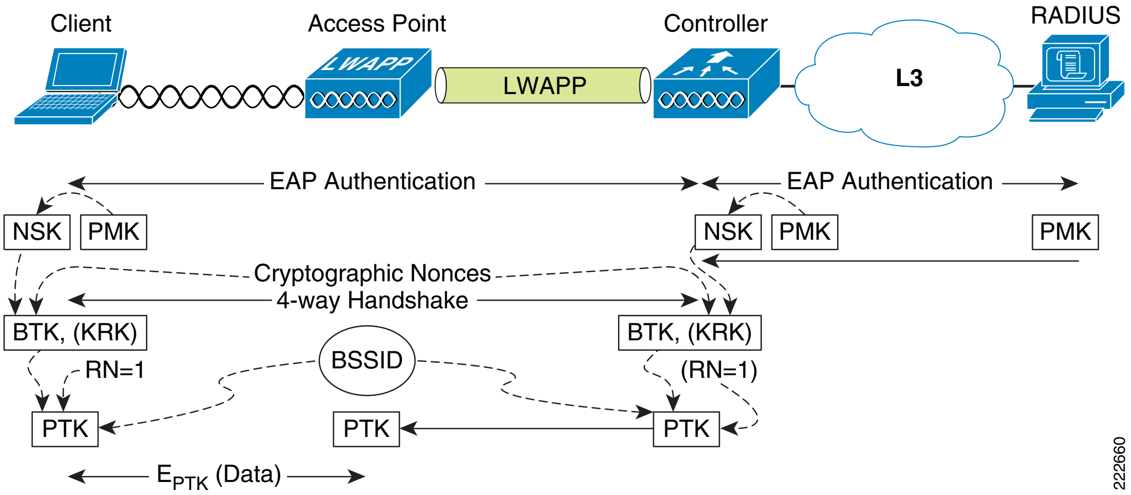
Both the client and the WLC hash the BTK, an initial Rekey Number (RN) = 1, and the BSSID to derive a PTK. The WLC then forwards the PTK to the AP over the LWAPP tunnel. See Figure 5-4.

Figure 5-4 CCKM Initial Key (Part 3 of 4)



The client and AP communicate using the PTK to encrypt the data sent between them. See Figure 5-5.

Figure 5-5 CCKM Initial Key (Part 4 of 4)



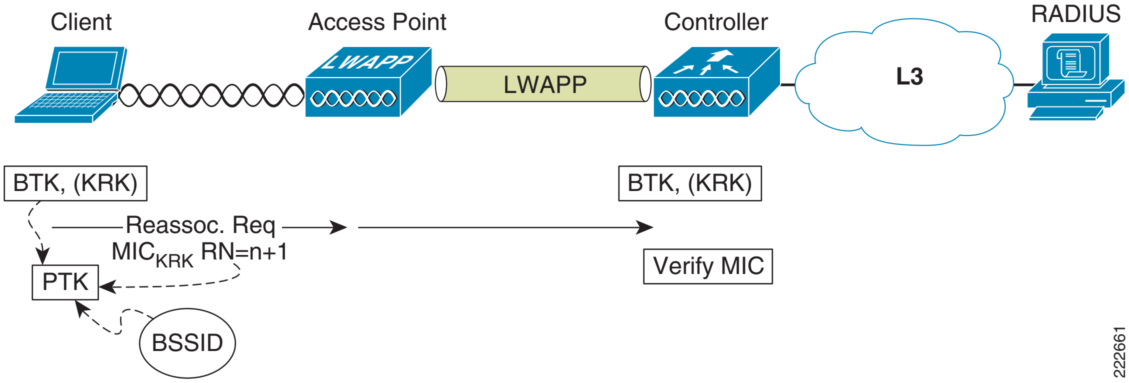
CCKM Roaming—Client Roam

CCKM exists to provide very fast roaming.

In the absence of CCKM, a WPA/WPA2 client must perform a full EAP authentication to a remote AAA/RADIUS server, followed by a WPA/WPA2 4-way handshake whenever it roams. This process can take more than one second. With CCKM, the roaming client and WLC can use pre-established keying material to immediately establish a PTK—normally within a few ten of milliseconds.

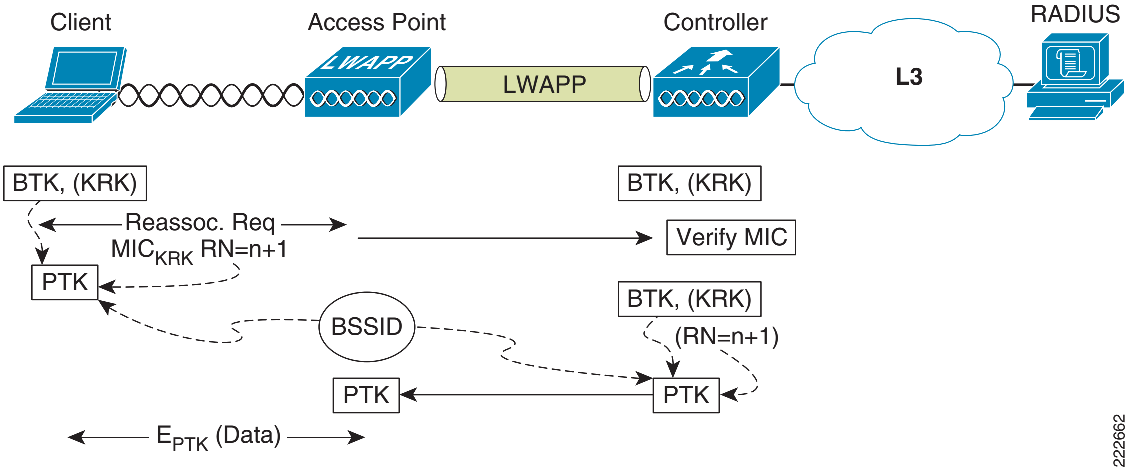
When the client roams to a new AP, the client sends a reassociate-request with the next sequential rekey-number. Protection against spoofed reassociate-requests is provided by the Message Integrity Check (MIC) that the client adds to the reassociate-request (the MIC is generated using the KRK as cryptographic input). The reassociate request is forwarded by the AP to the WLC and the MIC is validated. See Figure 5-6.

Figure 5-6 CCKM Roam Key (Part 1 of 2)



The WLC calculates the next PTK, and forwards it to the AP. The client and the AP can now communicate using the new PTK to encrypt the data sent between them. See Figure 5-7.

Figure 5-7 CCKM Roam Key (Part 2 of 2)



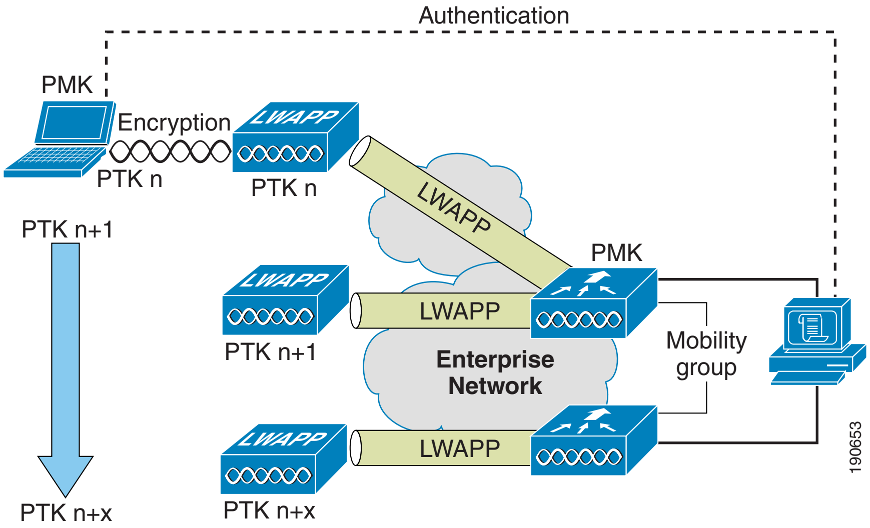
Fast Roaming with Proactive Key Caching

PKC is an IEEE 802.11i extension that allows for the proactive caching (before the client roaming event) of the WPA/WPA2 PMK that is derived during a client IEEE 802.1 x/EAP authentication at the AP (see Figure 5-8). If a PMK (for a given WLAN client) is already present at an AP when presented by the associating client, full IEEE 802.1X/EAP authentication is not required. Instead, the WLAN client can simply use the WPA 4-way handshake process to securely derive a new session encryption key for communication with that AP.

Note PKC is an IEEE 802.11i extension and so is supported in WPA2—not WPA.

The distribution of these cached PMKs to APs is greatly simplified in the Cisco Unified Wireless deployment. The PMK is simply cached in the WLC(s) and made available to all APs that connect to that WLC, and between all WLCs that belong to the mobility group of that WLC in advance of a client roaming event.

Figure 5-8 PKC Roam



IP Layer Configuration

When a client roams from one AP to another, it must determine if it requires a new IP address, or if it can continue to use its old IP address. Actions that might be required by the client include:

- Acquiring a valid IP address via DHCP
- IP duplicate address detection
- Mobile IP signaling (if required)
- Virtual private network (VPN) Internet Key Exchange (IKE) signaling (if required)

In a Cisco WLC deployment, client IP addresses do not change when they roam within the same *mobility group*. WLC deployments support client roaming across APs managed by one or more WLCs in the same mobility group on the same or different subnets. This roaming is transparent to the client because the session is sustained and a tunnel between the WLCs allows the client to continue using the same DHCP-assigned or client-assigned IP address as long as the session remains active.

Clients roaming without a Cisco fast secure roaming protocol (CCKM or PKC), will typically send a DHCP request asking for their current IP address. In a Cisco WLC environment, the WLC infrastructure will ensure the client stays on the same subnet and can continue to use its old IP address. Next, the client will typically perform duplicate address detection by pinging its own IP address and ensuring there are no replies from WLAN clients using that same address. If a client is running mobile IP or VPN, those protocols would run after the IP address is verified unique.

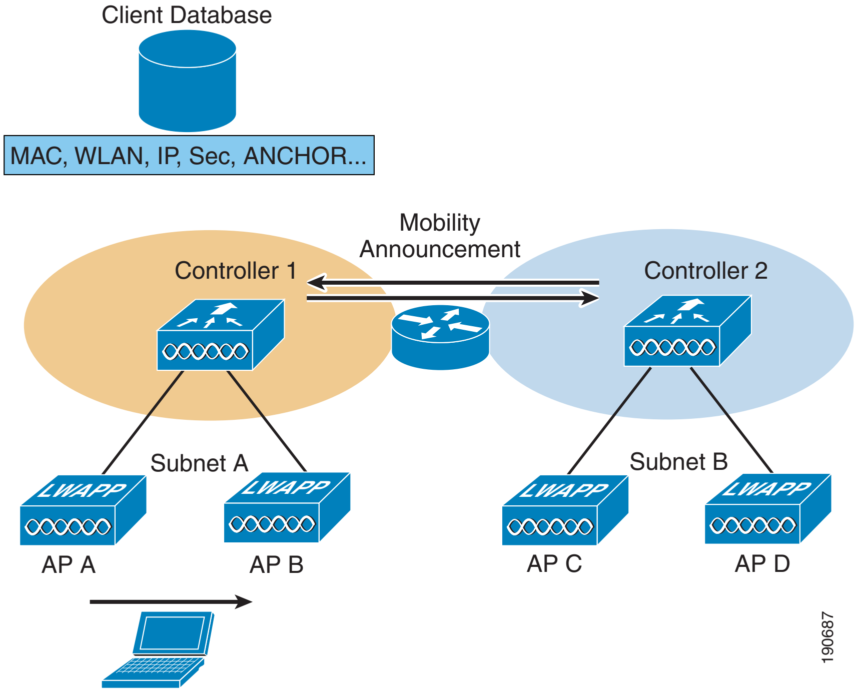
Infrastructure Impacts of Client Roaming

When a wireless client authenticates and associates with an AP, the WLC of the AP places an entry for that client in its mobility 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 updates the client database with the new associated AP. If necessary, new security context and associations are established as well.

Multiple-WLC deployments support client roaming across APs managed by WLCs in the same mobility group on the same or different subnets. This roaming is transparent to the client because the session is sustained and a tunnel between the WLCs allows the client to continue using the same DHCP-assigned or client-assigned IP address as long as the session remains active. Figure 5-9 illustrates the roaming in this context.

Figure 5-9 WLAN Infrastructure—Roam



Measuring Roam Latency

A roam can be segmented into the following components;

- Client roam decision
- Choosing a new AP to which a client roams
- Reauthenticating to the new AP
- IP layer configuration
- Infrastructure impacts of client roam

Each of these components have the potential to add latency to a roam. However, there is no industry consensus on how to measure roam latency.

The most realistic measure of roam latency is from the last packet sent by the roaming client on the old AP to the first packet received by the roaming client on the new AP. This ensures all the above components are measured and ensures that 2-way communication is as show in Table 5-2.

Table 5-2 Summary of Roam Latency Measurement Process

Roam Action	Measurement Point	Description
Start	Last packet sent by roaming client on old AP	Ensures 2-way communication is still established when the roam latency measurement commences; it is common for frames to continue to be forwarded to the roaming client on the old AP after the client has started the roam.
End	First packet received by roaming client on new AP	This again ensures 2-way communication by ensuring that the client's new location has been learned by the network infrastructure and that the client is receiving packets as well as sending them.

When comparing roam latency for different WLAN implementations, take care that the same criteria for measuring roam latency is used in each case.

Monitoring Client Roaming

In addition to the Cisco Compatible Extensions v4 channel scanning capabilities, Cisco Compatible Extensions v4 clients also send a *Roam Reason Report* to report the reason why they roamed to a new AP. It also allows network administrators to build and monitor a roam history.

Use the following commands to view information about Cisco Compatible Extensions Layer-2 client roaming.

To view the current RF parameters configured for client roaming for the IEEE 802.11a or IEEE 802.11b/g network, enter the following command:

show {IEEE 802.11a | IEEE 802.11bg} l2roam rf-params

To view the Cisco Compatible Extensions Layer-2 client roaming statistics for a particular AP, enter the following command:

show {IEEE 802.11a | IEEE 802.11bg} l2roam statistics *ap_mac*

This command provides the following information:

- The number of roam reason reports received
- The number of neighbor list requests received
- The number of neighbor list reports sent
- The number of broadcast neighbor updates sent

To view the roaming history for a particular client, enter the following command:

show client roam-history *client_mac*

This command provides the following information:

- The time when the report was received
- The MAC address of the AP to which the client is currently associated
- The MAC address of the AP to which the client was previously associated
- The channel of the AP to which the client was previously associated
- The SSID of the AP to which the client was previously associated

- The time when the client disassociated from the previous AP
- The reason for the client roam
- To obtain debug information for the Cisco Compatible Extensions Layer 2 client roaming, use the following command:

  debug l2roam {**detail** | **error** | **packet** | **all**} **enable**

CHAPTER 6

Voice over WLAN Campus Test Architecture

This chapter describes the campus deployments of voice over wireless LAN (VoWLAN). The campus network used for the VoWLAN end-to-end testing was built based on the design recommendations documented in the existing campus CVD *Routed Access Design Guide*

Additional information on the existing campus CVD, including detailed test results, can be found under the campus heading at:
http://www.cisco.com/en/US/netsol/ns742/networking_solutions_program_category_home.html.

Elements from the following design guides were also used and documented in the network built for this this chapter:

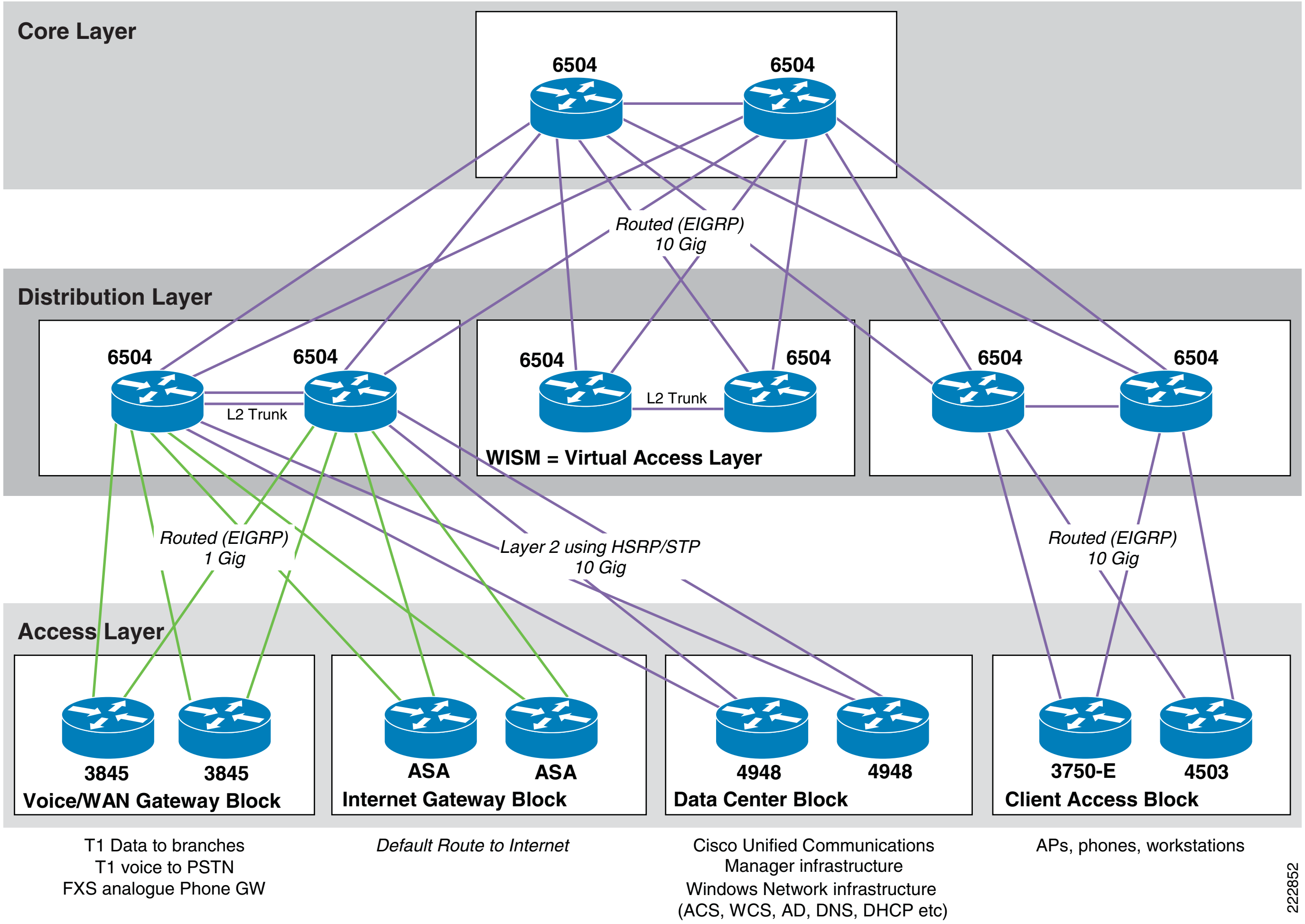
- *Enterprise QoS Solution Reference Network Design Guide Version 3.3*—
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html
- *Cisco AVVID Network Infrastructure IP Multicast Design (SRND)*—
http://www.cisco.com/application/pdf/en/us/guest/tech/tk363/c1501/ccmigration_09186a008015e7cc.pdf
- *Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x*—
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/6x/uc6_0.html
- *Enterprise Mobility 4.1 Design Guide*—
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html
- *Data Center Infrastructure Design Guide 2.5*—
http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCI_SRND_2_5_book.html

Campus Design Overview

The campus design used for the VoWLAN testing is shown in Figure 6-1. Most readers will be familiar with the hierarchical, access, distribution, core design used in this network. In the past, it was common to run Layer 2 links between the access layer and the distribution layer, and to use Spanning Tree Protocol (STP) to create a redundant, loop-free topology. Current design best practice replaces this Layer 2 STP configuration with a configuration that instead routes IP packets at the access layer. Routing in the access layer allows for faster re-convergence around failure, and simplifies the network by eliminating the need for STP and Hot standby Routing Protocol (HSRP). The campus CVD design documents referenced above provide additional information and detailed test results on the advantages of a routed access layer over a Layer 2 connection.

Data center devices have some unique network connectivity requirements that make it necessary to continue to connect to the access layer using Layer 2 and not routed IP. The unique requirements of the data center network connections are described in Campus Layer 2 Spanning Tree Protocol Design for Data Center , page 6-9.

Figure 6-1 VoWLAN Campus Architecture



The architecture shown in Figure 6-1 differs from the existing campus CVD *Routed Access Design Guide* in that multiple access layer blocks are connected to a single distribution block. In a production deployment, the campus CVD *Routed Access Design Guide* topology should be followed. This would result in each access layer block connecting to a dedicated distribution block, where policy appropriate to that type of access layer could be applied. Following the campus CVD *Routed Access Design Guide* would result in the voice/WAN gateway, the Internet Gateway, and the data center access blocks all connecting to dedicated distribution blocks rather than sharing a distribution block, as is shown in Figure 6-1.

In accordance with the campus design recommendations, all router interconnections use fiber optic transport due to the superior link failure detection capabilities fiber links have when compared to wired Ethernet connections.

The Configuration section provides sample configurations that can be used as a basis for implementing the policies discussed in the following sections.

Voice and Data VLAN Separation

Separate voice and data VLANs are used for the following reasons;

- Address space conservation and voice device protection from external networks—Private addressing of phones on the voice or auxiliary VLAN enables address conservation and ensures that phones are not accessible directly via public networks. PCs and servers are typically addressed with publicly routed subnet addresses; however, voice endpoints should be addressed using RFC 1918 private subnet addresses.
- QoS trust boundary extension to voice devices—QoS trust boundaries can be extended to voice devices without extending these trust boundaries and, in turn, QoS features to PCs and other data devices.
- Protection from malicious network attacks—Subnet access control, can provide protection for voice devices from malicious internal and external network attacks such as worms, denial-of- service (DoS) attacks, and attempts by data devices to gain access to priority queues.
- Ease of management and configuration—Separate VLANs for voice and data devices at the access layer provide ease of management and simplified QoS configuration.

Campus IP Routing Design

Most of the information in this section was taken directly from the campus CVD *Routed Access Design Guide*. The campus CVD *Routed Access Design Guide* advocates the use of Layer 3 routing to the access layer in order to obtain the highest possible network availability. Test results in the *HA Campus Recovery Analysis* document (available at http://www.cisco.com/en/US/netsol/ns815/networking_solutions_program_home.html) confirm the advantages of Layer 3 design over Layer 2 designs.

EIGRP Routing Protocol

The campus documents referenced above describe the use of both OSPF and EIGRP as appropriate choices for the campus routing protocol. The test results show convergence for both of these routing protocols to be essentially equivalent. For this chapter, we chose to implement EIGRP due to its superior ease of deployment.

Minimizing EIGRP Reconvergence Time

The length of time it takes for EIGRP or any routing protocol to restore traffic flows, after a network outage, within the campus is bounded by the following three main factors:

- The time required to detect the loss of a valid forwarding path
- The time required to determine a new best path
- The time required to update software and associated hardware forwarding tables

In the cases where the switch has redundant equal-cost paths, all three of these events are performed locally within the switch and controlled by the internal interaction of software and hardware. In the case where there is no second equal-cost path nor a feasible successor for EIGRP to use, the time required to determine the new best path is variable and primarily dependent on EIGRP query and reply propagation across the network. To minimize the time required to restore traffic in the case where a full EIGRP routing convergence is required, it is necessary to provide strict bounds on the number and range of the queries generated.

Although EIGRP provides a number of ways to control query propagation, the two main methods are route summarization and the EIGRP stub feature. In the routed access hierarchical campus design, it is necessary to use both of these mechanisms.

EIGRP Stub

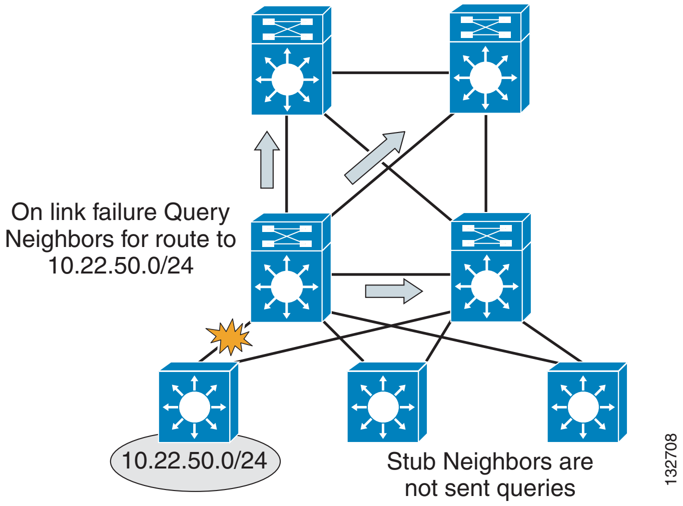
Configuring EIGRP stub on the Layer 3 access switches prevents the distribution switch from generating downstream queries.

Access Switch EIGRP Routing Process Stub Configuration

```
A4R-Top#sh run | beg router eigrp 100
router eigrp 100
 passive-interface default
 no passive-interface TenGigabitEthernet1/0/1
 no passive-interface TenGigabitEthernet2/0/1
 network 10.0.0.0
 no auto-summary
 eigrp router-id 10.33.9.19
 eigrp stub connected
```

By configuring the EIGRP process to run in “stub connected” state, the access switch advertises all connected subnets matching the network 10.0.0.0 0.255.255.255 range. It also advertises to its neighbor routers that it is a stub or non-transit router, and thus should never be sent queries to learn of a path to any subnet other than the advertised connected routes. With the design in Figure 6-2, the impact on the distribution switch is to limit the number of queries generated to 3 or less for any link failure.

Figure 6-2 EIGRP Stub Limits the Number of Queries Generated to 3


On link failure Query Neighbors for route to 10.22.50.0/24
10.22.50.0/24
Stub Neighbors are not sent queries
132708

To confirm that the distribution switch is not sending queries to the access switches, examine the EIGRP neighbor information for each access switch and look for the flag indicating queries being suppressed.

```
D3L#sh ip eigrp neigh det te 2/6
IP-EIGRP neighbors for process 100
H   Address                 Interface        Hold Uptime   SRTT   RTO  Q  Seq
                                             (sec)         (ms)       Cnt Num
```

```
3   10.33.3.3               Te2/6             2 00:00:15 1004  5000  0  36
   Version 12.2/1.2, Retrans: 0, Retries: 0
   Stub Peer Advertising ( CONNECTED REDISTRIBUTED ) Routes
   Suppressing queries
```

Configuring the access switch as a stub; router enforces hierarchical traffic patterns in the network. In the campus design, the access switch is intended to forward traffic only to and from the locally connected subnets. The size of the switch and the capacity of its uplinks are specified to meet the needs of the locally-connected devices. The access switch is never intended to be a transit or intermediary device for any data flows that are not to or from locally-connected devices. The hierarchical campus is designed to aggregate the lower speed access ports into higher speed distribution uplinks, and then to aggregate that traffic up into high-speed core links. The network is designed to support redundant capacity within each of these aggregation layers of the network, but not to support the re-route of traffic through an access layer. Configuring each of the access switches as EIGRP stub routers ensures that the large aggregated volumes of traffic within the core are never forwarded through the lower bandwidth links in the access layer, and also ensures that no traffic is ever mistakenly routed through the access layer, bypassing any distribution layer policy or security controls.

Each access switch in the routed access design should be configured with the EIGRP stub feature to aid in ensuring consistent convergence of the campus by limiting the number of EIGRP queries required in the event of a route recalculation, and to enforce engineered traffic flows to prevent the network from mistakenly forwarding transit traffic through the access layer.

For more information on the EIGRP stub feature, see the following URL:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/eigrpstb.html

Distribution Summarization

Configuring EIGRP stub on all of the access switches reduces the number of queries generated by a distribution switch in the event of a downlink failure, but it does not guarantee that the remaining queries are responded to quickly. In the event of a downlink failure, the distribution switch generates three queries; one sent to each of the core switches, and one sent to the peer distribution switch. The queries generated ask for information about the specific subnets lost when the access switch link failed. The peer distribution switch has a successor (valid route) to the subnets in question via its downlink to the access switch, and is able to return a response with the cost of reaching the destination via this path. The time to complete this event depends on the CPU load of the two distribution switches and the time required to transmit the query and the response over the connecting link. In the campus environment, the use of hardware-based CEF switching and GigE or greater links enables this query and response to be completed in less than a 100 msec.

This fast response from the peer distribution switch does not ensure a fast convergence time, however, EIGRP recovery is bounded by the longest query response time. The EIGRP process has to wait for replies from all queries to ensure that it calculates the optimal loop free path. Responses to the two queries sent towards the core need to be received before EIGRP can complete the route recalculation. To ensure that the core switches generate an immediate response to the query, it is necessary to summarize the block of distribution routes into a single summary route advertised towards the core.

```
D3L#sh run | begin TenGigabitEthernet2/1
interface TenGigabitEthernet2/1
 description from D3L to CL
 ip address 10.33.1.11 255.255.255.254
 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 3
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp-chain
 ip pim sparse-mode
 ip summary-address eigrp 100 10.33.48.0 255.255.240.0 5
 logging event link-status
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
```

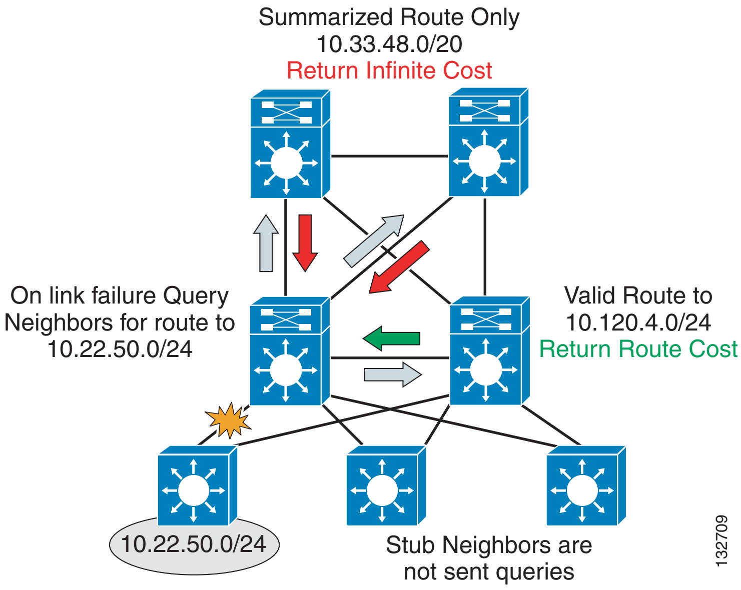
The summary-address statement is configured on the uplinks from each distribution switch to both core nodes. In the presence of any more specific component of the 10.33.0.0/16 address space, it causes EIGRP to generate a summarized route for the 10.33.0.0/16 network, and to advertise only that route upstream to the core switches.

```
CL#sh ip route 10.33.50.0
Routing entry for 10.33.48.0/20
  Known via "eigrp 100", distance 90, metric 3328, type internal
  Redistributing via eigrp 100
  Last update from 10.33.1.11 on TenGigabitEthernet2/5, 4w3d ago
  Routing Descriptor Blocks:
  * 10.33.1.13, from 10.33.1.13, 4w3d ago, via TenGigabitEthernet2/6
      Route metric is 3328, traffic share count is 1
      Total delay is 30 microseconds, minimum bandwidth is 1000000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
    10.33.1.11, from 10.33.1.11, 4w3d ago, via TenGigabitEthernet2/5
      Route metric is 3328, traffic share count is 1
      Total delay is 30 microseconds, minimum bandwidth is 1000000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
```

With the upstream route summarization in place, whenever the distribution switch generates a query for a component subnet of the summarized route, the core switches reply that they do not have a valid path (cost = infinity) to the subnet query. The core switches are able to respond within less than 100 msec if they do not have to query other routers before replying back to the subnet in question.

Figure 6-3 shows an example of summarization toward the core.

Figure 6-3 Summarization toward the Core Bounds EIGRP Queries for Distribution Block Routes



Using a combination of stub routing and summarizing the distribution block routes upstream to the core both limits the number of queries generated and bounds those that are generated to a single hop in all directions. Keeping the query period bounded to less than 100 msec keeps the network convergence similarly bounded under 200 msec for access uplink failures. Access downlink failures are the worst case scenario because there are equal-cost paths for other distribution or core failures that provide immediate convergence.

Route Filters

The discussion on EIGRP stub above noted that in the structured campus model, the flow of traffic follows the hierarchical design. Traffic flows pass from access through the distribution to the core and should never pass through the access layer unless they are destined to a locally attached device. Configuring EIGRP stub on all the access switches aids in enforcing this desired traffic pattern by preventing the access switch from advertising transit routes. As a complement to the use of EIGRP stub, Cisco recommends applying a distribute-list to all the distribution downlinks to filter the routes received by the access switches. The combination of “stub routing” and route filtering ensures that the routing protocol behavior and routing table contents of the access switches are consistent with their role, which is to forward traffic to and from the locally connected subnets only.

Cisco recommends that a default route (0.0.0.0 mask 0.0.0.0) be the only route advertised to the access switches.

```
D3L#sh run | begin router eigrp 100
router eigrp 100
...
 network 10.0.0.0
 distribute-list only-default out TenGigabitEthernet2/4
 distribute-list only-default out TenGigabitEthernet2/6
...
 eigrp router-id 10.33.9.8
!
...
!
ip access-list standard only-default
 permit 0.0.0.0
 remark redistribute default route to access layer stub-routers
```

No mask is required in the configuration of this access list because the assumed mask, 0.0.0.0, permits only the default route in the routing updates.

In addition to enforcing consistency with the desire for hierarchical traffic flows, the use of route filters also provides for easier operational management. With the route filters in place, the routing table for the access switch contains only the essential forwarding information. Reviewing the status and/or troubleshooting the campus network is much simpler when the routing tables contain only essential information.

```
A4L#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.33.3.24 to network 0.0.0.0

     2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2 is directly connected, Loopback2
     10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
C       10.33.49.0/24 is directly connected, Vlan49
C       10.33.48.0/24 is directly connected, Vlan48
C       10.33.3.4/31 is directly connected, TenGigabitEthernet1/1
```

```
C       10.33.3.24/31 is directly connected, TenGigabitEthernet1/2
C       10.33.9.20/32 is directly connected, Loopback1
D*EX 0.0.0.0/0 [170/3584] via 10.33.3.24, 3w4d, TenGigabitEthernet1/2
               [170/3584] via 10.33.3.4, 3w4d, TenGigabitEthernet1/1
```

If the network does not contain a default route, it may be acceptable to use an appropriate full network summary route in its place; that is, 10.0.0.0/8, or a small subset of summary routes that summarize all possible destination addresses within the network.

CEF Switching

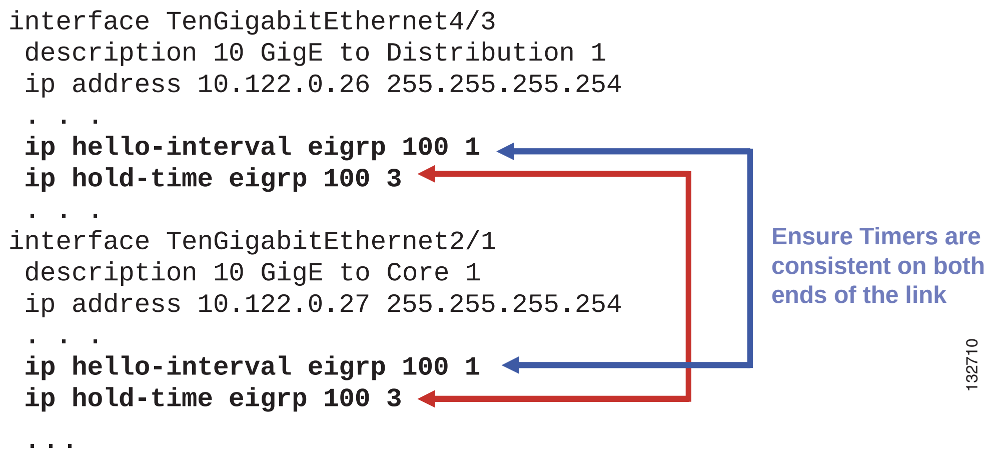
Per-destination load balancing is enabled by default when you enable CEF, and is the load balancing method of choice for most situations. Per-destination load balancing allows the router to use multiple paths to achieve load sharing. Packets for a given source-destination host pair are guaranteed to take the same path, even if multiple paths are available.

When you enable CEF or dCEF globally, all interfaces that support CEF are enabled by default.

Adjusting EIGRP timers

The recommended best practice for campus design is to use point-to-point fiber connections for all links between switches. Link failure detection via 802.3z and 802.3ae remote fault detection mechanism provide for recovery from most campus switch component failures. Cisco recommends in the Layer 3 campus design that the EIGRP hello and dead timers be reduced to 1 and 3 seconds, respectively (see Figure 6-4). The loss of hellos and the expiration of the dead timer provides a backup to the L1/2 remote fault detection mechanisms. Reducing the EIGRP hello and hold timers from defaults of 5 and 15 seconds provides for a faster routing convergence in the rare event that L1/2 remote fault detection fails to operate, and hold timer expiration is required to trigger a network convergence because of a neighbor failure.

Figure 6-4 Reducing EIGRP Hello and Dead Timers



```
interface TenGigabitEthernet4/3
 description 10 GigE to Distribution 1
 ip address 10.122.0.26 255.255.255.254
 . . .
 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 3
 . . .
interface TenGigabitEthernet2/1
 description 10 GigE to Core 1
 ip address 10.122.0.27 255.255.255.254
 . . .
 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 3
 . . .
```

Ensure Timers are consistent on both ends of the link

Campus Layer 2 Spanning Tree Protocol Design for Data Center

Much of the information in this section is summarized from the *Data Center Infrastructure 2.5 Design Guide*. For details, refer to this guide at: http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCI_SRND_2_5_book.html.

Data Center Layer Introduction

In the test network used for this document, the data center is used to connect network infrastructure devices such as Cisco Unified Communications Manager, Cisco Unified Unity, ACS, WCS, DNS, DHCP.

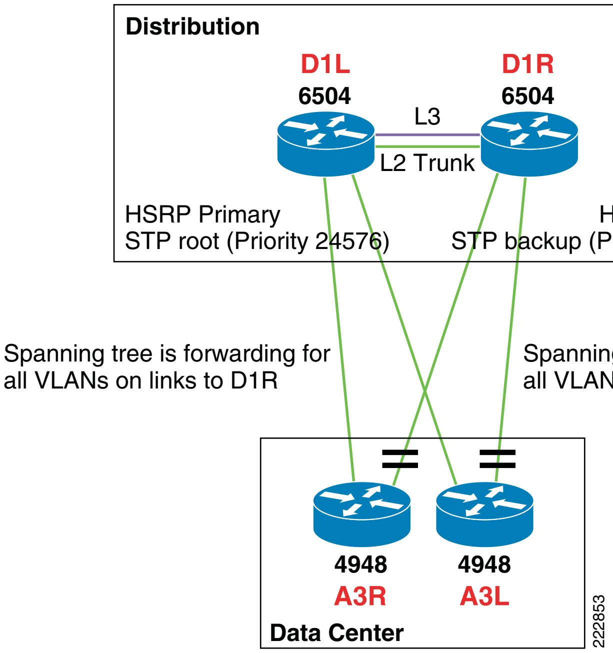
While the rest of the campus network uses Layer 3 routing (EIGRP) all the way to the access layer, the unique requirements of data center deployments require a Layer 2 connection to the data center. A Layer 2 access topology provides the following unique capabilities required in the data center:

- VLAN extension—The Layer 2 access topology provides the flexibility to extend VLANs between switches that are connected to a common aggregation module. This makes provisioning of servers to a particular subnet/VLAN simple, and without the worry of physical placement of the server in a particular rack or row.
- Layer 2 adjacency requirements—NIC teaming, high availability clusters, and database clusters are application examples that typically require NIC cards to be in the same broadcast domain (VLAN). The list of applications used in a clustered environment is growing, and Layer 2 adjacency is a common requirement.
- Custom applications—Many developers write custom applications without considering the Layer 3 network environment. This can create challenges in a Layer 3 IP access topology. These servers usually depend on Layer 2 adjacency with other servers and may require rewriting of code when changing IP addresses.
- Service modules—A Layer 2 access permits services provided by service modules or appliances to be shared across the entire access layer. Examples of this are when using the FWSM, CSM, and SSLSM. The active-standby modes of operation used by service modules require Layer 2 adjacency with the servers that use them.

Spanning Tree Triangle Looped Topology

The triangle looped topology utilized in the network used for this document is currently the most widely implemented in the enterprise data center. This topology provides a deterministic design that makes it easy to troubleshoot while providing a high level of flexibility (see Figure 6-5).

Figure 6-5 Triangle Looped Access Topology


Distribution
D1L
6504
D1R
6504
L3
L2 Trunk
HSRP Primary
STP root (Priority 24576)
HSRP Backup
STP backup (Priority 28672)
Spanning tree is forwarding for all VLANs on links to D1R
Spanning tree is blocked for all VLANs on links to D1R
4948
A3R
4948
A3L
Data Center
222853

In a triangle looped access layer design, it is desirable to align the spanning tree root, HSRP default gateway, and active service modules on the same aggregation switch, as shown in Figure 6-5. Aligning the access layer switch uplink that is in the forwarding state directly to the same switch that is the primary default gateway and active service module/appliance optimizes the traffic flows. Otherwise, traffic flows can hop back and forth between aggregation switches, creating undesirable conditions and difficulty in troubleshooting.

Lab Implementation Deviations from Standard Design Principals in the Data Center

In the network used for this chapter, multiple access layer blocks are connected to a single distribution block. This was done to reduce the number of distribution layer switches required. In a production deployment, the data center access-block would connect to a dedicated distribution block. In a production network, the distribution block dedicated to the data center access-block would run a variety of service modules supporting data center access. Example service modules include:

- Firewall Services Modules (FWSM)
- Secure Sockets Layer Services Modules (SSLSM)
- Content Switching Module (CSM)
- Intrusion Detection
- Network Analysis Module (NAM)
- Distributed denial-of-service attack protection (Cisco Guard)

While some combination of these would be expected in a production distribution layer block, our test network is not specifically focused on data center testing, and we have implement the network without any of these service modules.

Campus Quality of Service (QoS)

Much of the information in this section is summarized from the *Enterprise QoS Solution Reference Network Design Guide Version 3.3*. For details refer to this guide at: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html.

QoS refers to the set of tools and techniques used to manage network resources. QoS technologies allow different types of traffic to contend inequitably for network resources. Using QoS, some network traffic such as Voice, video, or critical data may be granted priority or preferential services from network devices; this prevents lower priority background traffic from degrading the quality of these strategic applications.

Until recently, QoS was not a great concern in the enterprise campus due to the large amount of available bandwidth as well as the asynchronous nature of data traffic and the ability of applications to tolerate the effects of buffer overflows and packet loss. However, with new applications such as voice and video, which are sensitive to packet loss and delay it is important to utilize quality of service features to protect high priority traffic.

Campus QoS Services Required

Access switches require the following QoS policies:

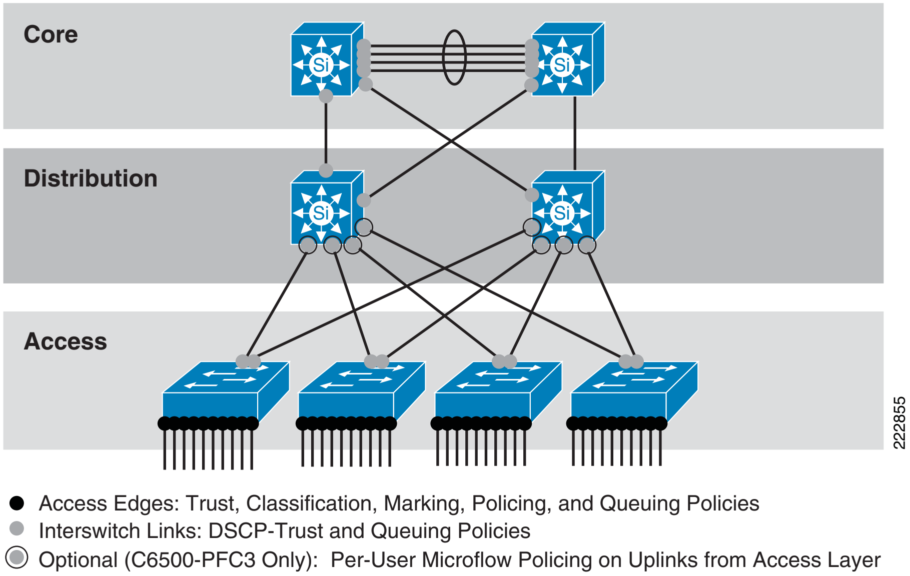
- Appropriate (endpoint-dependant) trust policies, and/or classification and marking policies
- Policing and markdown policies
- Queuing policies

Distribution and core switches require the following QoS policies:

- DSCP trust policies
- Queuing policies
- Optional per-user microflow policing policies (only on supported platforms)

These recommendations are summarized in Figure 6-6.

Figure 6-6 Typical Campus Oversubscription Ratios

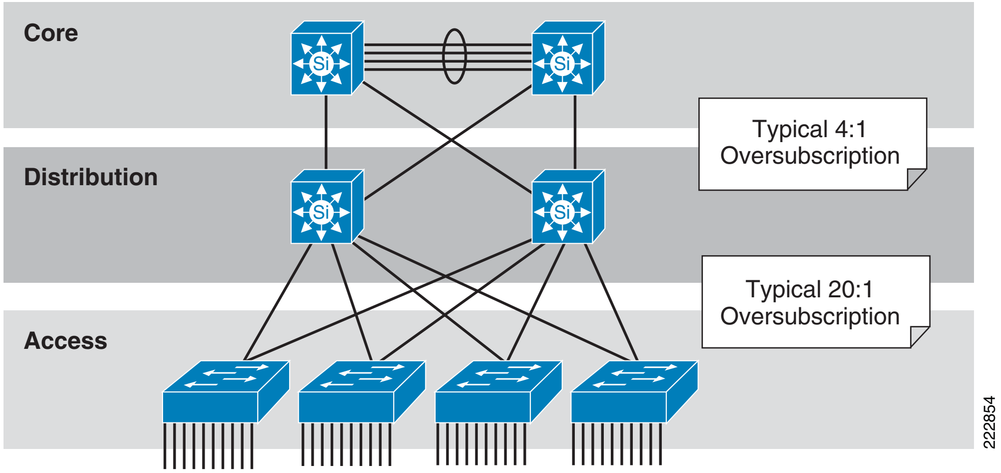

Core
Distribution
Access
Si
222855
● Access Edges: Trust, Classification, Marking, Policing, and Queuing Policies
● Interswitch Links: DSCP-Trust and Queuing Policies
◎ Optional (C6500-PFC3 Only): Per-User Microflow Policing on Uplinks from Access Layer

Campus QoS and Interface Queuing

Many campus links are underutilized. Some studies have shown that 95 percent of campus access layer links are used at less than 5 percent of their capacity. This means that you can design campus networks to accommodate oversubscription between access, distribution and core layers. Oversubscription allows for uplinks to be used more efficiently and more importantly, reduces the overall cost of building the campus network.

Common campus oversubscription values are 20:1 for the access-to-distribution layers and 4:1 for the distribution-to-core layers, as shown in Figure 6-7.

Figure 6-7 QoS Requirement within the Campus



The potential for congestion exists in campus uplinks because of oversubscription ratios and speed mismatches in campus downlinks (for example, GigabitEthernet to FastEthernet links). The only way to provision service guarantees in these cases is to enable advanced interface queuing at these points.

For a given input or output interface, Cisco IOS can manage multiple queues. Traffic of a particular priority is mapped into the appropriate queue for that traffic class. Cisco IOS queue scheduling algorithms can then be configured to service those queues, giving more priority to servicing the queues containing higher priority traffic. In this way, higher priority traffic is protected from queue overruns caused by lower priority traffic.

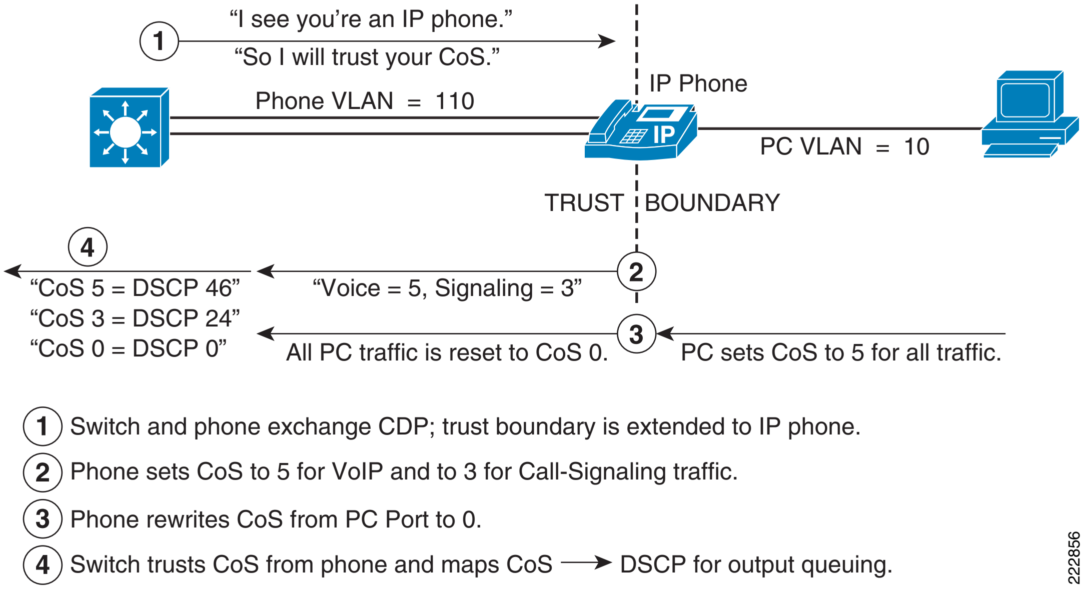
QoS and Wired IP Phones

This section is specific to wired Ethernet-attached IP phone. Wireless LAN IP phones such as the Cisco 7921G use a different QoS procedure and are discussed in Chapter 10, "Cisco Unified IP Phone 7921 Implementation for Voice over WLAN."

Cisco wired IP phones perform an intelligent exchange of information between the phone and the switchport it is plugged into using Cisco Discovery Protocol (CDP). When the switch discovers a Cisco IP phone, it can extend QoS trust to it dynamically.

Figure 6-8 shows a conditional trust boundary extension granted to an IP phone that has passed a CDP exchange.

Figure 6-8 Conditionally Trusted Endpoint Trust Boundary Extension and Operation


1
"I see you're an IP phone."
"So I will trust your CoS."
Phone VLAN = 110
IP Phone
IP
PC VLAN = 10
TRUST BOUNDARY
4
"CoS 5 = DSCP 46"
"CoS 3 = DSCP 24"
"CoS 0 = DSCP 0"
"Voice = 5, Signaling = 3"
2
3
All PC traffic is reset to CoS 0.
PC sets CoS to 5 for all traffic.
1 Switch and phone exchange CDP; trust boundary is extended to IP phone.
2 Phone sets CoS to 5 for VoIP and to 3 for Call-Signaling traffic.
3 Phone rewrites CoS from PC Port to 0.
4 Switch trusts CoS from phone and maps CoS → DSCP for output queuing.
222856

The sequence shown in Figure 6-8 is the following:

Step 1 Switch and phone exchange CDP; trust boundary is extended to IP phone.

Step 2 Phone sets CoS to 5 for VoIP and to 3 for call signaling traffic.

Step 3 Phone rewrites CoS from PC to 0.

Step 4 Switch trusts CoS from phone and maps CoS to DSCP for output queuing.

AutoQoS and VoIP

When the main business objective of the QoS deployment is to enable QoS for IP Telephony only (i.e., without Scavenger-class QoS), then the network administrator may choose to take advantage of the Cisco AutoQoS VoIP feature.

AutoQoS VoIP is essentially an intelligent macro that enables an administrator to enter one or two simple AutoQoS commands to enable all the appropriate features for the recommended QoS settings for VoIP and IP telephony for a specific platform and/or a specific interface.

AutoQoS VoIP automatically configures the best-practice QoS configurations (based on previous Cisco Enterprise QoS SRNDs) for VoIP on Cisco Catalyst switches and IOS routers. By entering one global and/or one interface command (depending on the platform), the AutoQoS VoIP macro then would expand these commands into the recommended VoIP QoS configurations (complete with all the calculated parameters and settings) for the platform and interface on which the AutoQoS VoIP macro is applied.

For example, on Cisco Catalyst switches, AutoQoS performs the following automatically:

- Enforces a conditional-trust boundary with any attached Cisco IP phones
- Enforces a trust boundary on Catalyst switch access ports and uplinks/downlinks
- Modifies CoS-to-DSCP (and IP Precedence-to-DSCP) mappings, as required
- Enables Catalyst strict priority queuing for voice (CoS 5/DSCP EF) and preferential queuing for Call-Signaling traffic (CoS 3/DSCP CS3) * Enables best-effort queuing for all other data (CoS 0/DSCP 0) traffic
- Modifies queue admission criteria (such as CoS-to-queue mapping)
- Modifies queue sizes and queue weights, where required

QoS Policing

At the time of writing, classification using a port trust state (for example, mls qos trust [cos | dscp | ip-precedence] and a policy map (for example, service-policy input policy-map-name) are mutually exclusive on the Catalyst 2970/3560/3750. The last one configured overwrites the previous configuration. This limitation is to be addressed; consult the latest Catalyst 2970/3560/3750 QoS documentation for updates on this limitation.

Because of the above limitation, policing will not be discussed in the configuration section of this document. For detailed guidance on policing configuration, refer to the *Enterprise QoS Solution Reference Network Design Guide Version 3.3* at the following URL:
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html

Campus Multicast

For complete details on the recommended campus multicast design, see the Cisco AVVID Network Infrastructure IP Multicast Design SRND at the following URL: http://www.cisco.com/application/pdf/en/us/guest/tech/tk363/c1501/ccmigration_09186a008015e7cc.pdf.

When designing multicast networking, a routed access design has advantages over a design that has Layer 2 to the distribution layer. In the Layer 2 design, there are two routers on the same subnet as the multicast hosts. This results in the following;

- One of the routers needs to be elected the PIM DR and IGMP querier
- One of the routers needs to be elected the HSRP active node
- One of the routers needs to be elected the Layer 2 root bridge

For each specific VLAN The root bridge, the HSRP active node, and the PIM DR should all be on the same distribution switch.

In the routed access design, this need for synchronized configuration is removed because there is only one router on the local segment, which by default results in synchronization of the unicast and multicast traffic flows. Additionally, with the migration of the multicast router from the distribution to the access, there is no longer a need to tune the PIM hello timers to ensure rapid convergence between the distribution nodes in the case of a failure. The same remote fault indicator mechanisms that trigger rapid unicast convergence drive the multicast software and hardware recovery processes, and there is no need for Layer 3 detection of path or neighbor failure across the Layer 2 access switch. The presence of a single router for each access VLAN also removes the need to consider non-reverse path forwarding (non-RPF) traffic received on the access side of the distribution switches. A multicast router drops any multicast traffic received on a non-RPF interface. If there are two routers for a subnet, the DR forwards the traffic to the subnet, and the non-DR receives that traffic on its own VLAN interface where it fails the RPF check and so must be dropped

Multicast Traffic Flows and Router Functions

In the Layer 3 access design, there is a single router on the access subnet and no non-RPF traffic flows. Although the current generation of Cisco Catalyst switches can process and discard all non-RPF traffic in hardware with no performance impact or access list configuration required, the absence of non-RPF traffic simplifies operation and management.

The following summarizes the campus multicast configuration implementation:

- The access layer switches have IGMP snooping enabled.
- The RPs are located on the two core layer switches (RPs should be close to the multicast sources. In our lab the core routers represented the best location.).
- PIM-SM is configured on all access layer, distribution layer, and core-layer switches.
- Anycast RP is configured for fast recovery of IP multicast traffic.
- PIM-SM and MSDP are enabled on all core layer switches. (auto RP is not used due to its reliance on PIM-sparse-dense)
- Each access layer switch points to the anycast RP address as its RP.
- MSDP is used to synchronize source active (SA) state between the core switches.

Campus Security

The Campus Security section is focused on the Catalyst Integrated Security Features (CISF) features found in the access layer switches connecting end-user devices to the network.

Much of the information in this section is summarized from *Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x* at the following URL:
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/6x/uc6_0.html

Refer to the above document as well as the relevant access-layer switch documentation for more details.

Catalyst Integrated Security Features (CISF)

Layer 2 switched environments can prove easy targets for security attacks. These attacks exploit normal protocol processing such as a switches' ability to learn MAC addresses, end-station Media Access Control (MAC) address resolution through Address Resolution Protocol (ARP) or Dynamic Host Configuration Protocol (DHCP) IP address assignments.

The rich set of integrated security features on Cisco Catalyst Switches (CISF) protect your critical network infrastructure with easy-to-use tools that effectively prevent the most common—and potentially damaging— Layer 2 security threats.

Port Security

Function

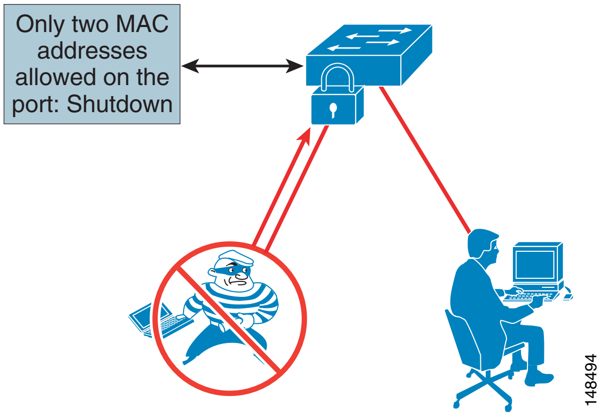
Shuts down MAC address-flooding attacks .

How It Works

A classic attack on a switched network is a MAC content-addressable memory (CAM) flooding attack. This type of attack floods the switch with so many MAC addresses that the switch does not know which port an end station or device is attached to. When the switch does not know which port a device is attached to, it broadcasts the traffic destined for that device to the entire VLAN. In this way, the attacker is able to see all traffic that is coming to all the users in a VLAN.

Port security limits the number of MAC addresses allowed to access individual switch ports thus protecting against MAC flooding attacks from hacker tools such as macof (see Figure 6-9).

Figure 6-9 Limited Number of MAC Addresses Prevents Rogue Network Extensions

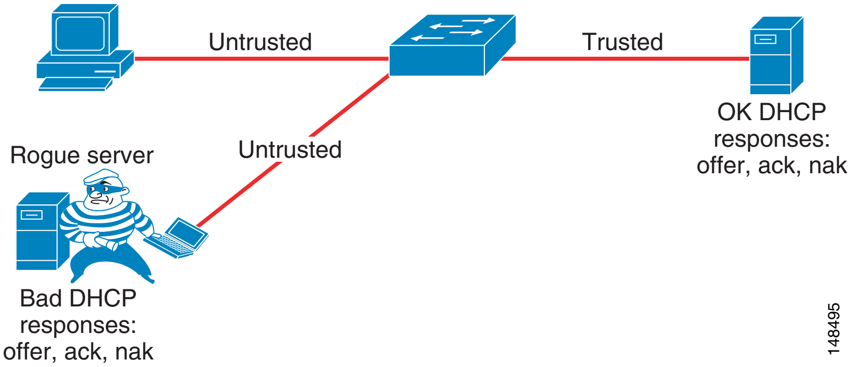


DHCP Snooping

Function

Prevent rogue DHCP server attacks, DHCP starvation attacks, create client binding information used by additional CISF tools

Figure 6-10 Using DHCP Snooping


Untrusted
Trusted
OK DHCP responses: offer, ack, nak
Rogue server
Untrusted
Bad DHCP responses: offer, ack, nak
148495

DHCP Snooping: Prevent Rogue DHCP Server Attacks

How It Works

Dynamic Host Configuration Protocol (DHCP) Snooping prevents a non-approved DHCP or rouge DHCP server from handing out IP addresses on a network by blocking all replies to a DHCP request unless that port is allowed to reply. When enabled, DHCP Snooping treats all ports in a VLAN as untrusted by default. An untrusted port is a user-facing port that should never make any reserved DHCP responses. If an untrusted DHCP-snooping port makes a DHCP server response, it will be blocked from responding. Therefore, rogue DHCP servers will be prevented from responding. However, legitimately attached DHCP servers or uplinks to legitimate servers must be trusted.

DHCP Snooping: Prevent DHCP Starvation Attacks

How It Works

DHCP address scope starvation attacks from tools such as Gobbler are used to create a DHCP denial-of-service (DoS) attack. Because the Gobbler tool makes DHCP requests from different random source MAC addresses, you can prevent it from starving a DHCP address space by using port security to limit the number of MAC addresses. However, a more sophisticated DHCP starvation tool can make the DHCP requests from a single source MAC address and vary the DHCP payload information. With DHCP Snooping enabled, untrusted ports will make a comparison of the source MAC address to the DHCP payload information and fail the request if they do not match

DHCP Snooping: Binding Information

How It Works

Another function of DHCP Snooping is to record the DHCP binding information for untrusted ports that successfully get IP addresses from the DHCP servers. The binding information is recorded in a table on the Cisco Catalyst switch. The DHCP binding table contains the IP address, MAC address, lease length, port, and VLAN information for each binding entry. The binding information from DHCP Snooping remains in effect for the length of the DHCP binding period set by the DHCP server (that is, the DHCP lease time). The DHCP binding information is used to create dynamic entries for Dynamic ARP Inspection (DAI) to limit ARP responses for only those addresses that are DHCP-bound. The DHCP binding information is also used by the IP source guard to limit sourcing of IP packets to only those addresses that are DHCP-bound.

Dynamic ARP Inspection

Function

Adds security to ARP using DHCP snooping table.

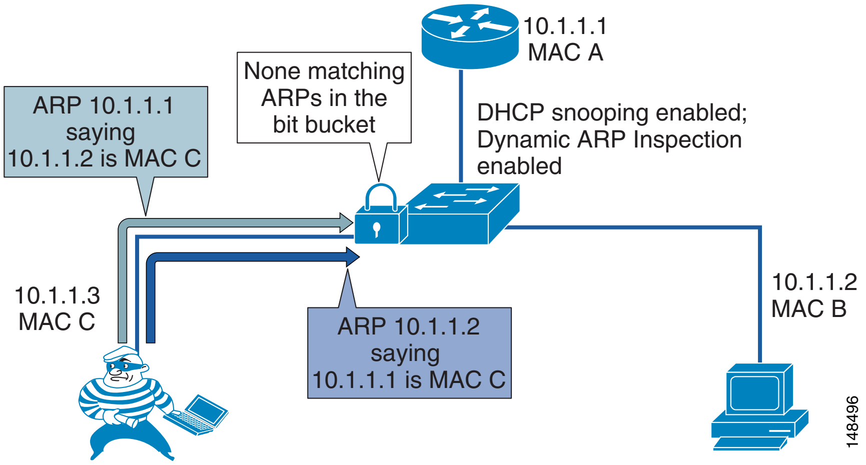
How It Works

Dynamic Address Resolution Protocol (ARP) Inspection (DAI) is a feature used on the switch to prevent Gratuitous ARP attacks on the devices plugged into the switch and on the router.

Gratuitous ARP can be exploited by malicious programs that want to illegitimately take on the identity of another station. When a malicious station redirects traffic to itself from two other stations that were talking to each other, the hacker who sent the GARP messages becomes the man-in-the-middle. Hacker programs such as ettercap do this with precision by issuing "private" GARP messages to specific MAC addresses rather than broadcasting them. In this way, the victim of the attack does not see the GARP packet for its own address. Ettercap also keeps its ARP poisoning in effect by repeatedly sending the private GARP messages every 30 seconds.

Dynamic ARP Inspection (DAI) is used to inspect all ARP requests and replies (gratuitous or non-gratuitous) coming from untrusted (or user-facing) ports to ensure that they belong to the ARP owner. The ARP owner is the port that has a DHCP binding which matches the IP address contained in the ARP reply. ARP packets from a DAI trusted port are not inspected and are bridged to their respective VLANs.

Figure 6-11 Using DHCP Snooping and DAI to Block ARP Attacks:


10.1.1.1
MAC A
None matching ARPs in the bit bucket
ARP 10.1.1.1 saying 10.1.1.2 is MAC C
DHCP snooping enabled; Dynamic ARP Inspection enabled
10.1.1.3
MAC C
ARP 10.1.1.2 saying 10.1.1.1 is MAC C
10.1.1.2
MAC B
148496

IP Source Guard

Function

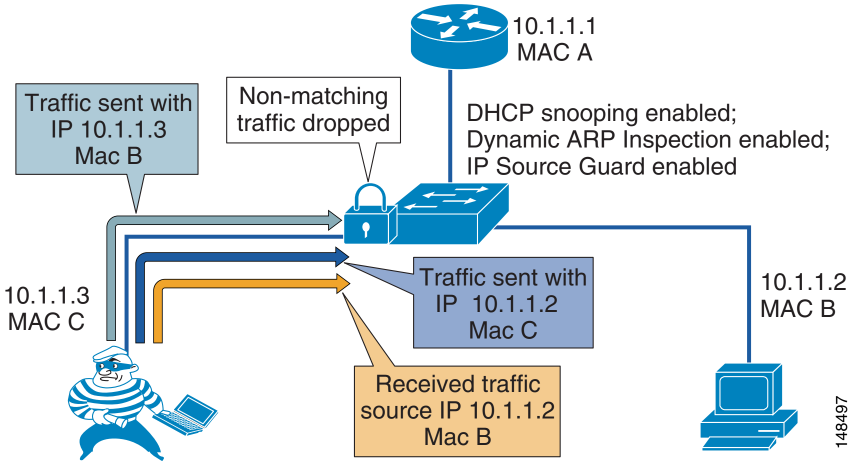
Prevents IP host spoofing.

How It Works

IP address spoofing is commonly used to perform DoS attacks on a second party. A simple example of this occurs when an attacker pings a third-party system while sourcing the IP address of the second party that is being attacked (see Figure 6-12). The ping response will be directed to the second party from the third-party system. Aggressive SYN-flooding originating from spoofed IP addresses is another common type of attack used to overwhelm a server with TCP half-sessions.

The IP Source Guard (IPSG) feature, when invoked, dynamically creates an ACL based on the contents of the DHCP Snooping binding table. This ACL ensures that traffic is sourced from the IP address issued at DHCP binding time and prevents any traffic from being forwarded by other spoofed addresses. While DHCP Snooping is a prerequisite for IP Source Guard, DAI is not. However, Cisco recommend that you enable DAI in addition to IP Source Guard to prevent ARP-poisoning man-in-the-middle attacks in addition to IP address spoofing.

Figure 6-12 Using IP Source Guard to Prevent Address Spoofing:


10.1.1.1
MAC A
Traffic sent with IP 10.1.1.3 Mac B
Non-matching traffic dropped
DHCP snooping enabled;
Dynamic ARP Inspection enabled;
IP Source Guard enabled
10.1.1.3
MAC C
Traffic sent with IP 10.1.1.2 Mac C
10.1.1.2
MAC B
Received traffic source IP 10.1.1.2 Mac B
148497

Network Time Services

An essential element of network management, troubleshooting, and security operations is to have all network elements (including routers switches and servers) synchronized to a common clock source.

Network Time Protocol (NTP) is most commonly used to synchronize clocks in network equipment. NTP provides accuracies typically within a millisecond on LANs and up to a few tens of milliseconds on WANs.

By synchronizing the clocks across the network it is possible to examine the exact sequence in which events occurred. This ability to analyze and correlate the sequence of events across multiple network elements makes it much easier to determine the root cause of network problems or security issues.

The configuration section of this document shows the commands used in our network to have NTP synchronize to an external time source. In most production the external time source used would be redundant, dedicated hardware that synchronizes via a GPS receiver to a clock source that is itself directly synchronized to an atomic clock.

NTP links

- http://support.ntp.org/bin/view/Main/WebHome
- http://en.wikipedia.org/wiki/Network_Time_Protocol
- http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml
- http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_white_paper0900aecd8037fdb5.shtml
- http://www.symmetricom.com/
- http://www.meinberg.de/english/products/

UniDirectional Link Detection (UDLD)

Use UDLD to protect against one-way up/up connections. In fiber topologies where fiber optic interconnections are used, which is common in a campus environment, physical misconnections can occur that allow a link to appear to be up/up when there is a mismatched set of transmit/receive pairs. When such a physical misconfiguration occurs, protocols such as EIGRP or STP can cause network instability. UDLD detects these physical misconfigurations and disables the ports in question

Configuration

Software versions used in test network

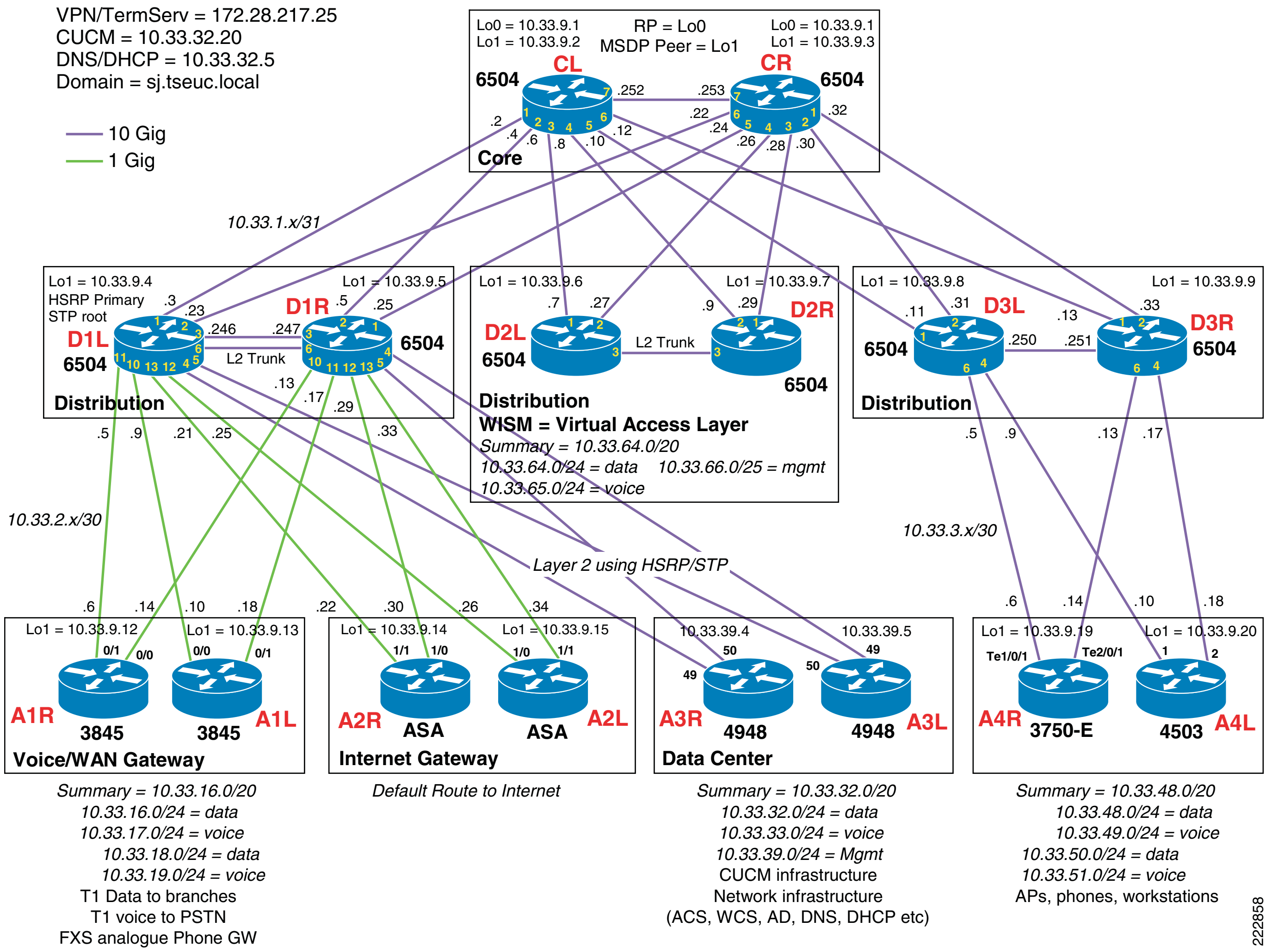
Table 6-1 Software Releases Used in Testing

Platform	Role	SW Version
6504	Campus Core	12.2(18)SXF9
6504	Campus Distribution	12.2(18)SXF9
6504	WLAN	12.2(18)SXF9
3845	Voice WAN gateway	12.4(15)T1
ASA	Internet gateway	7.2(2)
4948	Data center	12.2(25)EWA8
4503	Access	12.2(37)SG
3750-E	Access	12.2(37)SE1
2821	Branch Router	12.4(15)T1

Lab Network used for Configuration Examples

Throughout the configuration section of this chapter, many configuration examples are shown from actual routers and switches used in the lab build-out used to test and write this document. Figure 6-13 provides a detailed view of the lab network, that will assist in understanding the configuration examples below.

Figure 6-13 TSE VoWLAN campus Architecture Detailed



Campus EIGRP Routing Configuration

Campus EIGRP Routing Configuration Common to all Routers

Table 6-2 shows the configuration commands that are common to all routers/switches in the example network. The IP addressing is based on the network diagram shown in Figure 6-1.

Table 6-2 Configuration Common to all Routers

Configuration Command (Switch D3L used for example configuration)	Description of Configuration
`ip cef distributed`	`Enable CEF`

`key chain eigrp-chain`
`key 100`
`key-string cisco`
	`Configure EIGRP authentication paramaters`
	`(Ensure a more secure key is used in production deployments`

Table 6-2 Configuration Common to all Routers (continued)

interface loopback1 description unique /32 interface on every router ip address 10.33.9.8 255.255.255.255	Provides a unique IP address for every router. Can be used by services like NTP and multicast. Also a good telnet address.
spanning-tree mode rapid-pvst	Enable spanning tree as a fail-safe practice
router eigrp 100 passive-interface Loopback1 network 10.0.0.0 no auto-summary eigrp router-id 10.33.9.8	* Enable EIGRP; this example uses AS 100, but any valid AS number can be substituted * Passive all interfaces not intended to form EIGRP neighbors. Add any other non-routing interfaces. * Define the networks to route using EIGRP * Ensure all subnets are routed unless explicitly summerized * Explicitly configure the EIGRP router id as a best practice. Use the Loopback1 address for this.
A similiar configuration is required on all links between core and distribution or distribution and access layers interface TenGigabitEthernet2/2 description from D3L to CR ip address . 10.33.1.31 255.255.255.254 ip hello-interval eigrp 100 1 ip hold-time eigrp 100 3 ip authentication mode eigrp 100 md5 ip authentication key-chain eigrp 100 eigrp-chain load-interval 30 carrier-delay msec 0 mls qos trust dscp logging event link-status	* Use of /31 addressing on point to point links optimizes use of IP address space in the campus * Tune EIGRP timers on interfaces between the Core and Distribution layers for faster convergence. Reduce EIGRP hello and hold timers to 1 and 3 seconds. In a point-point L3 campus design the EIGRP timers are not the primary mechanism used for link and node failure detection (physical detection of fiber breaks are). They are intended to provide a fail-safe mechanism only. * enable eigrp authentication on this interface * Reduce load-interval to set the length of time (in seconds; default is 300) for which data is used to compute load statistics on this interface * Reduce carrier delay to 0. Tuning carrier delay no longer has an impact on GigE or 10GigE interfaces but is recommended to be configured as a best practice for network operational consistency * Configure trust DSCP to provide for maximum granularity of internal QoS queuing

Note The base EIGRP configuration shown in the section above is common to all routers.

EIGRP Configuration Specific to Core Routers

There is no special routing policy applied to the core routers; their configuration is left as simple as possible so as to not interfere with their primary function of routing packets.

EIGRP Configuration Specific to Distribution Routers

Table 6-3 EIGRP Configuration Specific to Distribution Routers

Configuration Command (Switch D3L used for example configuration)	Description of Configuration
ip access-list standard only-default permit 0.0.0.0	Access-list used by eigrp to only send default route to access layer

Table 6-3 EIGRP Configuration Specific to Distribution Routers (continued)

`router eigrp 100`
`distribute-list only-default out TenGigabitEthernet2/4`
`distribute-list only-default out TenGigabitEthernet2/6`
	Apply a distribute list filtering all routes other than select default(s) to the access switches

On the interfaces to the core routers only
`Interface TenGigabitEthernet2/1`
`ip summary-address eigrp 100 10.33.48.0 255.255.240.0 5`
	Advertise a summary address for the entire distribution block upstream to the core
	The "5" parameter is the administrative distance which is used to advertise a summary without installing it in the routing table.

EIGRP Configuration Specific to Access Routers

Table 6-4 EIGRP Configuration Specific to Access Routers

Configuration Command (Switch A4R used for example configuration)	Description of Configuration

`router eigrp 100`
`passive-interface default`
`no passive-interface TenGigabitEthernet2/0/1`
`no passive-interface TenGigabitEthernet2/0/1`
`eigrp stub connected summary`
	* Configure EIGRP as an EIGRP stub router; advertising connected routes upstream to the distribution.
	* Make passive-interface the default and explicitly remove it from the links to the distribution

Campus Layer 2 Spanning Tree Protocol Design for Data Center Configuration

Table 6-5 Layer 2 Configuration Specific to Distribution Switch/Routers

Configuration Command (Switch D1L used for example configuration)	Description of Configuration

`vtp domain datacenter`
`vtp mode transparent`
	Define a VTP domain, and make all switches in it transparent mode

`spanning-tree mode rapid-pvst`
`no spanning-tree optimize bpdu transmission`
`spanning-tree extend system-id`
`spanning-tree pathcost method long`
`spanning-tree vlan 1-4094 priority 24576`
	Configure Rapid Per-VLAN Spanning tree. Make one of the Distribution layer switches the STP root by configuring it with priority 24576. Make the other Distribution layer switch the backup STP root by configuring it with priority 28672

`router eigrp 100`
`passive-interface`
	Ensure routing updates are not sent out the Layer 2 VLANs

`vlan 32`
`name DataCenter-Data32`
	define each VLAN

Table 6-5 Layer 2 Configuration Specific to Distribution Switch/Routers

interface Vlan32 description DataCenter-Data32 ip address 10.33.32.2 255.255.255.0 no ip redirects standby 1 ip 10.33.32.1 standby 1 timers 1 3 standby 1 priority 120 standby 1 preempt delay minimum 60	Configure each of the VLANs servicing the datacenter access layer with IP address. Make the same router STP root and HSRP primary by configuring it with priority 120. Make the other Distribution layer switch the HSRP secondary by configuring it with priority 115
interface TenGigabitEthernet3/6 description Layer2_connection_TO_D1R switchport switchport trunk encapsulation dot1q switchport trunk native vlan 2 switchport trunk allowed vlan 2,32-35 switchport mode trunk no ip address logging event link-status	Configure the Layer 2 interface between the 2 Distribution layer switches and between the Distrbution layer switches and the Data Centers access layer switches. Trunk the Data Center VLANs

Table 6-6 Layer 2 Configuration Specific to Data Center L2 Access Switches

Configuration Command (Switch A3R used for example configuration)	Description of Configuration
vtp domain datacenter vtp mode transparent	Define a VTP domain, and make all switches in it transparent mode
spanning-tree mode rapid-pvst spanning-tree loopguard default spanning-tree portfast bpduguard default no spanning-tree optimize bpdu transmission spanning-tree extend system-id spanning-tree pathcost method long	Configure spanning tree. The priority statements on the distribution layer switches will ensure the one of them will always be the root
vlan 32 name DataCenter-Data32	define each VLAN
interface GigabitEthernet1/1 description All Ports assigned to access VLAN 32 switchport access vlan 32 switchport mode access no cdp enable spanning-tree portfast	Assign each access port to a VLAN
interface TenGigabitEthernet1/49 description to_D1L switchport trunk encapsulation dot1q switchport trunk native vlan 2 switchport mode trunk logging event link-status	Configure each of the uplinks to the distribution layer
interface Vlan32 ip address 10.33.32.4 255.255.255.0 exit ip default-gateway 10.33.32.1 ip route 0.0.0.0 0.0.0.0 10.33.32.1	Give 1 of the VLANs an IP address so the switch can be managed via Telnet and SNMP, and so that the switch can connect to the NTP server Define a default gateway and default route so the switch can communicate with IP devices on different subnets

Campus QoS Configuration

The **auto qos voip** commands shown below are macros. They generate many configuration statements that configure CoS-to-DSCP mappings, interface queue discard thresholds, the mapping of specific CoS and DSCP values to a particular queue and threshold, and queue buffer sizes as well as generating the specific interface QoS trust policies. The commands generated can be observed by entering the **debug auto qos** command before beginning the configuration.

Table 6-7 Campus QoS Configuration Common to all Switch/Routers

Configuration Command	Description of Configuration
debug auto qos	Enable debugging for auto-QoS. When debugging is enabled, the switch displays the QoS configuration that is automatically generated when auto-QoS is enabled.
For uplinks/downlinks (interfaces connected directly to other switch/routers) interface *interface-id* auto qmls qos trust dscp end	* Specify the switch port identified as connected to a trusted switch or router, and enter interface configuration mode * Configure inter-switch links to trust the DSCP settings that have been marked by auto-qos at the network edge. * Return to privileged EXEC mode.

Table 6-8 Campus QoS Configuration for Access Layer Switch/Routers

Configuration Command	Description of Configuration
debug auto qos	Enable debugging for auto-QoS. When debugging is enabled, the switch displays the QoS configuration that is automatically generated when auto-QoS is enabled.
For interfaces connected directly to Cisco IP Phones cdp enable interface *interface-id* auto qos voip cisco-phone exit	* Enable CDP globally. By default, it is enabled. * Specify the switch port connected to the Cisco IP Phone, and enter interface configuration mode. * Enable auto-QoS on the port, and specify that the port is connected to a Cisco IP Phone. The QoS labels of incoming packets are trusted only when the Cisco IP Phone is detected. * Return to global configuration mode. * Repeat for as many ports as are connected to Cisco IP Phones.
For interfaces connected to directly Cisco LWAPP APs interface *interface-id* auto qos voip trust mls qos trust dscp exit	* Specify the switch port connected to the Cisco LWAPP, and enter interface configuration mode. * Enable auto-QoS on the port, and specify that the port is to trust QoS and prioritize voice traffic. * With the auto qos voip trust macro, in addition to setting interface queuing parameters, the switch automatically sets the ingress classification to trust the CoS value received in the packet on a nonrouted port or to trust the DSCP value received in the packet on a routed port. We use this macro to have the interface queuing parameters automatically set, but an LWAPP AP sets its QoS values in DSCP bits not CoS bits, so we need to change the generated *mls qos trust cos* to *mls qos trust dscp* * Return to global configuration mode. * Repeat for as many ports as are connected to Cisco LWAPP APs.

Campus Routed Multicast configuration

This section provides the configuration required for the campus network with the exception of the connection to the datacenter where slightly different configuration is required for the Layer 2 connections from the distribution to the access layers.

Campus Multicast Configuration Common to all Multicast-enabled Routers

The voice/WAN Gateway routers and the Internet Gateway routers are not multicast enabled.

Table 6-9 Campus Multicast Configuration Common to all Routers

Configuration Command (sample multicast groups used for illustration purposes)	Description of configuration
ip multicast-routing	Globally enable multicast
interface Te1/0/1 ip pim sparse-mode	Enable PIM on all multicast-enabled interfaces (including VLAN interfaces)
interface Loopback2 description Garbage-CAN RP ip address 2.2.2.2 255.255.255.255	Define a local loopback address to provide a sink hole route point for invalid multicast groups
ip access-list standard GOOD-IPMC permit 239.1.2.3 0.0.0.0 permit 230.230.0.0 0.0.255.255 permit 239.192.240.0 0.0.3.255 permit 239.192.248.0 0.0.3.255	Explicitly define what multicast groups to be forwarded to the RP -- permit LWAPP multicast tunnel -- Permit Vocera traffic -- Permit music on hold traffic -- Permit IPTV medium-rate traffic
ip pim rp-address 10.33.9.1 GOOD-IPMC override	Send all traffic permitted by the GOOD-IPMC access-list to the anycast RP address
ip pim rp-address 2.2.2.2	Send all multicast traffic that does not match the multicast groups defined in GOOD-IPMC access-list to the locally-defined Garbage-Can RP.

Campus Multicast Configuration for Core Routers

Table 6-10 Campus Multicast Configuration for Core Routers

Configuration Command (Switch CL used for example configuration)	Description of Configuration
interface Loopback0 description shared MSDP local peer address ip address 10.33.9.1 255.255.255.255	Loopback0 is the shared IP address that is used by all routers providing RP functionality. All RPs can use this address concurrently. The MSDP protocol keeps the RPs in synch with SA information. The DRs use whichever RP its unicast routing protocol finds closest. The unicast routing protocol will automatically provide failover if a RP fails.
interface Loopback1 description unique router address (for MSDP/RP and other uses) ip address 10.33.9.2 255.255.255.255 ip pim sparse-mode	Loopback1 is the unique IP address used to keep the redundant RPs in synch by exchanging Source Active (SA) information via the MSDP protocol.

Table 6-10 Campus Multicast Configuration for Core Routers (continued)

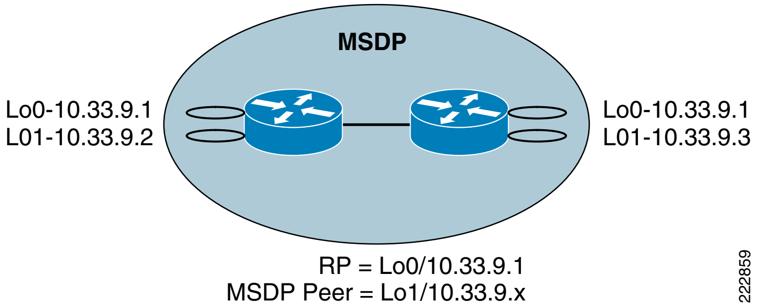
`ip msdp peer 10.33.9.3 connect-source Loopback1`	Multicast Source Distribution Protocol (MSDP) is the protocol that ensures that all RPs which are sharing a single IP address receive updates from each other (as muticast sources join one or other of the RPs). The command defines the peer routers MSDP address (its loopback1) and uses this routers loopback1 as the source IP address
`ip msdp cache-sa-state`	Cache SA-pairs learnt from MSDP peer (even when there is no registered receiver for that multicast group); this sacrifices some router memory in order to reduce join latency.
`ip msdp originator-id Loopback1`	Tells an MSDP speaker that originates an SA message to use the IP address of the Loopback1 as the RP address in the SA message

`ip access-list extended PERMIT-SOURCES`
`permit ip 10.33.66.0 0.0.0.255 239.1.2.3 0.0.0.0`
`permit ip 10.33.65.0 0.0.0.255 230.230.0.0 0.0.255.255`
`permit ip 10.33.32.0 0.0.0.255 239.192.240.0 0.0.3.255`
`permit ip 10.33.32.0 0.0.0.255 239.192.248.0 0.0.3.255`
	Example list of multicast source/groups permitted to register with the RPs
	-- permit LWAPP multicast tunnel from controller management interfaces
	-- Permit Vocera traffic from WLAN Voice VLAN on controller
	-- Permit music on hold from the Data Center access VLAN
	-- Permit IPTV medium-rate traffic from the Data Center access VLAN

`ip pim accept-register list PERMIT-SOURCES`	Configure the RPs to only accept register messages from sources explicity defined in the PERMIT-SOURCES access list

Figure 6-14 provides a logical view of the MSDP configuration of the core switches.

Figure 6-14 Logical View of MSDP Configuration



Campus Multicast Configuration for Distribution Routers

No multicast-specific configuration is required on distribution routers.

Campus Multicast Configuration for Access Routers

Table 6-11 Campus Multicast configuration for Access Routers and

Configuration Command (Switch A4R used for example configuration)	Description of Configuration
`ip pim spt-threshold infinity`	Reduces multicast state (S,G) from the leaf routers by keeping traffic on the shared tree. (Optional)

`interface VLAN 50`
`ip pim query-interval 250 msec`
	Increase the speed with which the router will detect other multicast routers on the same subnet; and then elect a designated router for IGMP queries and to send source registration messages to the rendezvous point (RP).

`IP igmp snooping VLAN 50 immediate-leave`	Enables IGMP Fast-leave processing; upon receiving an "IGMP leave group" message, the switch immediately removes the interface from its Layer 2 forwarding table. Only enable this on vlans where only one host is connected to each Layer 2 LAN interface.

Campus Multicast Configuration for Layer 2 Switches used for Data Center

This section provides the configuration required for the datacenter where slightly different configuration is required for the Layer 2 connections from the distribution to the access layers.

Campus Multicast configuration for Layer 2 Distribution-Layer switches used for Datacenter

Table 6-12 Campus Multicast configuration for Layer 2 Distribution-Layer Switches used for Data Center

configuration command (Switch D1L used for example config)	Description of configuration
`ip multicast-routing`	Globally enable multicast

`spanning-tree vlan 32 root primary`
`interface VLAN 32`
`standby 1 priority 120`
`ip pim dr-priority 120`
	The root STP bridge, the HSRP active node, and the PIM DR should all be on the same distribution switch for each specific VLAN.

`interface VLAN 32`
`ip pim query-interval 250 msec`
	Increase the speed with which the router will detect other multicast routers on the same subnet; and then elect a designated router for IGMP queries and to send source registration messages to the rendezvous point (RP).

`interface vlan32`
`ip igmp snooping fast-leave`
	Enables IGMP Fast-leave processing; upon receiving an "IGMP leave group" message, the switch immediately removes the interface from its Layer 2 forwarding table. Only enable this on vlans where only one host is connected to each Layer 2 LAN interface.

`interface VLAN 32`
`ip pim sparse-mode`
	Enable PIM on all multicast-enabled VLANs

`interface Loopback2`
`description Garbage-CAN RP`
`ip address 2.2.2.2 255.255.255.255`
	Define a local loopback address to provide a sink hole route point for invalid multicast groups

`ip access-list standard GOOD-IPMC`
`permit 239.1.2.3 0.0.0.0`
`permit 230.230.0.0 0.0.255.255`
`permit 239.192.240.0 0.0.3.255`
`permit 239.192.248.0 0.0.3.255`
	Explicitly define what multicast groups to be forwarded to the RP
	-- permit LWAPP multicast tunnel
	-- Permit Vocera traffic
	-- Permit music on hold traffic
	-- Permit IPTV medium-rate traffic

Table 6-12 Campus Multicast configuration for Layer 2 Distribution-Layer Switches used for Data Center (continued)

ip pim rp-address 10.33.9.1 GOOD-IPMC override	Send all traffic permitted by the GOOD-IPMC access-list to the anycast RP address
ip pim rp-address 2.2.2.2	Send all multicast traffic that does not match the multicast groups defined in GOOD-IPMC access-list to the locally-defined Garbage-Can RP.

Campus Multicast Configuration for Layer 2 ACcess-Layer Switches used for Data Center

No multicast-specific configuration is required on L2 access layer switches.

Campus Multicast Configuration for Layer 2 Switches used for Data Center Verification

Table 6-13 Verifying the L2 Multicast Configuration for the Data Center

configuration command	Description of configuration
show spanning-tree summary show standby brief show ip pim interface	These commands can be used to check that spanning-tree root, HSRP active, and PIM DR are all on the same router for a given VLAN

Access Switch Catalyst Integrated Security Features (CISF) Configuration

The configuration below is applied to all access layer switches that will have end-users or APs connected to them. The port security configuration permits a maximum of 2 MAC addresses; this is enough for a Cisco IP phone with an attached PC to be connected. An LWAPP AP tunnels all client traffic to the LWAPP controller, so the switch it is connected to will only ever see the MAC and IP address of the AP on that port.

Table 6-14 Switch Security Configuration

Configuration command	Description of Configuration
DHCP Snooping ip dhcp snooping vlan 50 51 no ip dhcp snooping information option ip dhcp snooping	Globally enable DHCP Snooping These commands will put every VLAN 50 and VLAN 51 port into "untrusted" state. If the path to the DHCP server is out one of these switch ports, that port should be manually set to "trusted"
Dynamic Arp Inspection (DAI) ip arp inspection vlan 50,51 ip dhcp snooping database tftp://10.33.32.10/tftpboot/cisco/a4r-dhcpdb	Globally enable Dynamic ARP Inspection (DAI), and make sure the DHCP snooping database is backed up. (DAI requires an accurate DHCP snooping database, and backing up to TFTP ensures its preservation - even if the switch reboots)

Table 6-14 Switch Security Configuration (continued)

Port Security interface GigabitEthernet1/0/1 switchport access vlan 50 switchport mode access switchport voice vlan 51 switchport port-security switchport port-security maximum 2 switchport port-security violation restrict switchport port-security aging time 2 switchport port-security aging type inactivity	interface commands to enable Port Security
IP Source Guard interface GigabitEthernet1/0/1 ip verify source	Interface command to enable IP Source Guard
interface GigabitEthernet1/0/1 ip dhcp snooping limit rate 10	Interface command to limit the number of DHCP messages an interface can receive per second

Router Time Services Configuration

Table 6-15 Campus Router Time Services Configuration

Configuration Command	Description of Configuration
service timestamps debug datetime msec localtime service timestamps log datetime msec localtime	Add timestamps with millisecond resolution to debug and log messages; use the local timezone to represent the time
clock timezone PST -8 clock summer-time PDT recurring clock update-calendar	* Internally, the router uses Universal Coordinated Time (AKA GMT); these commands configure the router to display time in a local time. * The *timezone command* uses a user-defined label and the local offset from UTC as parameters. * The *summer-time* command configures the router to automatically adjust the local-time displayed in accordance with daylight saving conventions; the default is for North America conventions, other regions daylight saving conventions can be explicitly configured if required
ntp source Loopback1 ntp server 10.33.32.16	* Source NTP Queries from Loopback1 interface instead of the interface that sends them. This ensures the NTP server always sees the same source IP and is useful if the NTP server limits the number of NTP Peers that can associate, of if it has Access Control Lists controlling what devices can sync with it. * The *NTP Server* command defines the IP address of the NTP server.
show ntp status show clock details	Useful show commands for verifying correct NTP operation

Uni-Directional Link Detection (UDLD) Configuration

Table 6-16 UniDirectional Link Detection (UDLD) Configuration

configuration command	Description of configuration
`uldp enable`	`Globally enables ULDP on all fiber-optic ports`

UDLD is not supported on the ASAs or 3800s used in this document, and is enabled by default on the 4948s.

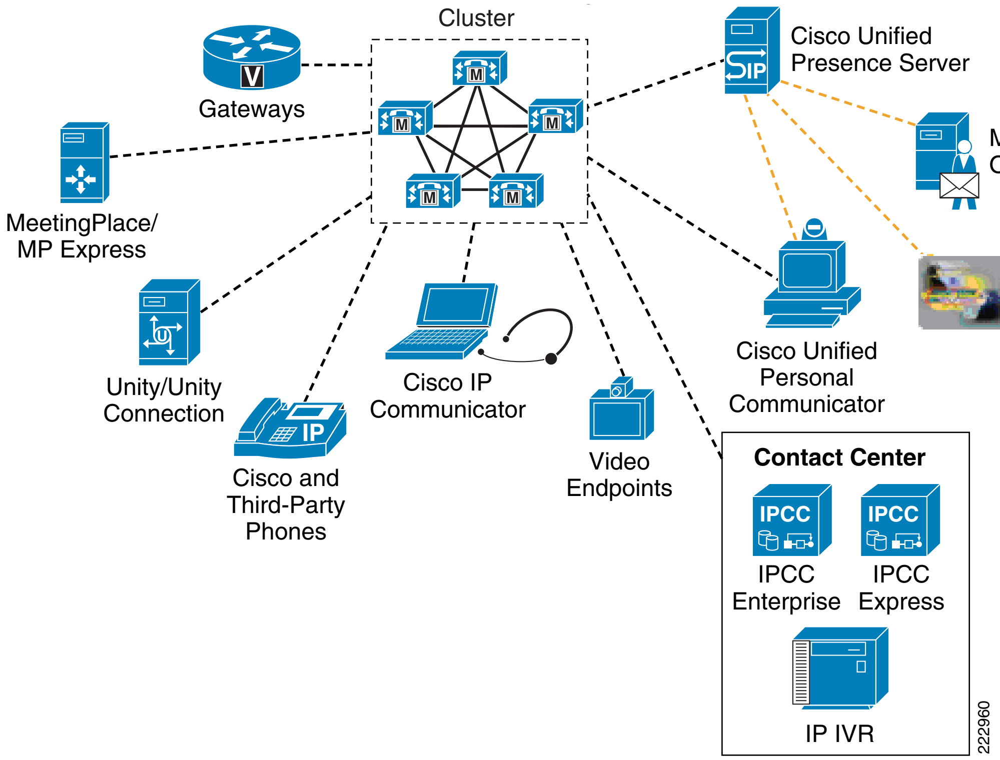
CHAPTER 7

Voice over WLAN Unified Communications Test Architecture

Cisco Unified Communications Manager Introduction

Cisco Unified Communications Manager (Cisco UCM) is the call-processing component of the Cisco Unified Communications System (previously known as Cisco CallManager). The Cisco UCM extends enterprise telephony features and capabilities to IP phones, media processing devices, gateways, mobile devices and multimedia applications. Additional services such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems interact with the IP telephony solution through Cisco UCM APIs. The Cisco UCM is installed on Cisco Media Convergence Server (MCS) 7800 Series of server platforms and selected third-party servers. An example of Cisco UCM and several possible services and endpoints is shown in Figure 7-1.

Figure 7-1 Cisco Unified Communications Manager Example



This Cisco UCM design is based on the existing *Cisco Unified Communications Solution Reference Network Design* (based on Cisco UCM Release 6.x):

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/6x/uc6_0.html

Cisco Unified Communications System Release Summary Matrix for IP Telephony:

http://www.cisco.com/en/US/docs/voice_ip_comm/uc_system/unified/communications/system/versions/IPTMtrix.html

Cisco Unified Communications Manager Design Overview

Deployment Models

There are several deployment models for Cisco UCM based on the following factors:

- Number of call processing agent clusters
- Number of IP phones
- Locations of the call processing cluster(s) and IP phones

Single Site

The single-site model for Cisco Unified Communications consists of a call processing agent cluster located at a single site, or campus, with no telephony services provided over an IP WAN.

Multisite WAN with Centralized Call Processing

The model for a multisite WAN deployment with centralized call processing consists of a single call processing cluster that provides services for many remote sites and uses the IP WAN to transport Cisco Unified Communications traffic between the sites.

Multisite WAN with Distributed Call Processing

The model for a multisite WAN deployment with distributed call processing consists of multiple independent sites, each with its own call processing cluster connected to an IP WAN that carries voice traffic between the distributed sites

Clustering Over the IP WAN

It is possible to deploy a single UCM cluster across multiple sites that are connected by a QoS-enabled IP WAN. For specific WAN requirements, refer to the Cisco Unified Communications Solution Reference Network Design:

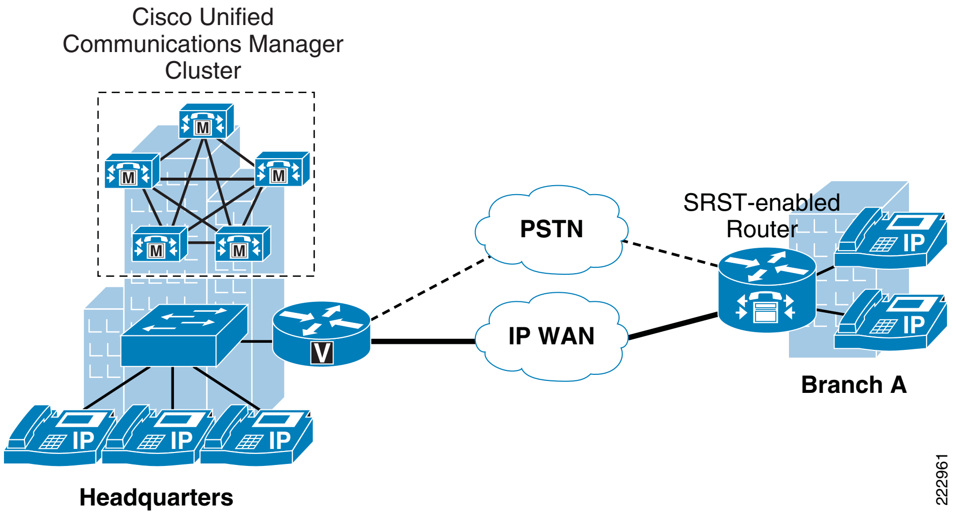
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/6x/uc6_0.html

Each deployment model has benefits and network requirements that should be considered. Further descriptions of the Cisco Unified Communications Manager Deployment models are available within the *Cisco Unified Communications Solution Reference Network Design*.

The design considerations presented in this chapter were based on the use of a Multisite WAN with Centralized Call Processing deployment. This model consists of a centralized call processing cluster and one or more remote sites using an IP WAN to transport voice and call control.

Figure 7-2 is an example of a Multisite WAN with Centralized Call Processing with one branch location.

Figure 7-2 Multisite with Centralized Call Processing



Cisco Unified Communications Manager Configuration

Wireless phones (and softphones) are inherently mobile so controlling the admission of their calls into a network is critical to maintaining the quality of calls by avoiding traffic collisions leading to loss, jitter and delay perceptible to the user. The next two sections will discuss CAC and Device Mobility and how Device Mobility configuration is important to maintaining accurate CAC decisions.

Call Admission Control

This chapter discusses Call Admission Control (CAC) by the Cisco UCM for those devices on the physical IP LAN/WAN, in the context of a single cluster design. This applies to wireless phones (Cisco 7920/7921) from the point of entry into the physical network. CAC must also be considered on the wireless network and is discussed in detail in the Chapter 2, "WLAN Quality of Service."

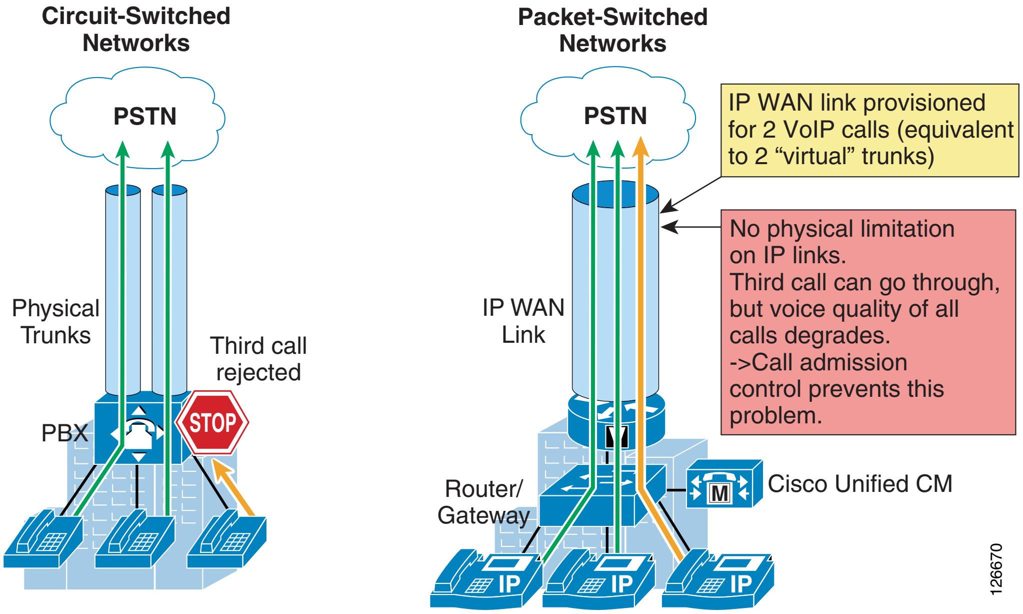
CAC in the context of this chapter is a concept that applies to real-time (voice) traffic only, not data traffic. If an influx of data traffic oversubscribes a particular link in the network, queuing, buffering, and packet drop decisions resolve the congestion. The extra traffic is simply delayed until the interface becomes available to send the traffic, or, if traffic is dropped, protocol timeouts or user-initiated actions will trigger the re-transmission of the information.

Network congestion cannot be resolved in this manner when real-time traffic, sensitive to both latency and packet loss, is present, without jeopardizing the quality of service (QoS) expected by the users of that traffic. For real-time delay-sensitive traffic such as voice, it is better to deny network access under congestion conditions than to allow traffic onto the network to be dropped and delayed, resulting in sporadic impairments perceived by the users.

QoS protects voice from being overrun by data. CAC on the other hand, protects voice from voice. If a link can support X calls, allowing X + 1 calls will have a negative impact on calls being carried by that link. CAC is therefore a deterministic and informed decision that is made before a voice call is established and is based on whether the required network resources are available to provide suitable QoS for the new call.

Considering Figure 7-3, because it is based on a packet-switched network (the IP network), no circuits are established to setup an IP telephony call. Instead, the IP packets containing the voice samples are simply routed across the IP network together with other types of data packets. QoS is used to differentiate the voice packets from the data packets, but bandwidth resources, especially on IP WAN links, are not infinite. Therefore, network administrators dedicate a certain amount of "priority" bandwidth to voice traffic on each IP WAN link. However, once the provisioned bandwidth has been fully used, the IP telephony system must reject subsequent calls to avoid oversubscription of the priority queue on the IP WAN link, which would cause quality degradation for all voice calls.

Figure 7-3 CAC Example


Circuit-Switched Networks
Packet-Switched Networks
PSTN
PSTN
IP WAN link provisioned for 2 VoIP calls (equivalent to 2 "virtual" trunks)
No physical limitation on IP links.
Third call can go through, but voice quality of all calls degrades.
->Call admission control prevents this problem.
Physical Trunks
Third call rejected
STOP
PBX
IP WAN Link
Router/ Gateway
Cisco Unified CM
M
IP
IP
IP
126670

Most CAC control mechanisms fall into two categories:

- Topology-unaware call admission control—Based on a static configuration within the call processing agent
- Topology-aware call admission control—Based on communication between the call processing agent and the network about the available resources

Topology-unaware CAC is based on the UCM construct of CAC static locations, with each branch site belonging to a unique location. All devices in a site are assigned to the same location. Based on the amount of bandwidth available, each site would support a specific number of calls over the IP WAN.

Topology-aware CAC limits the number of calls across the IP WAN using real-time communications about the availability of network resources between the UCM and the network. This CAC mechanism works well in environments with constant topology changes as it can dynamically adjust to the changes, or with non hub-and-spoke WAN topologies. Resource Reservation Protocol (RSVP) is the primary industry-standard signaling protocol that enables an application to reserve bandwidth dynamically across an IP network. Using RSVP, applications can request a certain amount of bandwidth for a data flow across a network (for example, a voice call) and can receive an indication of the outcome of the reservation based on actual resource availability.

For this version of the design guide, static locations-based CAC (topology-unaware) was used. For an in-depth discussion of CAC, refer to *Cisco Unified Communications Solution Reference Network Design* at the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/6x/uc6_0.html

Device Mobility

Mobility of wireless phones includes not just moving between access points within a building but also moving between buildings and locations. If a wireless phone user is defined with a UCM region and location specific to their home location (for example, San Jose) takes their phone to a branch office in somewhere else (for example, in RTP), it is important that device mobility is configured so the WAN links between these location are not oversubscribed. Without device mobility, when the users phone registers in the branch location (RTP), the UCM configuration for the phone assumes they have registered in San Jose. If the user dials a PSTN number in RTP, UCM may use a gateway in San Jose and also not deduct bandwidth that the phone is using over the WAN link between RTP and San Jose, possibly causing and over-subscription environment.

Device mobility allows UCM to make device configuration decisions based on the subnet of the device that is registering. Some of the device mobility elements include:

- Device Mobility Info—Configures IP subnets and associates device pools to the IP subnets.
- Device Mobility Group—Defines a logical group of sites with similar dialing patterns (for example, US_dmg and EUR_dmg).
- Physical Location—Defines the physical location of a device pool. In other words, this element defines the geographic location of IP phones and other devices associated with the device pool.

UCM uses a new set of parameters under the device pool configuration to accommodate device mobility. These parameters are of the following two main types:

- Roaming Sensitive Settings
- Device Mobility Related Settings

Roaming Sensitive Settings

The parameters under these settings override the device-level settings when the device is roaming within or outside a device mobility group. The parameters included in these settings are:

- Date/Time Group
- Region
- Media Resource Group List
- Location
- Network Locale
- SRST Reference
- Physical Location
- Device Mobility Group

The roaming sensitive settings primarily help in achieving proper CAC and voice codec selection, because the location and region configurations are used based on the device's roaming device pool. The roaming sensitive settings also update the media resource group list (MRGL) so that appropriate remote media resources are used for music on hold, conferencing, transcoding, and so forth, thus utilizing the network efficiently. The roaming sensitive settings also update the Survivable Remote Site Telephony (SRST) gateway. Mobile users register to a different SRST gateway while roaming.

Device Mobility Related Settings

The parameters under these settings will override the device-level settings only when the device is roaming within a device mobility group. The parameters included in these settings are:

- Device Mobility Calling Search Space
- AAR Calling Search Space
- AAR Group

The device mobility related settings affect the dial plan because the calling search space dictates the patterns that can be dialed or the devices that can be reached. Device mobility group, as explained earlier, defines a logical group of sites with similar dialing patterns (for example, sites having the same PSTN access codes and so forth). With this guideline, all sites have similar dialing patterns in the site-specific calling search spaces. Sites having different dialing behavior are in a different device mobility group. A user roaming within a device mobility group may preserve his dialing behavior at the remote location even after receiving a new calling search space. A user roaming outside the device mobility group may still preserve his dialing behavior at the remote location because he uses his home calling search space. However, if a device mobility group is defined with sites having different dialing patterns (for example, sites having different PSTN access codes), then a user roaming within that device mobility group might not preserve his same dialing behavior at all locations. A user might have to dial digits differently at different locations after receiving a new calling search space at each location.

For an in-depth discussion of device mobility, refer to Cisco *Unified Communications Solution Reference Network Design:*

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/6x/uc6_0.html

Network Infrastructure

Refer to the *Cisco Unified Communications Solution Reference Network Design* for additional network infrastructure recommendations.

UCM and Phone versions

This design guide use the following Cisco UCM and phone versions:

- Cisco UCM 6.0.1
- 7960—SCCP41.8-3-1S
- 7921—CP7921G-1.0.34

CHAPTER 8

Voice over WLAN Wireless LAN Controller Design and Configuration

Wireless LAN Controller (WLC) configuration can vary from VoWLAN handset to VoWLAN handset and specific configuration settings can also depend on the requirements of the overall WLAN data network. Variations are principally targeted to the WLAN configuration on the WLC. There are also certain key Cisco Unified Wireless configuration considerations that directly affect the overall VoWLAN design and implementation—in particular, IEEE 802.11 wireless network configurations can have an effect.

Chapter 3, "Voice over WLAN Radio Frequency Design," addresses the guidelines for AP location, AP density, and Auto-RF features. This chapter focuses on Auto-RF configuration and WLC network configuration.

RF design cannot be ignored. Implementing an architecture featuring the correct location and density of APs for a WLAN network is the equivalent of correctly installing the cable plant for a wired network. In wired network, problems in the cable plant cannot be completely overcome by advanced features. Similarly, in the WLAN network, Auto-RF is unlikely to overcome a flawed AP deployment. This chapter addresses wireless network and Auto-RF configuration.

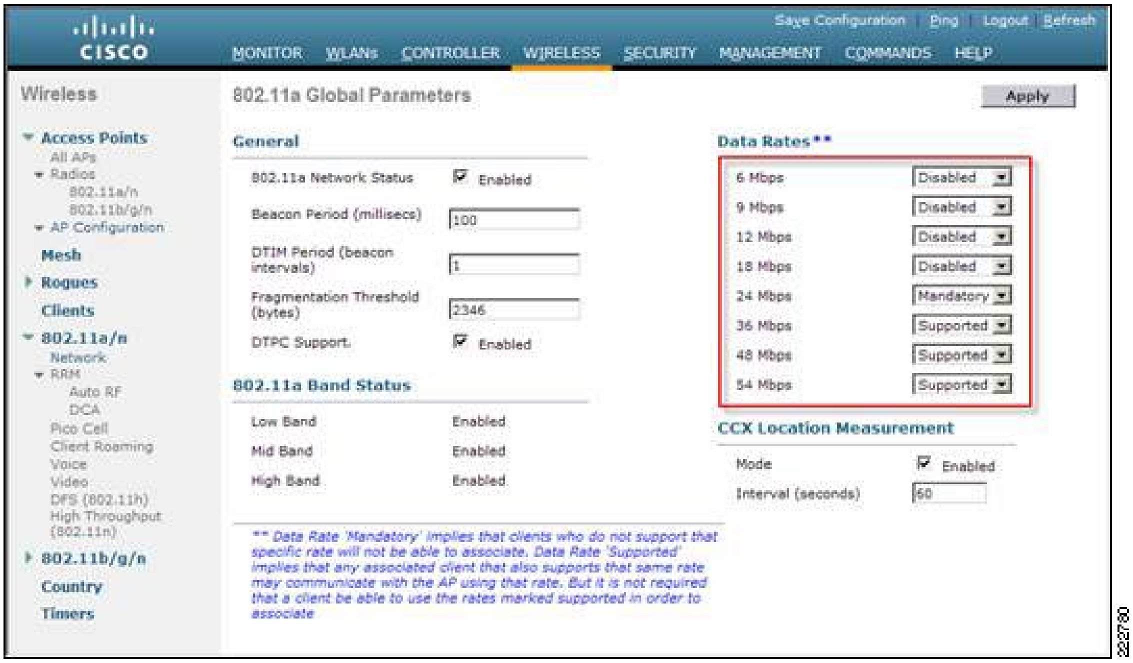
Network Configuration

The radio configuration of each AP should be left to Auto-RF , unless there are know issues at the site that preclude the effective use of Auto-RF.. The configuration for the AP network is performed under the IEEE 802.11b/g/n and IEEE 802.11a/n subsections of the wireless menu.

Data Rates

The goal in setting the data rates for the VoWLAN network is to match the data rates of VoWLAN handsets as closely as possible. For example, if the VoWLAN RF network design was based on a 24 Mbps data-rate, lower data-rates should be excluded if possible. This would only be possible when not supporting IEEE 802.11 1Mbps and 2Mbps and IEEE 802.11b 5.5Mbps and 11Mbps clients. Any lowering of the data-rate below that used in the RF design extends the AP cell size, increases co-channel interference, and reduces call capacity. Higher data rates than the site survey rate can be enabled, but a VoWLAN client might not take advantage of these rates because some VoWLANs prefer not to data rate shift. An example of the 24 Mbps and above configuration is shown in Figure 8-1.

Figure 8-1 Channel Data Rate Setting



802.11a Global Parameters

General

802.11a Network Status	☑ Enabled
Beacon Period (millisecs)	100
DTIM Period (beacon intervals)	1
Fragmentation Threshold (bytes)	2346
DTPC Support.	☑ Enabled

802.11a Band Status

Low Band	Enabled
Mid Band	Enabled
High Band	Enabled

Data Rates**

6 Mbps	Disabled
9 Mbps	Disabled
12 Mbps	Disabled
18 Mbps	Disabled
24 Mbps	Mandatory
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

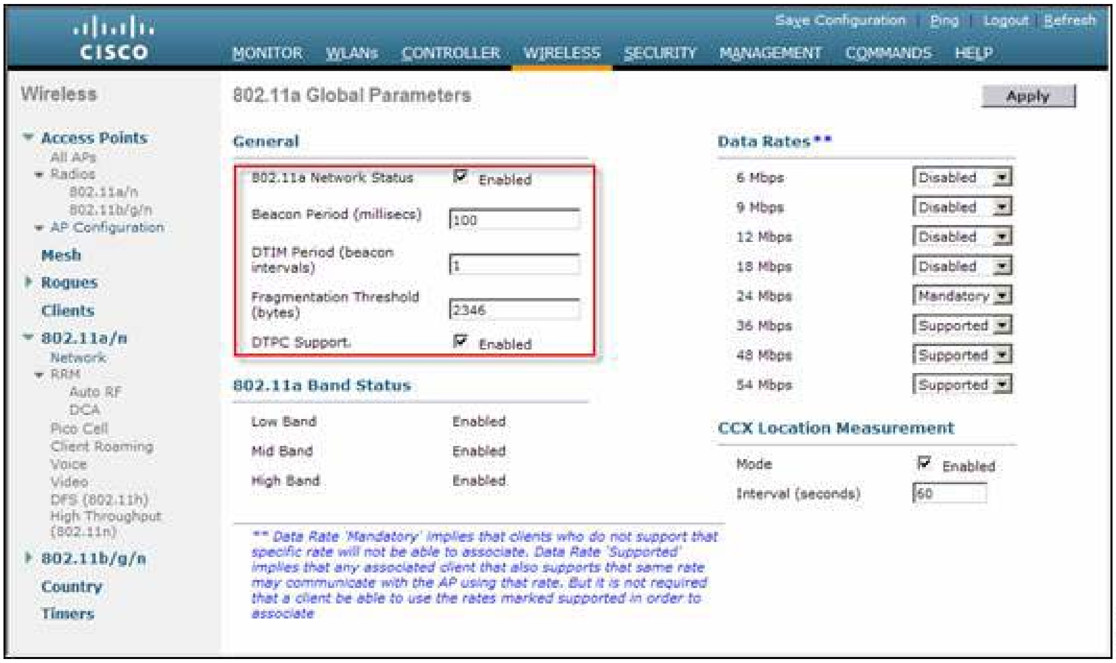
CCX Location Measurement

Mode	☑ Enabled
Interval (seconds)	60

*** Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate*

The general global parameters (see Figure 8-2) for a channel can normally be kept at the default values. Some VoWLAN handsets might require the delivery traffic indication Map (DTIM) to be increased to maximize battery life, but this change should only be done based on design recommendation specific to the handset. The DTIM period sets the number of beacon intervals that a WLAN client will sleep before waking up to see whether any traffic has been buffered for it (when in power save mode). Multicast and broadcast traffic must be buffered—as well as any unicast traffic—when destined for power saving clients. This can affect application performance, so DTIM should only be adjusted to the levels recommend by the VoWLAN handset vendor. DTIM settings are global for the band and are not changed on a per WLAN basis; therefore, changing the DTIM value will affect each WLAN on a given AP radio.

Figure 8-2 General Global Parameters



802.11a Global Parameters

General

802.11a Network Status	☑ Enabled
Beacon Period (millisecs)	100
DTIM Period (beacon intervals)	1
Fragmentation Threshold (bytes)	2346
DTPC Support.	☑ Enabled

802.11a Band Status

Low Band	Enabled
Mid Band	Enabled
High Band	Enabled

Data Rates**

6 Mbps	Disabled
9 Mbps	Disabled
12 Mbps	Disabled
18 Mbps	Disabled
24 Mbps	Mandatory
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

CCX Location Measurement

Mode	☑ Enabled
Interval (seconds)	60

** Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate

Radio Resource Management

Radio Resource Management (RRM) can adjust AP channels (dynamic channel assignment) and power (dynamic transmit power control) to maintain the RF coverage and quality:

- It adjusts the power level of the APs to maintain a baseline signal strength with neighboring APs at -70 dBm (configurable, and default value changed from -65dBm to -70dBm in the 4.1.185 code Release).
- It adjust the power levels of the APs to increase the SNR of WLAN clients that are detected with poor SNRs.
- It adjusts the channel of the AP when it notices nearby interference sources on the channel which the AP is currently located.
- It continues to optimize the RF coverage for the best reception and throughput for the wireless network.

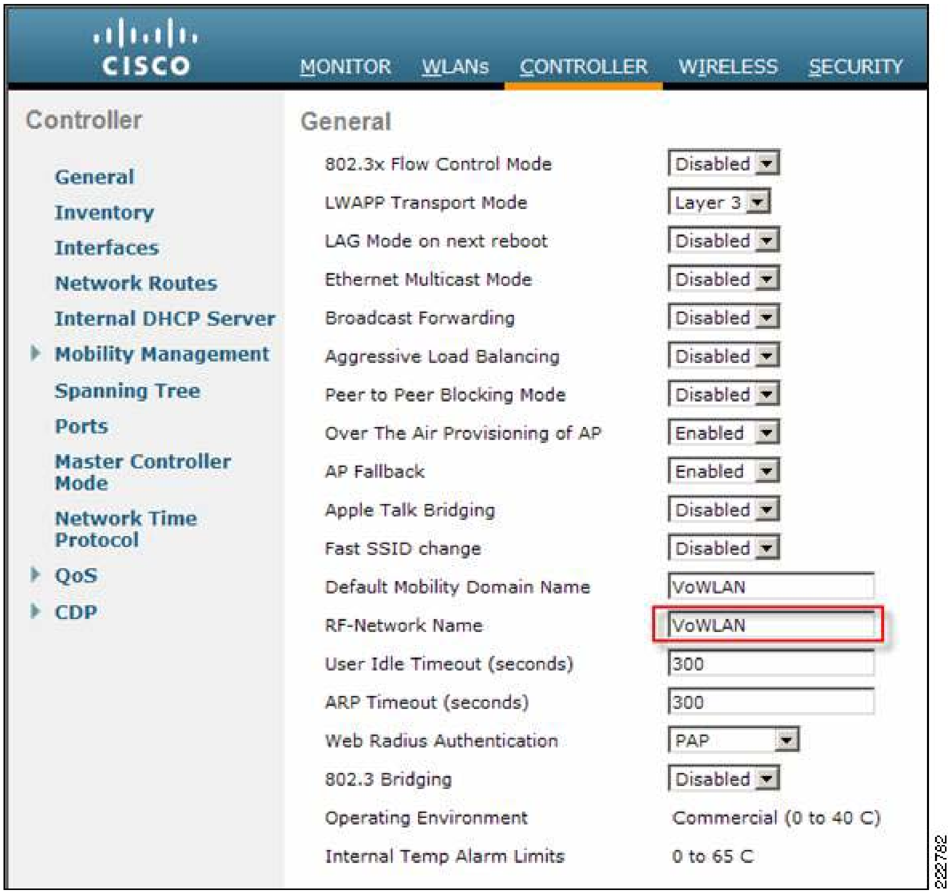
RRM addresses the issue that RF environments are not static. As different RF variables change (people in the room, amount of devices stored in the facility, leaves on trees for outside deployment, interference from different RF sources, and so on), the RF coverage changes with them.

Because these variables change continuously, monitoring for the RF coverage and adjusting it periodically is necessary, and RRM is an automatic mechanism for adjusting for changes in RF variables. For more detailed information on RRM (Auto-RF), see the following URL:
http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a008072c759.shtml

RRM Architecture Overview

Each WLC is configured with a RF-Network Name (the RF-Group Name, which is by default the same as the Mobility Group Name). WLCs with the same RF-Network Name can be part of the same RF Group. The RF-Network Name configuration is found in the Controller General Configuration menu, as shown in Figure 8-3.

Figure 8-3 RF-Network Name



General

802.3x Flow Control Mode	Disabled
LWAPP Transport Mode	Layer 3
LAG Mode on next reboot	Disabled
Ethernet Multicast Mode	Disabled
Broadcast Forwarding	Disabled
Aggressive Load Balancing	Disabled
Peer to Peer Blocking Mode	Disabled
Over The Air Provisioning of AP	Enabled
AP Fallback	Enabled
Apple Talk Bridging	Disabled
Fast SSID change	Disabled
Default Mobility Domain Name	VoWLAN
RF-Network Name	VoWLAN
User Idle Timeout (seconds)	300
ARP Timeout (seconds)	300
Web Radius Authentication	PAP
802.3 Bridging	Disabled
Operating Environment	Commercial (0 to 40 C)
Internal Temp Alarm Limits	0 to 65 C

In each RF group (if Group Mode is enabled in the Auto-RF configuration, Figure 8-4), the WLCs 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 WLCs and do the channel/power computation for an optimal system-wide map. If Group Mode is not enabled, the WLCs run computations based only on the neighbor data gathered from the APs connected to that WLC via LWAPP, trying to optimize the signal to -70 dBm between APs.

The APs transmit 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 WLC.
- If they can validate the message hash and confirm that it belongs to the same RF group, the packet is sent to the WLC; otherwise, the AP drops the neighbor packet.

- The APs forwards validated messages to the WLC, filling in the LWAPP packet status field with the SNR and RSSI of the received neighbor packet.

Logical RF Sub-groups

Within an AP group there may be clusters of APs that do not see each other, even if they are connected to the same WLC or connected to different WLCs that are part of the same RF group. In this case, theses APs form a logical RF sub-group whose RF parameters are calculated separately(i.e., the Auto-RF algorithms are calculated per RF sub-group).

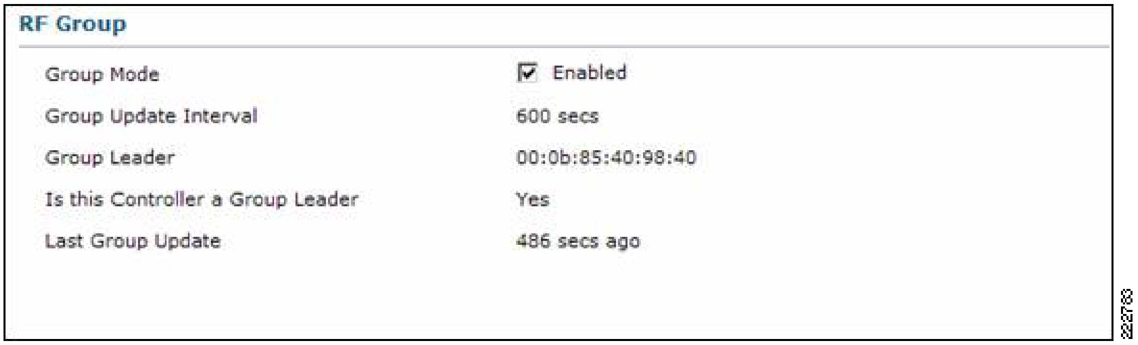
Channel Scanning

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 WLC, where they are analyzed to detect rogue APs, whether service set identifiers (SSIDs) are broadcast or not, rogue clients, ad-hoc clients, and interfering APs. By default, each AP spends approximately 0.2 percent of its time off-channel. This is statistically distributed across all APs so that no two adjacent APs are scanning at the same time. Packets received by the AP from clients are forwarded to the WLC with the LWAPP status field filled-in, which provides the WLC with radio information including RSSI and signal-to-noise ratio (SNR) for all packets received by the AP during reception of the packet. For more detailed information on RRM (Auto-RF), see the following URL:
http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a008072c759.shtml

RF Group

Figure 8-4 shows the RF Group configuration section of Auto-RF. In this area the Group Mode is enabled (if it is not enabled. the WLC considers only its own AP information in its RRM calculations). The display also identifies the Group Leader (the WLC responsible for the RF Group).

Figure 8-4 RF Group Configuration



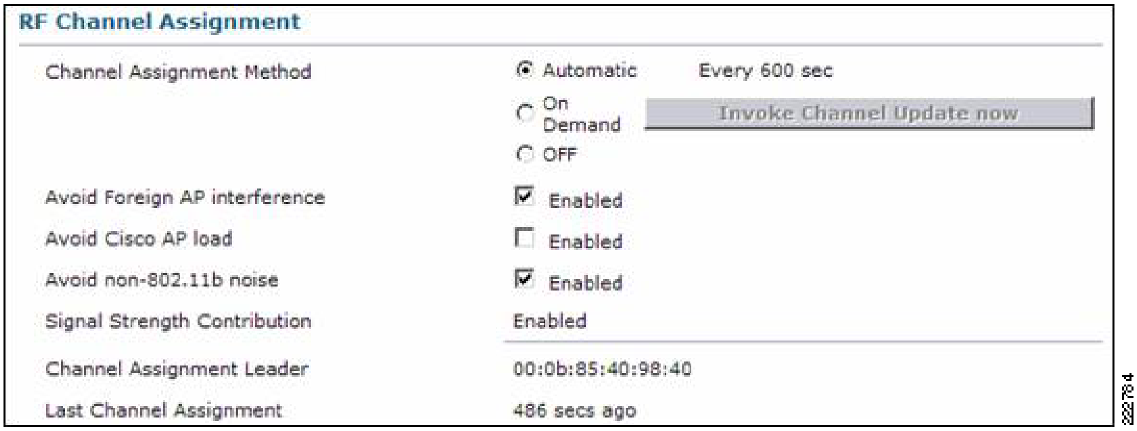
RF Group

Group Mode	☑ Enabled
Group Update Interval	600 secs
Group Leader	00:0b:85:40:98:40
Is this Controller a Group Leader	Yes
Last Group Update	486 secs ago

Dynamic Channel Assignment

The next section in the Auto RF configuration section is RF Channel Assignment, shown in Figure 8-5. This feature controls Dynamic Channel Assignment (DCA).

Figure 8-5 RF Channel Assignment



RF Channel Assignment

Channel Assignment Method ● Automatic Every 600 sec
○ On Demand
○ OFF

Avoid Foreign AP interference ☑ Enabled
Avoid Cisco AP load □ Enabled
Avoid non-802.11b noise ☑ Enabled
Signal Strength Contribution Enabled
Channel Assignment Leader 00:0b:85:40:98:40
Last Channel Assignment 486 secs ago

The DCA algorithm, run by the RF Group Leader (the Channel Assignment Leader), is applied on a per-RF (sub) Group basis to determine optimal AP channel settings for all the RF (sub) Group APs. With the DCA process, the RF Group Leader (a WLC) considers a group of RF metrics to determine whether a change in AP channel scheme is appropriate.

- *Avoid Foreign AP Interference*—APs report the percentage of the medium taken up by interfering IEEE 802.11 transmissions (this can be caused by overlapping signals from foreign APs, as well as non-neighbors).This field allows the co-channel interference metric to be included in DCA algorithm calculations. This field is enabled by default.
- *Avoid Cisco AP Load*—Every AP measures the percentage of total time occupied by transmitting or receiving IEEE 802.11 frames This field allows the utilization of APs to be considered when determining which AP's channels need changing. AP load is a frequently changing metric and its inclusion might not be always desired in the RRM calculations. As such, this field is disabled by default. The Cisco AP Load parameter is a measure of channel load seen by the APs in the RF Group. It includes the co-channel interference generated by neighboring APs and clients.
- *Avoid non-IEEE 802.11b Noise*—APs calculate noise values on every serviced channel. This field allows each AP's non-IEEE 802.11 noise level to be a contributing factor to the DCA algorithm. This field is enabled by default.
- *Signal Strength Contribution*—Every AP listens for Neighbor Messages on all serviced channels and records the RSSI values at which these messages are heard. This AP signal strength information is the most important metric considered in the DCA calculation of channel energy. The signal strength of neighboring APs is always included in DCA calculations. This is a display-only field and cannot be modified.

These values are used by the RF Group Leader to determine whether another channel schema will result in an improvement of at least 5 dB (SNR) for the worst performing AP. A weighting is given to APs on their operating channels to bias them into maintaining their channels. As a result, adjustments are kept local; the weighting dampens changes preventing a domino effect in which a single change triggers system-wide channel alterations. Preference is also given to APs based on utilization (derived from each AP's load measurement report). A less-used AP has a higher likelihood of having its channel changed (as compared to a heavily used neighbor) in the event a change is needed.

Note Whenever an AP channel is changed, clients are briefly disconnected. Clients can either reconnect to the same AP (on its new channel), or roam to a nearby AP depending on client roaming behavior. Fast, secure roaming—offered by both Cisco Centralized Key Management (CCKM) and Proactive Key Caching (PKC)—will help reduce this brief disruption, assuming clients are compatible.

The following WLC commands provide visibility of the RF data collected by each AP:

```
show ap auto-rf IEEE 802.11b ap-name
show ap auto-rf IEEE 802.11a ap-name
```

The following is an example output using the **show ap auto rf** command:

```
Cisco Controller> show ap auto-rf IEEE 802.11b AP0012.d92b.5cfa

Number Of Slots.................................. 2
AP Name.......................................... AP0012.d92b.5cfa
 MAC Address...................................... 00:12:d9:2b:5c:fa
  Radio Type..................................... RADIO_TYPE_IEEE 80211b/g
  Noise Information
    Noise Profile................................ PASSED
    Channel 1....................................  -97 dBm
    Channel 2....................................  -96 dBm
    Channel 3....................................  -95 dBm
    Channel 4....................................  -99 dBm
    Channel 5....................................  -96 dBm
    Channel 6....................................  -96 dBm
    Channel 7....................................  -93 dBm
    Channel 8....................................  -95 dBm
    Channel 9.................................... -100 dBm
    Channel 10...................................  -96 dBm
    Channel 11...................................  -96 dBm
  Interference Information
    Interference Profile......................... PASSED
    Channel 1.................................... -128 dBm @  0 % busy
    Channel 2....................................  -82 dBm @  1 % busy
    Channel 3.................................... -128 dBm @  0 % busy
    Channel 4.................................... -128 dBm @  0 % busy
    Channel 5....................................  -76 dBm @  1 % busy
    Channel 6.................................... -128 dBm @  0 % busy
    Channel 7....................................  -75 dBm @  1 % busy
    Channel 8.................................... -128 dBm @  0 % busy
    Channel 9.................................... -128 dBm @  0 % busy
    Channel 10................................... -128 dBm @  0 % busy
    Channel 11...................................  -70 dBm @  2 % busy
  Load Information
    Load Profile................................. PASSED
    Receive Utilization.......................... 2 %
    Transmit Utilization......................... 1 %
    Channel Utilization.......................... 3 %
    Attached Clients............................. 0 clients
  Coverage Information
    Coverage Profile............................. PASSED
    Failed Clients............................... 0 clients
  Client Signal Strengths
    RSSI -100 dbm................................ 0 clients
    RSSI  -92 dbm................................ 0 clients
    RSSI  -84 dbm................................ 0 clients
    RSSI  -76 dbm................................ 0 clients
    RSSI  -68 dbm................................ 0 clients
    RSSI  -60 dbm................................ 0 clients
    RSSI  -52 dbm................................ 0 clients
  Client Signal To Noise Ratios
    SNR    0 dB.................................. 0 clients
    SNR    5 dB.................................. 0 clients
    SNR   10 dB.................................. 0 clients
    SNR   15 dB.................................. 0 clients
    SNR   20 dB.................................. 0 clients
    SNR   25 dB.................................. 0 clients
    SNR   30 dB.................................. 0 clients
  SNR   35 dB.................................. 0 clients
  SNR   40 dB.................................. 0 clients
  SNR   45 dB.................................. 0 clients
Nearby APs
  AP 00:0b:85:51:63:60 slot 1..................  -36 dBm  on    6 (192.168.60.10)
  AP 00:0b:85:52:40:d0 slot 1..................  -36 dBm on  11 (192.168.60.10)
  AP 00:12:44:b3:c1:f0 slot 0..................  -32 dBm on   6 (192.168.60.10)
  AP 00:14:1b:59:40:20 slot 0..................  -36 dBm on  11 (192.168.60.10)
  AP 00:17:df:36:99:80 slot 0..................  -59 dBm on  11 (192.168.60.10)
Radar Information
Channel Assignment Information
  Current Channel Average Energy............... unknown
  Previous Channel Average Energy.............. unknown
  Channel Change Count......................... 0
  Last Channel Change Time..................... Fri Oct 12 01:37:57 2007
  Recommended Best Channel..................... 1
RF Parameter Recommendations
  Power Level.................................. 7
  RTS/CTS Threshold............................ 2347
  Fragmentation Tnreshold...................... 2346
  Antenna Pattern.............................. 0
```

Tx Power Level Assignment

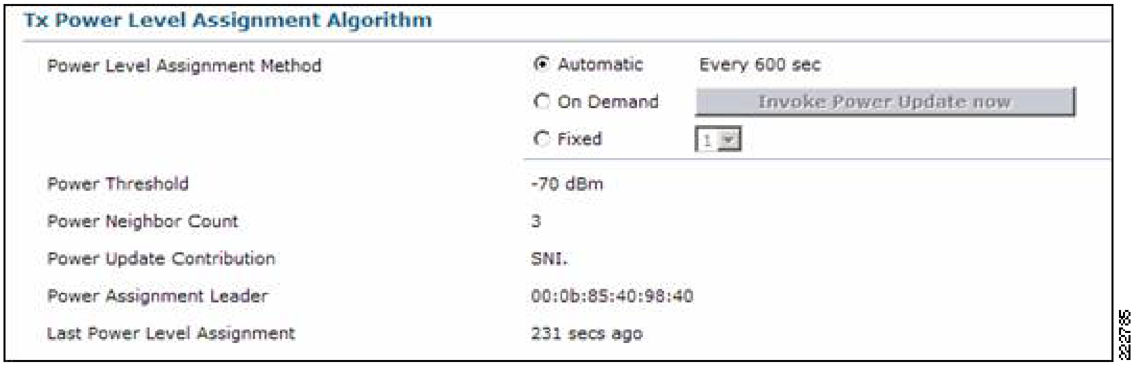
The *Tx Power Level Assignment* is controlled by the Transmission Power Control (TPC) algorithm (see Figure 8-6) is run at fixed 10-minute intervals by default. It is used by the RF Group Leader to determine AP RF proximity and adjust each band's transmit power level in order to limit excessive cell overlap and co-channel interference. Each AP reports an RSSI-ordered list of all neighboring APs and—provided an AP has three or more neighboring APs—the RF Group Leader will apply the TPC algorithm on a per-band, per-AP basis in order to adjust AP power transmit levels *downward* such that the third loudest neighbor AP will then be heard at a signal level of -70 dBm (default value, with the 4.1.185 code release, but earlier code default of -65dBm may be inherited from a pre-existing configuration) or lower. Power changes are only made when an AP's third loudest neighbor is heard at a signal level higher than the default value of -70 dBm (there is a 6dB hysteresis used built into the TPC algorithm to prevent it from continuously hunting for the -70dBm value).

The TPC algorithm it not aware of the physical location of the APs or of requirements to run the APs at a higher or lower power due to some deployment issues. This needs to be considered in AP planning and deployment.

TPC is not aware of AP location or the coverage requirements of the WLAN deployment following should be observed for optimal power level and coverage:

- APs should be located close to the perimeters of the building to ensure that coverage extends to these areas.
- APs should be distributed as evenly as possible to ensure that neighbor signals reflective of coverage requirements
- As the TPC algorithm is three dimensional, and an even AP distribution assists TPC, different floors should not have the same AP layout (i.e., APs should be staggered per floor).
- TPC not is aware of the goals for RF coverage and cell overlap that drove your AP placement. Therefore you should verify that your RF needs are being met by Auto-RF by performing a site survey after deployment and Auto-RF has performed its adjustments.
- Auto-RF should be monitored to track the adjustments made by Auto-RF. Auto-RF will be making adjustments to assist the WLAN network to make changes, but these change can mean that something has happened that you did not plan our design for, and this should be investigated.

Figure 8-6 Tx Power Level Assignment Algorithm



Tx Power Level Assignment Algorithm

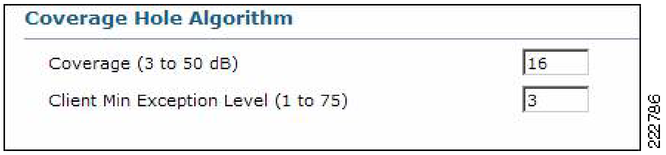
Power Level Assignment Method ● Automatic Every 600 sec
○ On Demand
○ Fixed 1

Power Threshold -70 dBm
Power Neighbor Count 3
Power Update Contribution SNI.
Power Assignment Leader 00:0b:85:40:98:40
Last Power Level Assignment 231 secs ago

Coverage Hole Algorithm

The *Coverage Hole Algorithm* is used to detect holes in coverage based on WLAN client signal measurements and to adjust AP power to address low client-signal levels. A coverage hole is considered to have occurred when client SNRs falls below a predetermined level. The number of clients required to trigger action is configurable as is the signal level. The Coverage Hole Algorithm section from the Auto-RF page is shown in Figure 8-7

Figure 8-7 Coverage Hole Algorithm



Coverage Hole Algorithm

Coverage (3 to 50 dB) 16
Client Min Exception Level (1 to 75) 3

Maintaining VoWLAN coverage is critical for a successful VoWLAN service, so coverage hole protection is an important component in a VoWLAN deployment. As with many design considerations, a decision must be made favoring one characteristic over another:

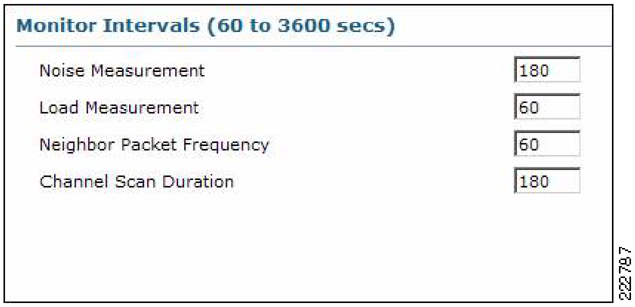
- If the Coverage Hole algorithm is made overly sensitive, it can trigger power increases in APs that are caused by client characteristics rather than coverage issues. This issue can occur with older non-Cisco compatible extension clients that might stay associated with an AP even though that association features a poor SNR. This can result in hole coverage being triggered and AP power being set too high. Poor planning can also trigger hole coverage. VoWLAN clients might be operating in an area where WLAN coverage was not planned and this might cause hole coverage to be triggered.
- If the Coverage Hole is too insensitive, VoWLAN clients might lose calls due to a coverage holes.

Given the variables involved, there are no hard-and-fast rules for specific the Coverage Hole settings. It is best to start with the default settings for the Coverage Hole Algorithm and to monitor any coverage adjustments. If many APs are increasing the power levels, there might be a client issue. If a small group of APs are making coverage adjustments there might be a RF coverage issue.

Monitor Intervals

The *Monitor Intervals* section for the Auto-RF page is shown in Figure 8-8. These parameters determine how often the AP stops serving clients to perform RRM and Wireless duties. There is no need to adjust these values as part of the design process and they should only be adjusted when directed by Cisco support.

Figure 8-8 Monitor Intervals



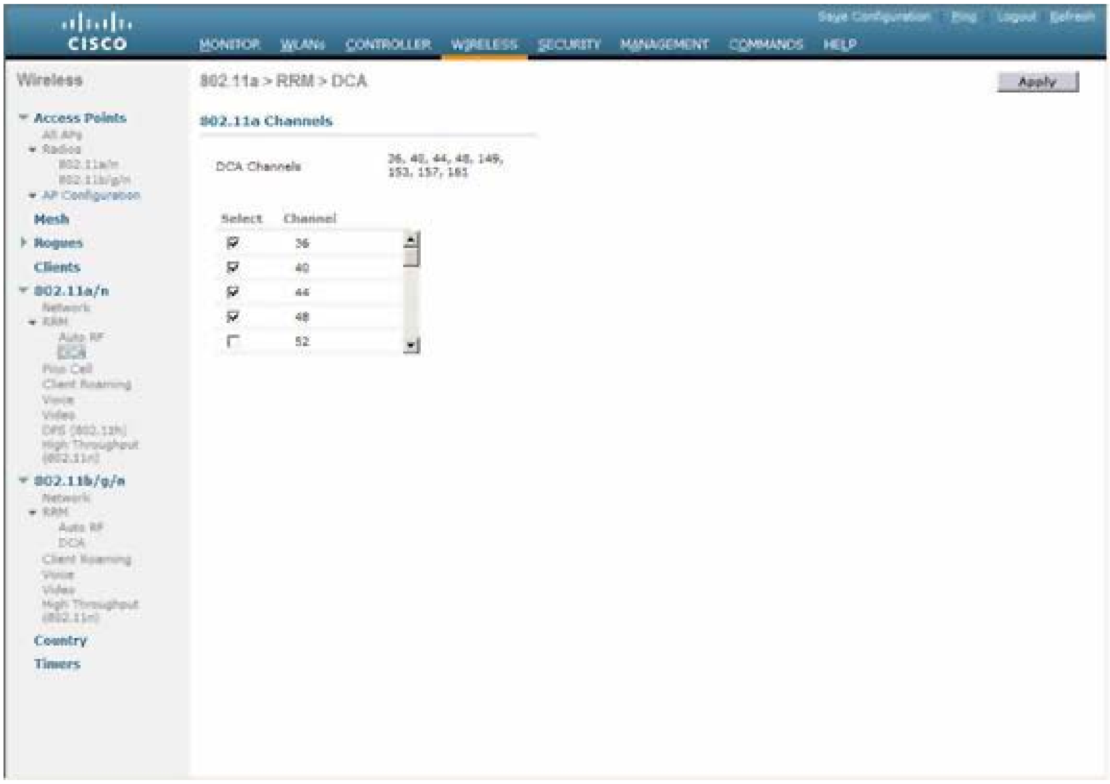
Monitor Intervals (60 to 3600 secs)

Noise Measurement	180
Load Measurement	60
Neighbor Packet Frequency	60
Channel Scan Duration	180

Dynamic Channel Allocation

Figure 8-9 shows the Dynamic Channel Allocation (DCA) screen of RRM. This screen allows the selection of channels for use by the DCA algorithm. Figure 8-9 shows the channels have been selected in the 5 GHz band for use in this example. In this case, the UNII-1 and UNII-3 bands have been chosen to avoid in any Dynamic Frequency Selection (DFS) issues that might affect the VoWLAN network. Channels subject to DFS may be selected if the customer is sure that DFS is not going to be triggered at that site. DFS is required to avoid radar that operates in nominated channels.

Figure 8-9 Channel Selection for DCA



802.11a > RRM > DCA

802.11a Channels

DCA Channels 36, 40, 44, 48, 149, 153, 157, 161

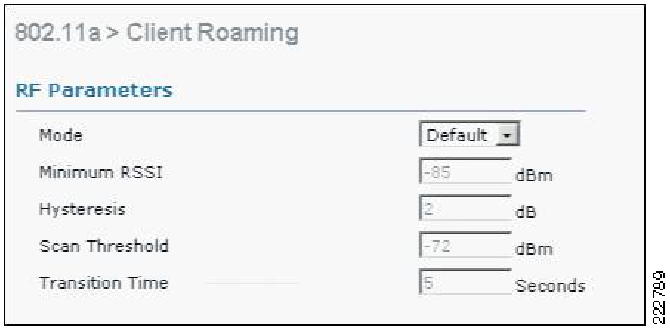
Select	Channel
☑	36
☑	40
☑	44
☑	48
☐	52

Client Roaming

Figure 8-10 shows the *Client Roaming Screen* of RRM. The parameters presented in this screen are communicated to Cisco compatible extension clients to inform them of parameters that should trigger a client roam. The default values might be a little low for a VoWLAN deployment because the AP cell sizes of VoWLAN deployments are usually smaller. While WLAN data clients can maintain their connection at a point where a VoWLAN client should roam, data clients should also roam as close as possible to the planned cell boundary to minimize the range of co-channel interference from these clients. The minimum values for the *Minimum RSSI* is -80 dBm, and the minimum value for the *Scan Threshold* is -70 dBm. These should be tested against typical WLAN data clients and used in VoWLAN deployments unless they are found to interfere with normal WLAN data client operation.

Note If the VoWLAN deployment is using lower client boundary power levels than our example, then different thresholds should be applied.

Figure 8-10 Client Roaming Parameters



802.11a > Client Roaming

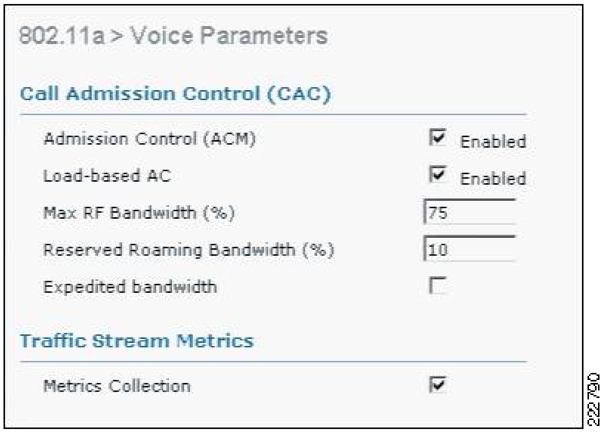
RF Parameters

Mode	Default ▾	
Minimum RSSI	-85	dBm
Hysteresis	2	dB
Scan Threshold	-72	dBm
Transition Time	5	Seconds

Voice Call Admission Control

Figure 8-11 shows the Voice Call Admission Control screen of RRM. The default values (Max RF Bandwidth value equals 75 percent) are set high to prevent rejection of calls when suitable capacity is available.

Figure 8-11 Voice Call Admission Control



802.11a > Voice Parameters

Call Admission Control (CAC)

Admission Control (ACM)	☑ Enabled
Load-based AC	☑ Enabled
Max RF Bandwidth (%)	75
Reserved Roaming Bandwidth (%)	10
Expedited bandwidth	☐

Traffic Stream Metrics

Metrics Collection	☑

For best performance, the most accurate assessment of call capacity—*Load-based AC*—should be enabled. *Admission Control* enabled by itself uses the APs capacity to calculate the Call Admission Control (CAC). Load-based AC incorporates the channel capacity into the CAC determination and gives a much more accurate assessment of the current call-carrying capacity of the AP. Settings for the *Max RF bandwidth* and *Reserved Bandwidth* values depend on the VoWLAN handsets, the data rates used, and the other sources of the WLAN load. However, the Max RF Reservation should not be greater than 60 percent. At levels greater than 60 percent, the IEEE 802.11 protocol itself can start to be under stress with increases in retransmission. This can impact call quality even if WMM is being used, particularly if the is a number of voice calls are already in progress. Testing with the Cisco Unified IP Phone 7921G in both the 2.4 GHz and 5 GHz bands using the recommended signal levels and SNR suggests that the minimum value for the *Maximum Bandwidth Reservation* parameter of between 40 to 60 percent is also the best setting for this specific phone. Call quality starts to deteriorate when the *Max RF Bandwidth* is set at or below these levels.

General Cisco Unified Wireless Network Configuration

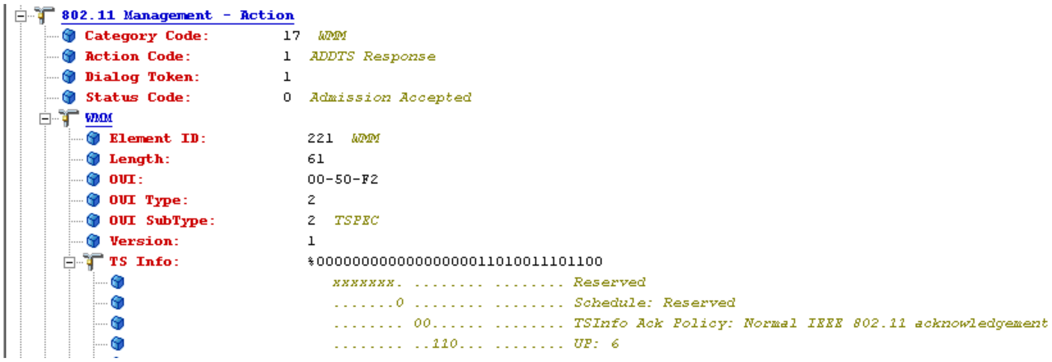
This section focuses on VoWLAN specifics of the WLC network configuration. The connection to the wired network is addressed in the *The Enterprise Mobility 4.1 Design Guide*, as are considerations affecting the decision to implement centralized or distributed WLCs.

The centralized WLC model was used in this design guide because it is the recommended deployment model of the *The Enterprise Mobility 4.1 Design Guide*, but no design features or characteristics unique to the centralized WLC model were implemented. The Cisco Unified IP Phone 7921G handset deployments discussed in this guide works equally well in either a centralized or distributed WLC deployment, but only the centralized model was tested and documented in this guide.

Quality of Service Policy

The quality-of-service (QoS) per-user bandwidth and over the air QoS policy settings on the WLC should be left at their defaults. The WLC, by default, does the appropriate conversion between IEEE class of service (CoS) values and Cisco QoS baseline, when CoS marking is enabled (Wired Protocol 802.1p) Differentiated Services Code Point (DSCP) and CoS values. An example of the a QoS Profile for Platinum QoS with CoS Marking is shown in Figure 8-12.

Figure 8-12 Example Platinum QoS Profile



```
802.11 Management - Action
    Category Code:      17  WMM
    Action Code:        1  ADDTS Response
    Dialog Token:       1
    Status Code:        0  Admission Accepted
    WMM
        Element ID:        221  WMM
        Length:            61
        OUI:               00-50-F2
        OUI Type:          2
        OUI SubType:       2  TSPEC
        Version:           1
        TS Info:           %000000000000000000011010011101100
                              xxxxxxx. ........ ........ Reserved
                              .......0 ........ ........ Schedule: Reserved
                              ........ 00...... ........ TSInfo Ack Policy: Normal IEEE 802.11 acknowledgement
                              ........ ..110... ........ UP: 6
```

We recommend that the QoS policy on the router/switch interfaces connected to the WLC be set to trust the CoS settings of the WLC. This means that the wired network responds to the CoS values controlled by the QoS policy set on the WLC. The WLC does not enforce any policy that changes the WLAN client DSCP values. The WLC policy effects will only be seen in the CoS values associated with the WLAN client traffic. If the routers and switches connecting to the WLC are set to trust DSCP, then a DSCP policy must be created and maintained on those router and switch interfaces—in addition to the policies applied on the WLC. For more information on WLAN QoS and traffic classification, refer to the Chapter 3, "Voice over WLAN Radio Frequency Design."

Note CSCsi78368 means that the WLC sets incorrect CoS values in the 4.1.185 code, but this is fixed in the WLC Release 4.2.61.0.

Mobility Groups

The APs (and associated WLCs) for an area of continuous VoWLAN coverage should be part of the same Mobility Group. If this is not the case, call quality is likely to be affected during a VoWLAN client roam between mobility groups because VoWLAN client state information will not be transferred between the WLCs of the two different groups. Given that there can be up to 24 WLCs per Mobility Group, it is unlikely that there is a requirement for multiple Mobility Groups in most enterprise deployments.

AP Groups

AP Groups were not used in this design guide. Customers might wish to implement AP Groups to map different VLANs on a WLC to the same WLAN SSID on different APs. This would allow VoWLAN client associated to APs in one building to use a different subnet to the VoWLAN clients from another building. The primary purpose of using AP Groups in this manner is to minimize the size of WLAN broadcast domains, or share WLAN client traffic across multiple VLANs. Another purpose is to have the WLAN subnet size fit a standard size used in the general campus design. Unless broadcast or multicast traffic has been enabled on the Cisco Unified Wireless Network, there is no need to minimize subnet size to control the WLAN broadcast domain because the Cisco Unified Wireless Network default prevents broadcast and multicast traffic from being sent over of the WLAN. This allows all the clients on the same WLC's WLAN to be on the same subnet without broadcast/multicast domain issues.

Multicast Traffic

The transmission of multicast and broadcast traffic over the WLAN is disabled by default on the Cisco Unified Wireless Network. Unless there is a specific application requirement (such as the use of *Vocera* badges), it should remained disabled. When multicast is enabled on the Cisco Unified Wireless Network, it is enabled on every WLAN—although it might only be required on a single WLAN. Given that the multicast traffic on a WLAN is sent out every AP radio with clients associated to that WLAN regardless of that client(s) requirements, every effort should be made to minimize the multicast traffic on every WLC WLAN interface. You can minimize the potential affects of multicast traffic by disabling IGMP on interfaces not requiring multicast and filtering multicast traffic on interfaces that have IGMP enabled.

For more information on WLC multicast features, refer to Chapter 6 of the *Enterprise Mobility 4.1 Design Guide* at this URL:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch6_Mcst.html

Note In WLC 4.2 software release, Internet Group Management Protocol (IGMP) snooping is introduced to better direct multicast packets, and block the unwanted multicast traffic addressed above. When this feature is enabled, an access point transmits multicast packets only if a client associated to the access point is subscribed to the multicast group. This feature was not tested and documented this guide, but it is recommended that customers implement the feature.

CHAPTER 9

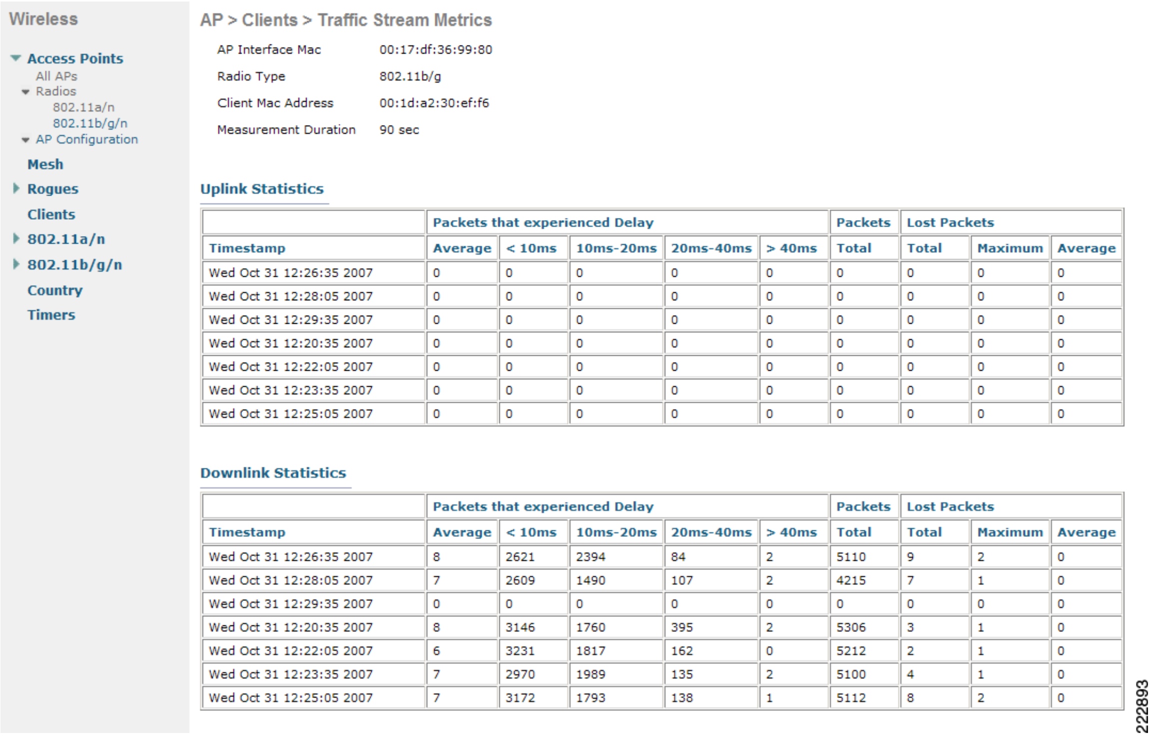
Voice over WLAN Troubleshooting and Management Tools

One of the challenges in mobility is the fact that users are mobile, and while they have an investment in ensuring that their end device is working correctly, they have less of an investment in a piece of geography. That is, while a user will address what they perceive as an equipment issue promptly, they are less likely to spend time addressing what they perceive as coverage issues as they will simply move on to another location. This means that you are more likely to get help desk calls if users cannot connect, but coverage and performance issues are more likely to be anecdotal. Unless time and effort are invested to ensure coverage issues are address proactively, user satisfaction can be low before the issues make into a operations and maintenance case. For this reason the primary focus in this chapter will be the use of tools to translate user anecdotes into system parameters, and tools to proactively identify potential coverage and performance issues.

WLC Tools

The WLC provides many different debug and show commands to assist in general trouble shooting. In the case of VoWLAN two help screens in analyzing VoWLAN quality issues are shown in Figure 9-1 and Figure 9-2. Figure 9-1 shows the client traffic Stream metrics, which provides information upon the packet delay and packet loss experience by a client on an AP. As packet delay and loss are key parameters in VoIP call quality the traffic stream measures provide network insight in to the call quality experienced by a client.

Figure 9-1 WLC Client Traffic Stream Metrics



AP > Clients > Traffic Stream Metrics

AP Interface Mac 00:17:df:36:99:80
Radio Type 802.11b/g
Client Mac Address 00:1d:a2:30:ef:f6
Measurement Duration 90 sec

Uplink Statistics

	Packets that experienced Delay					Packets	Lost Packets		
Timestamp	Average	< 10ms	10ms-20ms	20ms-40ms	> 40ms	Total	Total	Maximum	Average
Wed Oct 31 12:26:35 2007	0	0	0	0	0	0	0	0	0
Wed Oct 31 12:28:05 2007	0	0	0	0	0	0	0	0	0
Wed Oct 31 12:29:35 2007	0	0	0	0	0	0	0	0	0
Wed Oct 31 12:20:35 2007	0	0	0	0	0	0	0	0	0
Wed Oct 31 12:22:05 2007	0	0	0	0	0	0	0	0	0
Wed Oct 31 12:23:35 2007	0	0	0	0	0	0	0	0	0
Wed Oct 31 12:25:05 2007	0	0	0	0	0	0	0	0	0

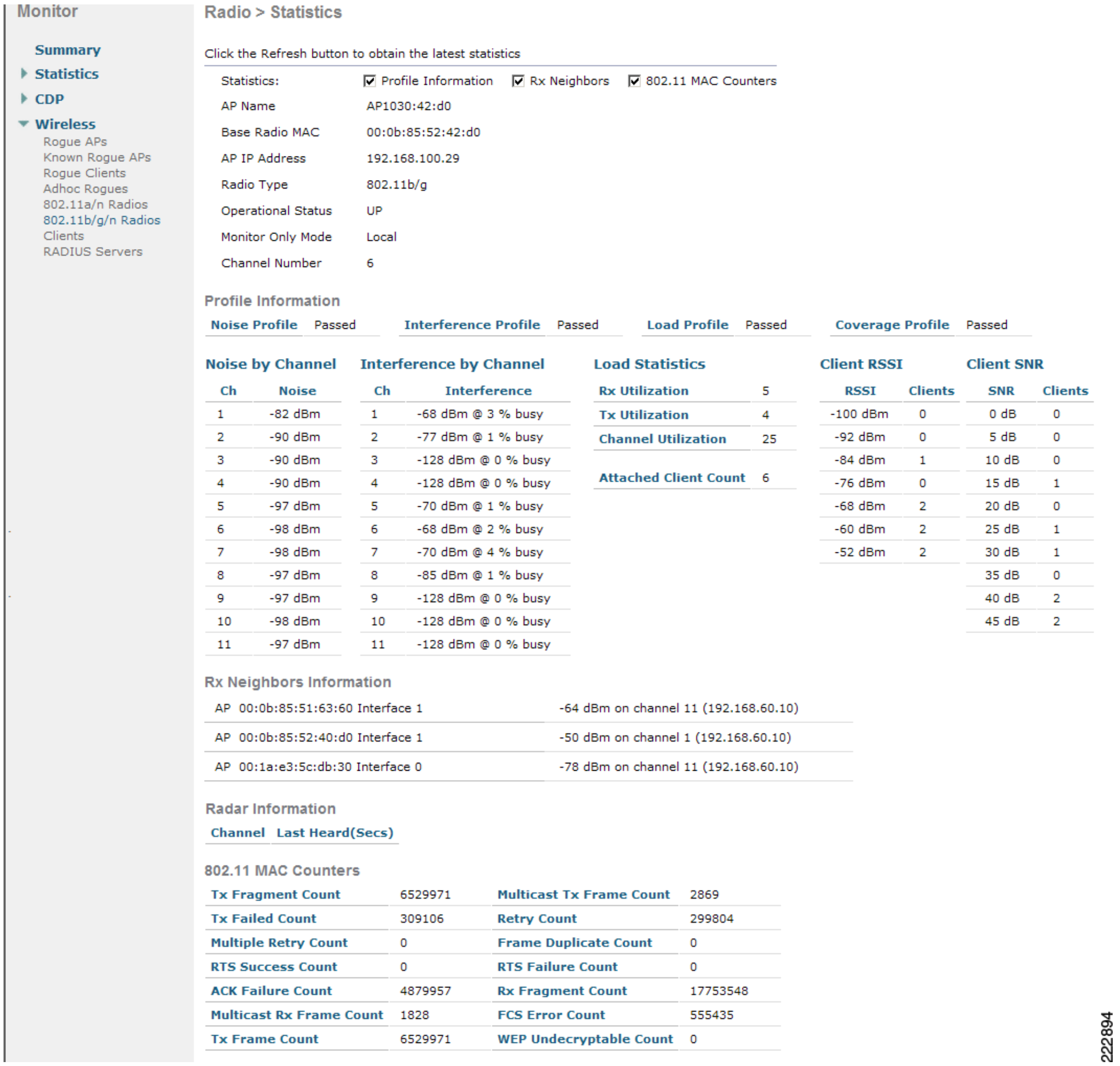
Downlink Statistics

	Packets that experienced Delay					Packets	Lost Packets		
Timestamp	Average	< 10ms	10ms-20ms	20ms-40ms	> 40ms	Total	Total	Maximum	Average
Wed Oct 31 12:26:35 2007	8	2621	2394	84	2	5110	9	2	0
Wed Oct 31 12:28:05 2007	7	2609	1490	107	2	4215	7	1	0
Wed Oct 31 12:29:35 2007	0	0	0	0	0	0	0	0	0
Wed Oct 31 12:20:35 2007	8	3146	1760	395	2	5306	3	1	0
Wed Oct 31 12:22:05 2007	6	3231	1817	162	0	5212	2	1	0
Wed Oct 31 12:23:35 2007	7	2970	1989	135	2	5100	4	1	0
Wed Oct 31 12:25:05 2007	7	3172	1793	138	1	5112	8	2	0

Note In Figure 9-1, uplink statistics have not been reported by the VoWLAN client, and therefore the data is all zeros.

Figure 9-2 shows AP radio statistics, including channel load, channel noise, client RSSI and SNR and AP Neighbor information from RRM. This can provide more general information about the RF environment that VoWLAN clients are operating in which parameters may be impacting VoWLAN call quality.

Figure 9-2 AP Radio Statistics



Radio > Statistics

Click the Refresh button to obtain the latest statistics

Statistics:	☑ Profile Information ☑ Rx Neighbors ☑ 802.11 MAC Counters
AP Name	AP1030:42:d0
Base Radio MAC	00:0b:85:52:42:d0
AP IP Address	192.168.100.29
Radio Type	802.11b/g
Operational Status	UP
Monitor Only Mode	Local
Channel Number	6

Profile Information

Noise Profile	Passed	Interference Profile	Passed	Load Profile	Passed	Coverage Profile	Passed

Noise by Channel

Ch	Noise
1	-82 dBm
2	-90 dBm
3	-90 dBm
4	-90 dBm
5	-97 dBm
6	-98 dBm
7	-98 dBm
8	-97 dBm
9	-97 dBm
10	-98 dBm
11	-97 dBm

Interference by Channel

Ch	Interference
1	-68 dBm @ 3 % busy
2	-77 dBm @ 1 % busy
3	-128 dBm @ 0 % busy
4	-128 dBm @ 0 % busy
5	-70 dBm @ 1 % busy
6	-68 dBm @ 2 % busy
7	-70 dBm @ 4 % busy
8	-85 dBm @ 1 % busy
9	-128 dBm @ 0 % busy
10	-128 dBm @ 0 % busy
11	-128 dBm @ 0 % busy

Load Statistics

Rx Utilization	5
Tx Utilization	4
Channel Utilization	25
Attached Client Count	6

Client RSSI

RSSI	Clients
-100 dBm	0
-92 dBm	0
-84 dBm	1
-76 dBm	0
-68 dBm	2
-60 dBm	2
-52 dBm	2

Client SNR

SNR	Clients
0 dB	0
5 dB	0
10 dB	0
15 dB	1
20 dB	0
25 dB	1
30 dB	1
35 dB	0
40 dB	2
45 dB	2

Rx Neighbors Information

AP 00:0b:85:51:63:60 Interface 1	-64 dBm on channel 11 (192.168.60.10)
AP 00:0b:85:52:40:d0 Interface 1	-50 dBm on channel 1 (192.168.60.10)
AP 00:1a:e3:5c:db:30 Interface 0	-78 dBm on channel 11 (192.168.60.10)

Radar Information

Channel	Last Heard(Secs)

802.11 MAC Counters

Tx Fragment Count	6529971	Multicast Tx Frame Count	2869
Tx Failed Count	309106	Retry Count	299804
Multiple Retry Count	0	Frame Duplicate Count	0
RTS Success Count	0	RTS Failure Count	0
ACK Failure Count	4879957	Rx Fragment Count	17753548
Multicast Rx Frame Count	1828	FCS Error Count	555435
Tx Frame Count	6529971	WEP Undecryptable Count	0

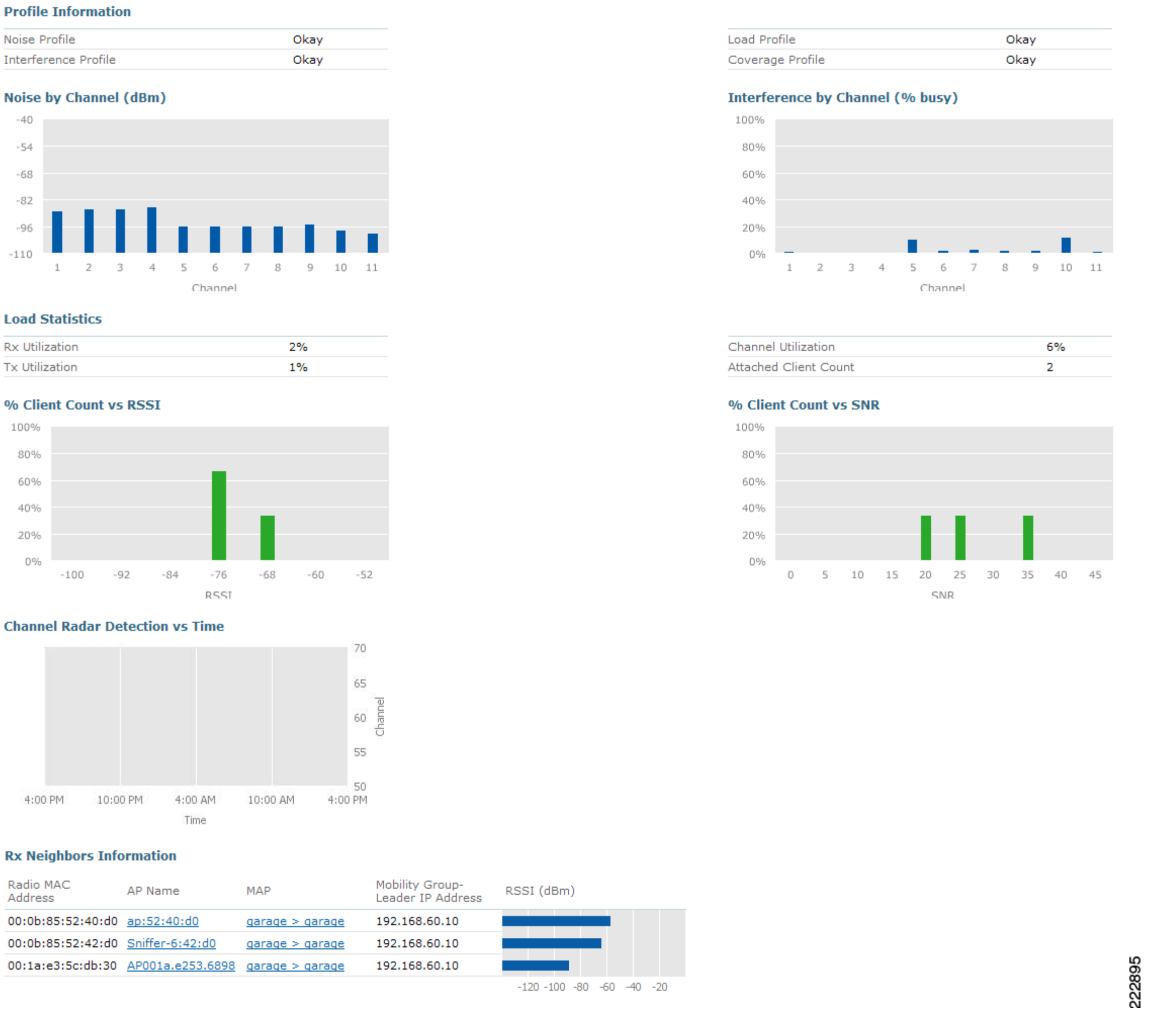
WCS Tools

While the WLC can provide AP statistics and client traffic stream statistics, the WCS is the best place to start VoWLAN trouble shooting. This is because the WCS provides the topological visibility through its building and floor plan maps providing a way to translate the user complaint "I seem to have trouble with calls in building *x* on floor *y*" into there seems to be an issue involving APs X1, X2, and X3. In addition to providing this translation between the physical world to the network world, the WCS provides a centralized location for viewing and aggregation of the same statistics shown by the WLC, as well as providing reports of how key parameters have changed over time

Monitoring

Figure 9-3 shows similar AP statistics to those shown in by the WLC in Figure 9-2; the WLC allows these to be shown in text format or graphical format.

Figure 9-3 AP Statistics



Profile Information

Noise Profile	Okay	Load Profile	Okay
Interference Profile	Okay	Coverage Profile	Okay

Load Statistics

Rx Utilization	2%	Channel Utilization	6%
Tx Utilization	1%	Attached Client Count	2

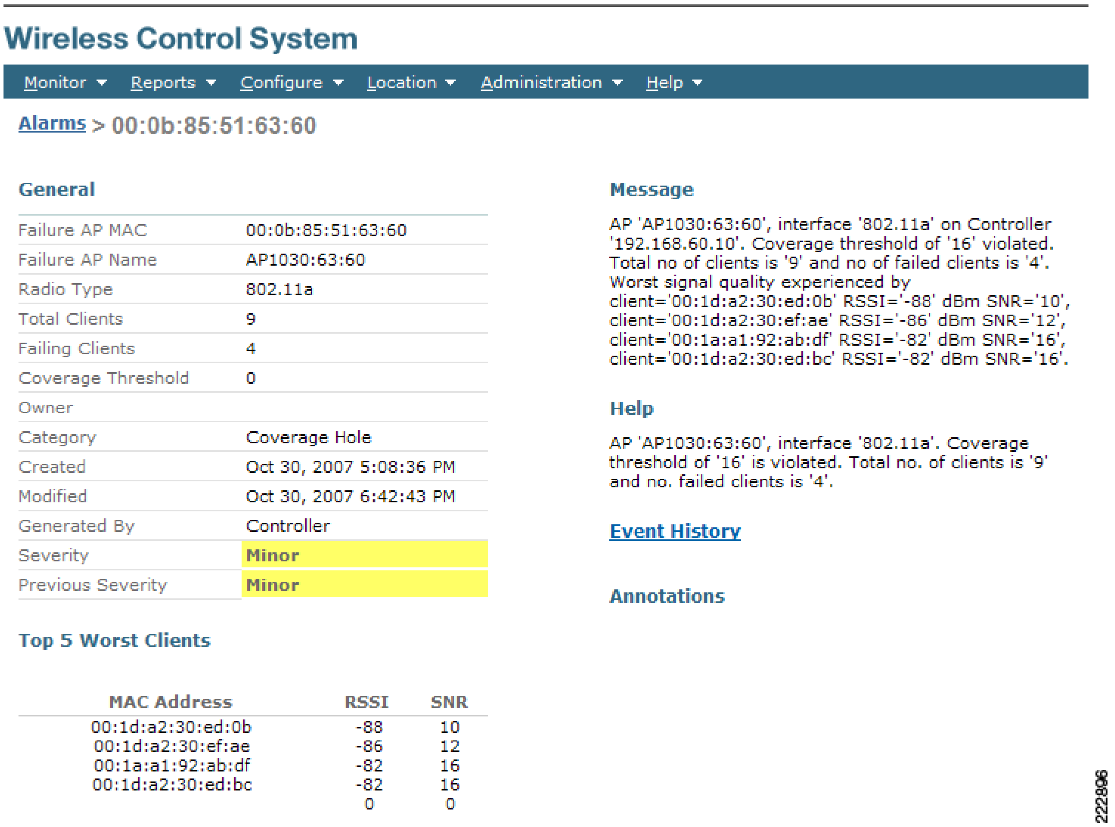
Rx Neighbors Information

Radio MAC Address	AP Name	MAP	Mobility Group-Leader IP Address	RSSI (dBm)
00:0b:85:52:40:d0	ap:52:40:d0	garage > garage	192.168.60.10	
00:0b:85:52:42:d0	Sniffer-6:42:d0	garage > garage	192.168.60.10	
00:1a:e3:5c:db:30	AP001a.e253.6898	garage > garage	192.168.60.10	

Alarms

The WCS provides an aggregation point for alarms. Figure 9-4 shows an example of an alarm that may provide input to a VoWLAN issue, that is, a Coverage Hole alarm. Excessive hole coverage alarms that are unrelated to an actual AP issue may indicate a RF coverage issue users are in an area inadequately covered due either to planning, implementation or operational issue. The Coverage Hole alarms may also be indicative of a sticky client issue where a WLAN client is not roaming into a better coverage area.

Figure 9-4 Hole Coverage Alarm



Alarms > 00:0b:85:51:63:60

General

Failure AP MAC	00:0b:85:51:63:60
Failure AP Name	AP1030:63:60
Radio Type	802.11a
Total Clients	9
Failing Clients	4
Coverage Threshold	0
Owner	
Category	Coverage Hole
Created	Oct 30, 2007 5:08:36 PM
Modified	Oct 30, 2007 6:42:43 PM
Generated By	Controller
Severity	Minor
Previous Severity	Minor

Message

AP 'AP1030:63:60', interface '802.11a' on Controller '192.168.60.10'. Coverage threshold of '16' violated. Total no of clients is '9' and no of failed clients is '4'. Worst signal quality experienced by client='00:1d:a2:30:ed:0b' RSSI='-88' dBm SNR='10', client='00:1d:a2:30:ef:ae' RSSI='-86' dBm SNR='12', client='00:1a:a1:92:ab:df' RSSI='-82' dBm SNR='16', client='00:1d:a2:30:ed:bc' RSSI='-82' dBm SNR='16'.

Help

AP 'AP1030:63:60', interface '802.11a'. Coverage threshold of '16' is violated. Total no. of clients is '9' and no. failed clients is '4'.

Event History

Annotations

Top 5 Worst Clients

MAC Address	RSSI	SNR
00:1d:a2:30:ed:0b	-88	10
00:1d:a2:30:ef:ae	-86	12
00:1a:a1:92:ab:df	-82	16
00:1d:a2:30:ed:bc	-82	16
	0	0

Reports

The WCS reports provide insight into key VoWLAN parameters over time, helping to correlate network parameters with the timing of particular incidents, and allowing trending of key parameters overtime. Figure 9-5 shows an example of the a graph from the AP TxPower and Channel report, excessive changes in this area may indicate a systematic RF interference issue to be investigated or an indication that the Auto-RF configuration of the network may need to be tuned to better fit the environment and deployment.

Figure 9-5 Power and Channel Reports

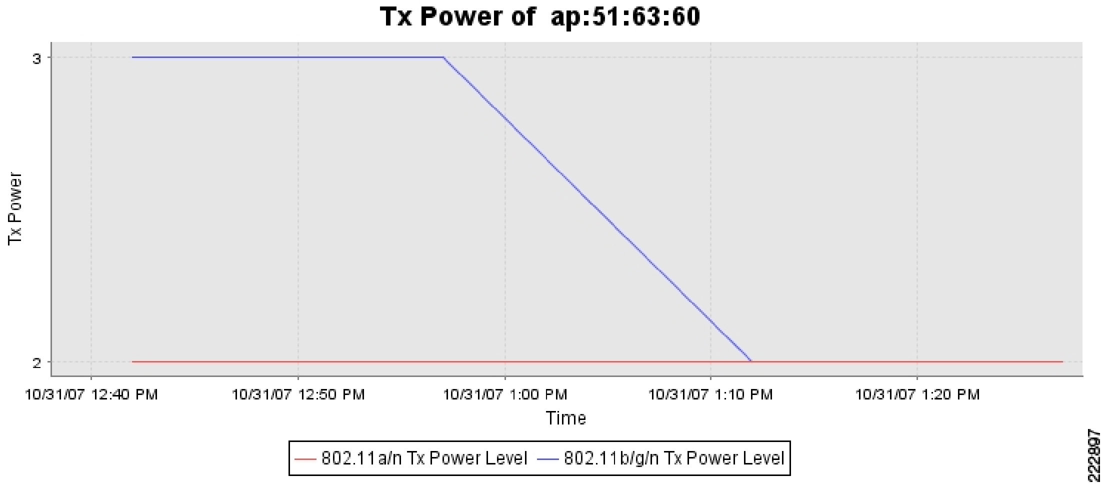


Figure 9-6 shows an example of the voice bandwidth statistics report, these reports can used to track possible call capacity and admission control issues.

Figure 9-6 Voice Statistics

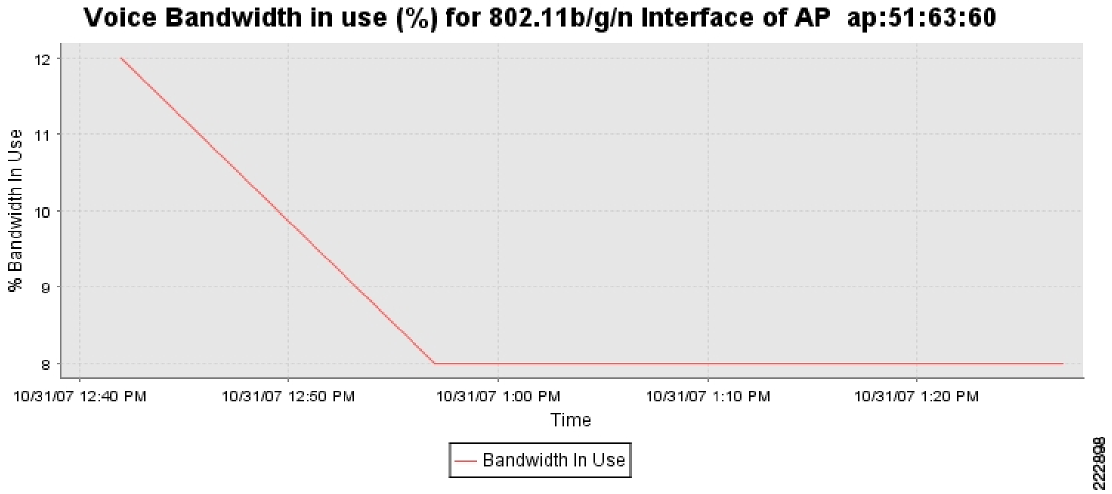
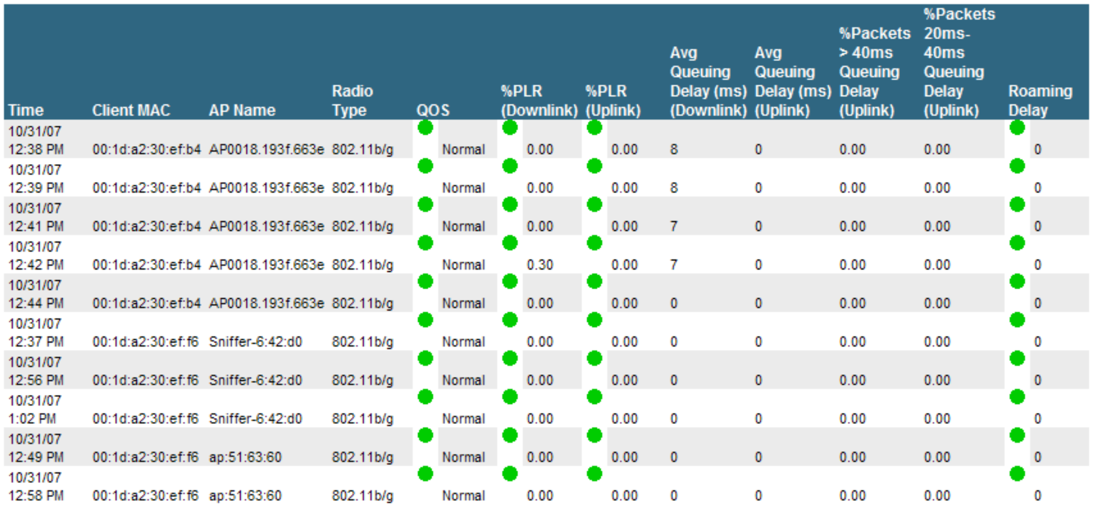


Figure 9-7 shows an example of the client traffic stream metrics, similar to that shown in the WLC in Figure 9-1, but it has the advantage of providing information upon roaming delay, and providing client traffic stream information across APs, and WLCs.

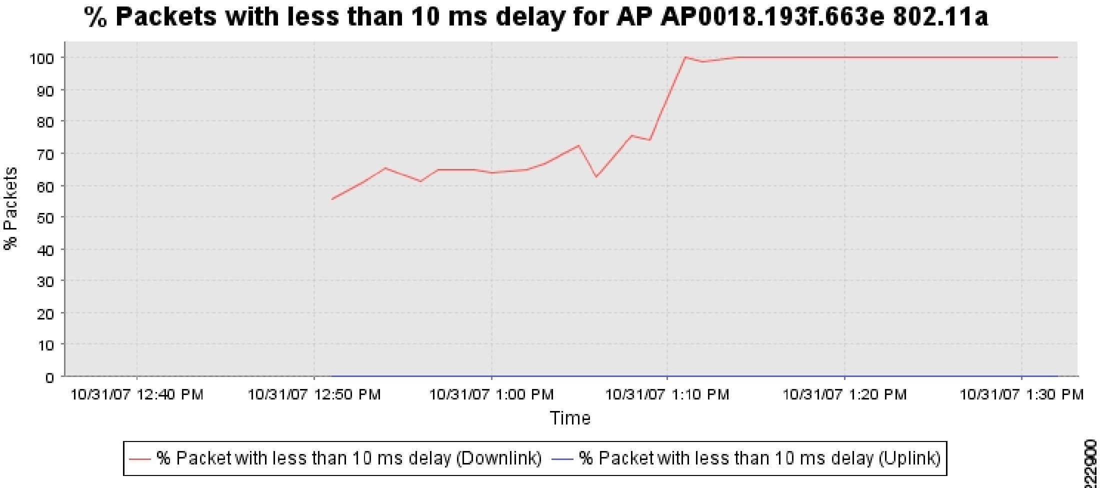
Figure 9-7 Traffic Stream Statistics



Time	Client MAC	AP Name	Radio Type	QOS	%PLR (Downlink)	%PLR (Uplink)	Avg Queuing Delay (ms) (Downlink)	Avg Queuing Delay (ms) (Uplink)	%Packets > 40ms Queuing Delay (Uplink)	%Packets 20ms-40ms Queuing Delay (Uplink)	Roaming Delay
10/31/07 12:38 PM	00:1d:a2:30:ef:b4	AP0018.193f.663e	802.11b/g	● Normal	● 0.00	● 0.00	8	0	0.00	0.00	● 0
10/31/07 12:39 PM	00:1d:a2:30:ef:b4	AP0018.193f.663e	802.11b/g	● Normal	● 0.00	● 0.00	8	0	0.00	0.00	● 0
10/31/07 12:41 PM	00:1d:a2:30:ef:b4	AP0018.193f.663e	802.11b/g	● Normal	● 0.00	● 0.00	7	0	0.00	0.00	● 0
10/31/07 12:42 PM	00:1d:a2:30:ef:b4	AP0018.193f.663e	802.11b/g	● Normal	● 0.30	● 0.00	7	0	0.00	0.00	● 0
10/31/07 12:44 PM	00:1d:a2:30:ef:b4	AP0018.193f.663e	802.11b/g	● Normal	● 0.00	● 0.00	0	0	0.00	0.00	● 0
10/31/07 12:37 PM	00:1d:a2:30:ef:f6	Sniffer-6:42:d0	802.11b/g	● Normal	● 0.00	● 0.00	0	0	0.00	0.00	● 0
10/31/07 12:56 PM	00:1d:a2:30:ef:f6	Sniffer-6:42:d0	802.11b/g	● Normal	● 0.00	● 0.00	0	0	0.00	0.00	● 0
10/31/07 1:02 PM	00:1d:a2:30:ef:f6	Sniffer-6:42:d0	802.11b/g	● Normal	● 0.00	● 0.00	0	0	0.00	0.00	● 0
10/31/07 12:49 PM	00:1d:a2:30:ef:f6	ap:51:63:60	802.11b/g	● Normal	● 0.00	● 0.00	0	0	0.00	0.00	● 0
10/31/07 12:58 PM	00:1d:a2:30:ef:f6	ap:51:63:60	802.11b/g	● Normal	● 0.00	● 0.00	0	0	0.00	0.00	● 0

Figure 9-8 shows an example of a traffic stream metrics graph which provides tracking of key stream parameters over time. This allows the correlation of traffic stream parameters with specific events and the trending of these parameters over time.

Figure 9-8 Traffic Stream Metrics Graph



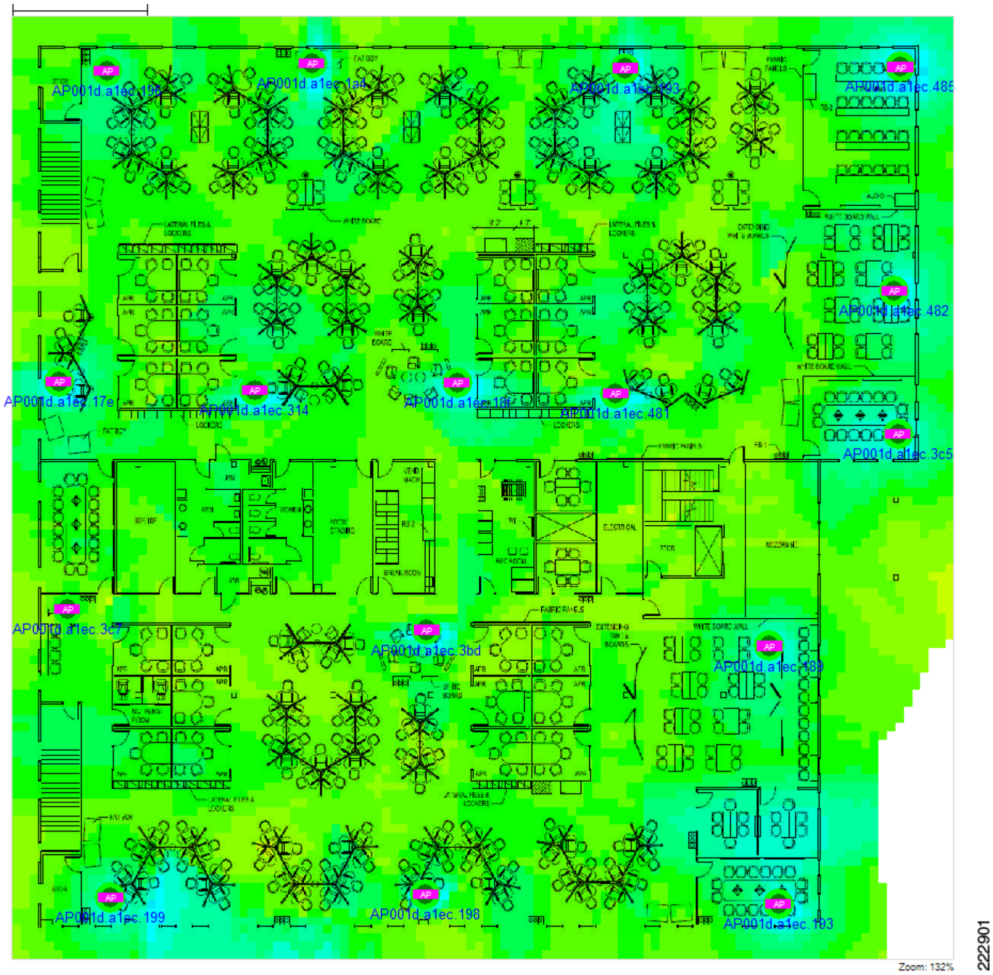
Third Party Tools

AirMagnet Surveyor Pro

We have already discussed the importance of site surveys in RF design session. While the WCS planning tools and WCS RF visualization tools provide a picture of the RF environment, but these are predictions of the RF environment, and if there is one invariable law of computing it is “Garbage in Garbage Out”.

Despite the effort and care applied at the front end of the system the only true measure of their quality and the prediction system is to measure the output. The means of output measurement is a site survey. A site survey can be as simple as measuring signal strength and performance on sample client devices, but, site survey tools such as Airmagnet provide a much richer interface view of the data collected and value added tools to analyze the RF data. The site survey data associated with the floor plan, as shown in Figure 9-9, allows the RF coverage maps of the WCS be validated against data in the WLAN client domain. Given that the WCS maps are a key remote trouble shooting tool, it is also key that these maps be validated by performing a site survey. http://www.airmagnet.com/products/survey/.

Figure 9-9 Example of an Airmagnet Survey

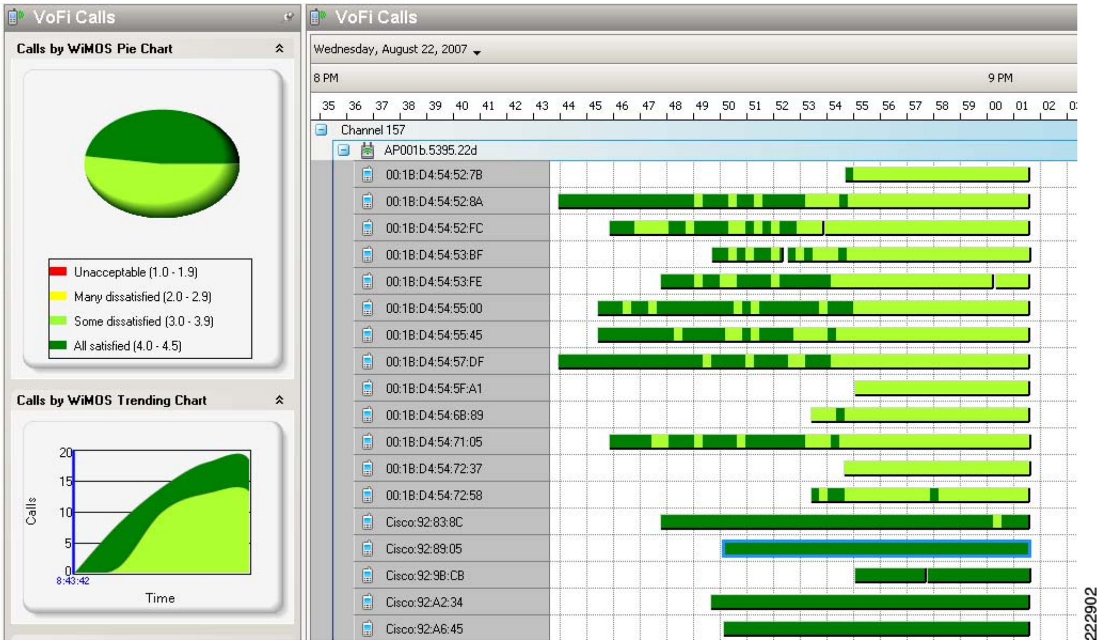


In addition the Airmagnet Site Survey through its AirWise feature provides and assessment of the the VoWLAN readiness of the environment analyzing key parameters such as coverage and AP overlap, and providing planning prediction of network changes based upon the collected survey data.

VoWLAN Analysis

One of the challenges in VoWLAN analysis is determining call quality. Most VoIP systems provide a Mean Opinion Score (MoS) score, but these MoS scores are not always readily accessible and their values are not consistent across devices. The VoFi analyzer from Airmagnet provides a readily accessible means of measuring VoWLAN voice quality overtime for multiple handsets. Figure 9-10 shows an example of a VoFi Analyzer capture for a group of 11a handsets. Section 1 shows a pie chart of the distribution of MoS scores across handsets, section 2 shows the a histogram of calls and MoS scores over time, and section three shows the MoS values of individual handsets over time.

Figure 9-10 VoFi 11a Analysis



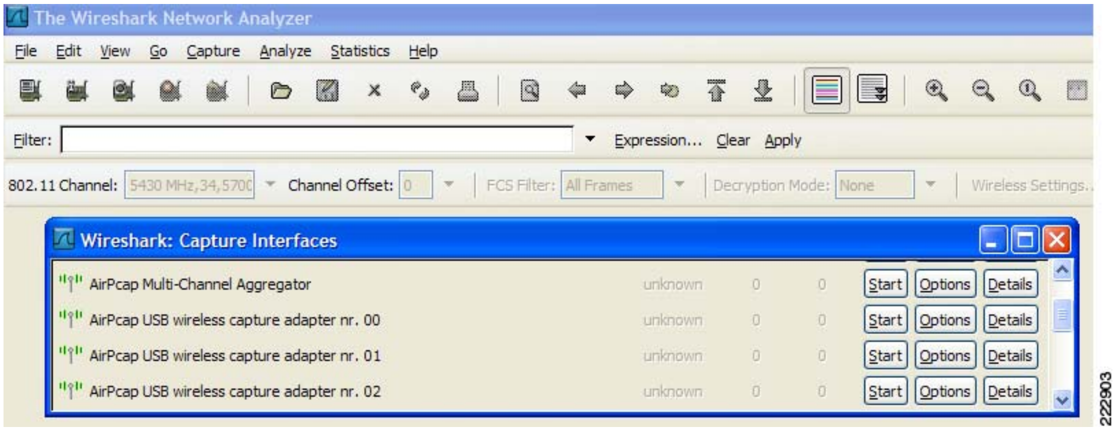
For more information about VoFi11a, refer to the following URL:

http://www.airmagnet.com/products/vofi_analyzer/

CACE Technologies and Wireshark

One of the challenges in troubleshooting WLAN issues is capturing traffic on multiple channels while maintaining accurate timing information. CACE Technologies provides USB WLAN NICs, and a USB hub with drivers to allow the multiple WLAN NICs configured for different channels and connected to the hub, can deliver capture data to Wireshark. Figure 9-11 shows an example of the AirPcap interfaces for Wireshark. The interfaces are available individually and an aggregated capture from all AirPcap adaptors is also available.

Figure 9-11 Wireshark Capture Interfaces


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
Wireless Settings...
Wireshark: Capture Interfaces
222903

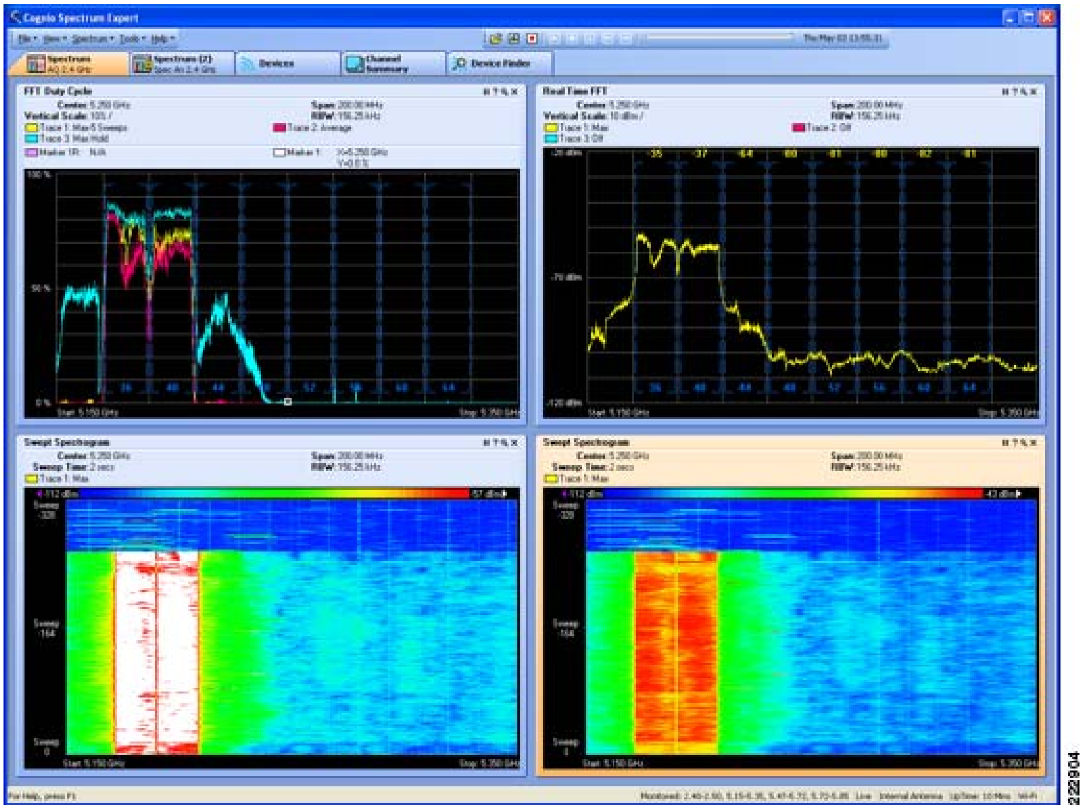
802.11 Channel: 5430 MHz,34,5700 Channel Offset: 0 FCS Filter: All Frames Decryption Mode: None

AirPcap Multi-Channel Aggregator	unknown	0	0	Start	Options	Details
AirPcap USB wireless capture adapter nr. 00	unknown	0	0	Start	Options	Details
AirPcap USB wireless capture adapter nr. 01	unknown	0	0	Start	Options	Details
AirPcap USB wireless capture adapter nr. 02	unknown	0	0	Start	Options	Details

Cisco Spectrum Expert

WLAN networks can suffer performance degradation caused by changes in the environment. Interference—caused by WLAN transmissions as well as signals radiating from WLAN electronic equipment—accounts for the majority of spectrum problems. Interfering devices may include Bluetooth devices, fluorescent lights, microwave ovens, wireless video and audio monitors, cordless computer mice, and millions of other device types. A standard WLAN site survey tool is designed to measure WLAN coverage. It uses a WLAN chipset to measure the signal strength of APs as you move around the building. Unfortunately, WLAN chips are designed to decode WLAN signals only, and can't tell you much about interference from other WLAN devices. (This is the same limitation experienced when using a WLAN packet analysis tool.) A WLAN site survey tool might indicate a general area where a WLAN signal was observed. But the tool can't directly help you determine the nature of the interference, the type of device causing it, or where the device is located. The Cisco Spectrum Expert analyzer has intelligent spectrum management tools that provide a straightforward view into exactly what devices are on the network at any given time and where they are located. With such visibility, enterprises can address critical problems dynamically and can also set policies that eliminate or control interfering devices that might be clogging the WLAN spectrum. At the time of writing, Cisco Spectrum Expert is a recent Cisco acquisition, please check www.cisco.com for the most up to date information on Cisco Spectrum Expert's availability and capabilities

Figure 9-12 Example Cisco Spectrum Expert Screen Capture



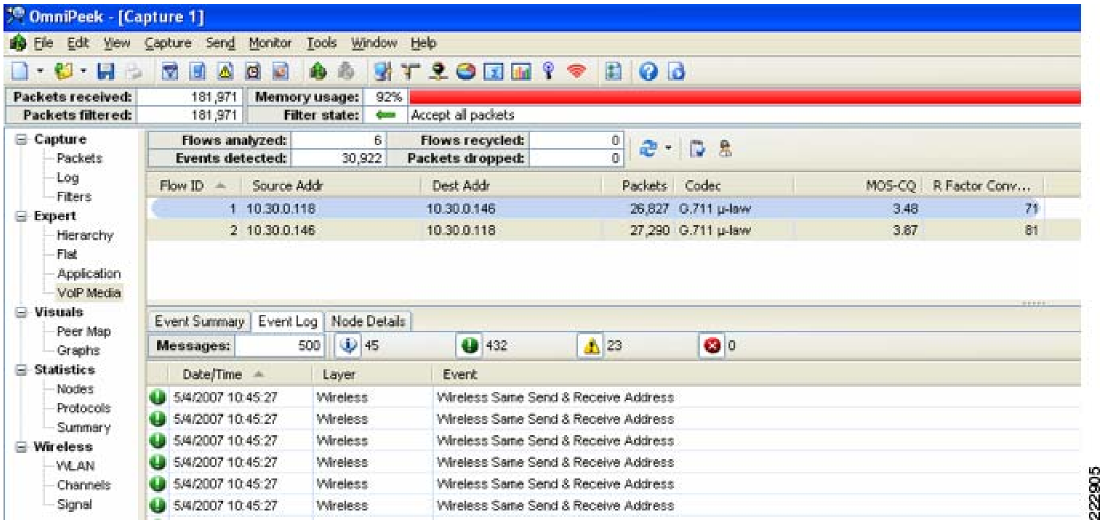
For more information about Cisco Spectrum Expert, refer to the following URL:

http://www.cisco.com/en/US/products/ps9393/index.html

WildPackets OmniPeek

The Omni Peak network analyzer provides comprehensive WLAN protocols decodes and an filtering as well as VoIP analysis. Unfortunately the VoIP analysis like that of the Wireshark relies upon analyzing the RTP stream, which on a typical WLAN would encrypted and unavailable from a WLAN capture. For VoIP analysis the capture and analysis must be performed after the WLC.

Figure 9-13 Example OmniPeek VoIP Analysis



Packets received:	181,971	Memory usage:	92%
Packets filtered:	181,971	Filter state:	Accept all packets

Flows analyzed:	6	Flows recycled:	0
Events detected:	30,922	Packets dropped:	0

Flow ID	Source Addr	Dest Addr	Packets	Codec	MOS-CQ	R Factor Conv...
1	10.30.0.118	10.30.0.146	26,827	G.711 µ-law	3.48	71
2	10.30.0.146	10.30.0.118	27,290	G.711 µ-law	3.87	81

Messages: 500 ⓘ 45 ● 432 ⚠ 23 ⊗ 0

Date/Time	Layer	Event
5/4/2007 10:45:27	Wireless	Wireless Same Send & Receive Address
5/4/2007 10:45:27	Wireless	Wireless Same Send & Receive Address
5/4/2007 10:45:27	Wireless	Wireless Same Send & Receive Address
5/4/2007 10:45:27	Wireless	Wireless Same Send & Receive Address
5/4/2007 10:45:27	Wireless	Wireless Same Send & Receive Address
5/4/2007 10:45:27	Wireless	Wireless Same Send & Receive Address

For more information about OmniPeek, refer to the following URL:

http://www.wildpackets.com/products/omnipeek/overview

CHAPTER 10

Cisco Unified IP Phone 7921 Implementation for Voice over WLAN

This chapter describes how to deploy the Cisco Unified Wireless IP Phone 7921G in the context of a Voice over WLAN (VoWLAN) environment. This chapter provides a brief introduction to the Cisco Unified Wireless IP Phone 7921G in general which is followed by detailed implementation guidance about the following deployment topics:

- Network Connectivity Test Configuration for Cisco Unified Wireless IP Phone 7921, page 10-2
- Cisco Unified Wireless IP Phone 7921 Security, page 10-16
- Cisco Unified Wireless IP Phone 7921 RF Considerations, page 10-24
- Cisco Unified Wireless IP Phone 7921 QoS, page 10-27
- Cisco Unified Wireless IP Phone 7921 Troubleshooting, page 10-33

Cisco Unified Wireless IP Phone 7921 Overview

The Cisco Unified Wireless IP Phone 7921G is an IEEE 802.11 dual-band wireless device that provides comprehensive voice communications in conjunction with Cisco Unified Communications Manager and Cisco Aironet IEEE 802.11a/b/g access points (AP) in a private business communications network. This phone model supports G.711a, G.711u, G.729a and G.729ab audio compression coder-decoders (CODEC). You must configure and manage a wireless IP phone like other IP phones and wireless devices on your network. The wireless IP phone supports multiple lines and most of the IP phone features of other Cisco Unified IP phones. Figure 10-1 shows the Cisco Unified Wireless IP Phone 7921G.

Figure 10-1 Cisco Unified Wireless IP Phone 7921G

Refer to the to the following URL for the complete list of Cisco Unified Wireless IP Phone 7921G features, specifications, and capabilities:

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

Network Connectivity Test Configuration for Cisco Unified Wireless IP Phone 7921

This section provides the minimal configuration necessary to get the Cisco Unified Wireless IP Phone 7921 connected to the network and communicating with the Cisco Unified Communications Manager. The intent of this section is to make it as simple as possible to verify that the network infrastructure is correctly configured for 7921 connectivity. Subsequent sections provide guidance for the addition of the necessary security, RF, and QoS features. Specific topics addressed in this section include the following:

- WLAN Controller Network Connectivity Test Configuration, page 10-2
- Network Infrastructure Base Configuration, page 10-4
- Cisco Unified Communications Manager Base Configuration, page 10-10
- Cisco Unified Wireless IP Phone 7921 Base Configuration, page 10-13
- Trace Analysis for a Base Configuration, page 10-14

Warning **This network connectivity test configuration should not be left active in a production network, as it provides no security against unauthorized access.**

WLAN Controller Network Connectivity Test Configuration

This section provides implementation guidance for initial WLAN Controller configuration.

Creating a Voice WLAN

Creating a WLAN with the minimum necessary configuration needed to test Cisco Unified Wireless IP Phone 7921 connectivity can be done using the following steps on the controller GUI.

Step 1 Click the **WLANs** tab in the controller GUI.

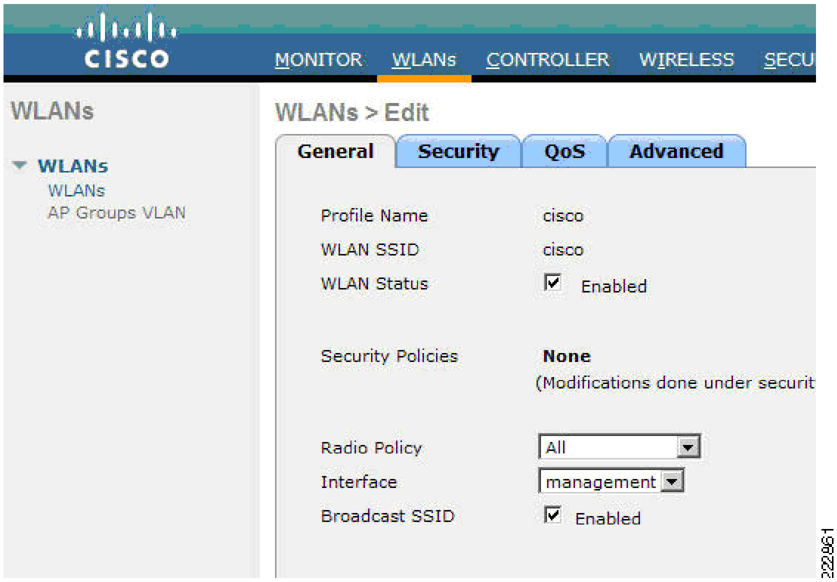
Step 2 Click the **New** button at the top-right corner of the page.

Step 3 For the new WLAN, define a profile name and use the Cisco Unified Wireless IP Phone 7921 default of **cisco** for the SSID.

Step 4 Click **Apply**.

Step 5 The *WLANs > Edit* page loads. See Figure 10-2.

Figure 10-2 WLANs > Edit Page



Profile Name cisco
WLAN SSID cisco
WLAN Status ☑ Enabled
Security Policies **None**
(Modifications done under securit
Radio Policy All
Interface management
Broadcast SSID ☑ Enabled

\

Step 6 Check **WLAN Status** box to signal that this new WLAN should be enabled.

Step 7 Change the *Interface* drop-down box to point to a user-defined dynamic interface (you must have predefined a dynamic interface; do not use the management interface)

Step 8 Click the **Security** tab.

Step 9 Change the *Layer-2 Security* drop-down box to **None**.

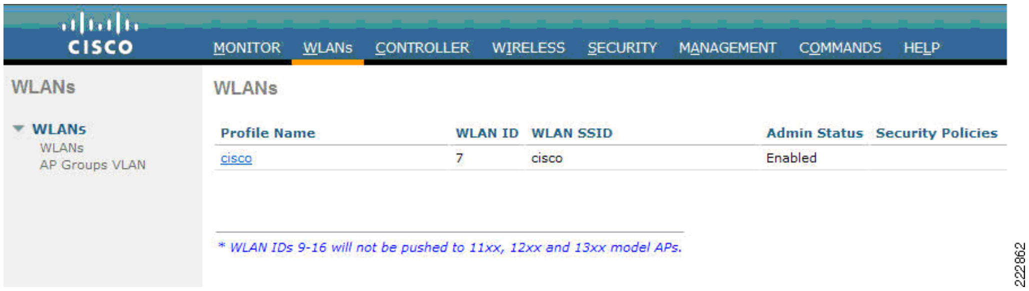
Step 10 Click the **QoS** tab.

Step 11 Change the *Quality of Service (QoS)* drop-down box to **Platinum (voice).**

Step 12 Click the **Apply** button at the top-right corner of the page

When the base controller WLAN configuration is complete, the WLAN window should look similar to Figure 10-3.

Figure 10-3 WLANs Page with Base Configuration



Profile Name	WLAN ID	WLAN SSID	Admin Status	Security Policies
cisco	7	cisco	Enabled	

* WLAN IDs 9-16 will not be pushed to 11xx, 12xx and 13xx model APs.

Network Infrastructure Base Configuration

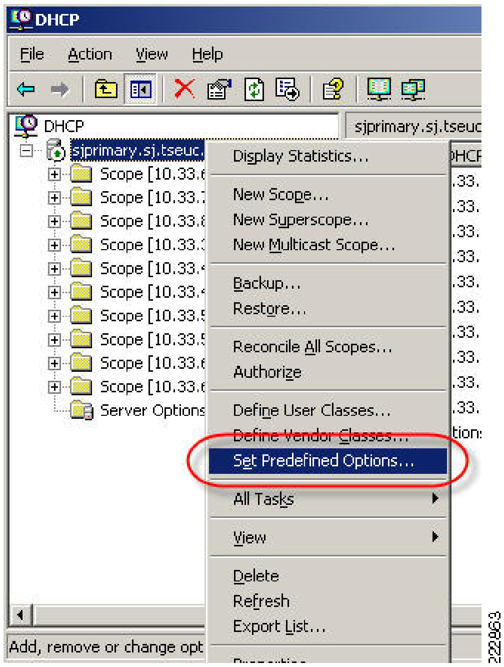
The network infrastructure used by the Cisco Unified Wireless IP Phone 7921 must provide DNS and DHCP services. These services are required for any Cisco IP phone, so they might be previously defined in many customer networks. If they are not defined, the following two sections provide details on how to define them.

Configuring the DHCP Server to Support Cisco Unified Communications Manager Option 150

To connect any Cisco IP phone, including the Cisco Unified Wireless IP Phone 7921, you must configure your DHCP server to provide option 150—the address of the TFTP server used by the phones to download the latest firmware version. Most networks use the default TFTP server provided with the Cisco Unified Communications Manager itself, so option 150 in the phones scope must point to the Cisco Unified Communications Manager IP address.

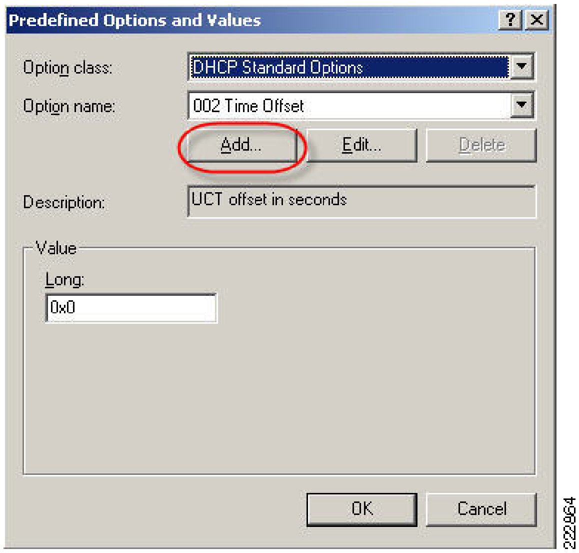
Step 1 Right-click appropriate DHCP Server and select **Set Predefined Options**. See Figure 10-4.

Figure 10-4 Setting Predefined Options



Step 2 Click **Add** in the *Predefined Options and Values* pop-up window. See Figure 10-5.

Figure 10-5 Selecting the Add Option



Option class: DHCP Standard Options

Option name: 002 Time Offset

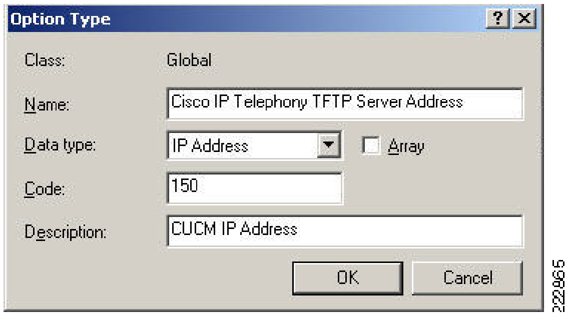
Description: UCT offset in seconds

Value

Long: 0x0

Step 3 Fill out the new option and click **OK**. See Figure 10-6.

Figure 10-6 Entering the Option Type Information



Option Type

Class: Global

Name: Cisco IP Telephony TFTP Server Address

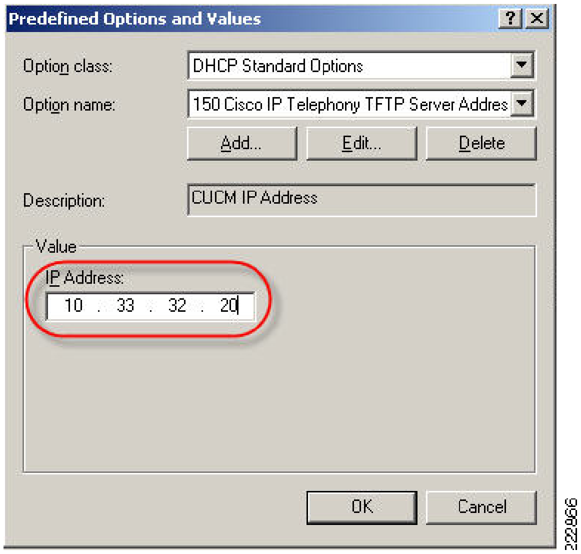
Data type: IP Address ☐ Array

Code: 150

Description: CUCM IP Address

Step 4 Enter in the *IP address* of the Cisco Unified Communications Manager and click **OK.** See Figure 10-7.

Figure 10-7 Entering IP Address in Predefined Options and Values



Predefined Options and Values

Option class: DHCP Standard Options

Option name: 150 Cisco IP Telephony TFTP Server Addres

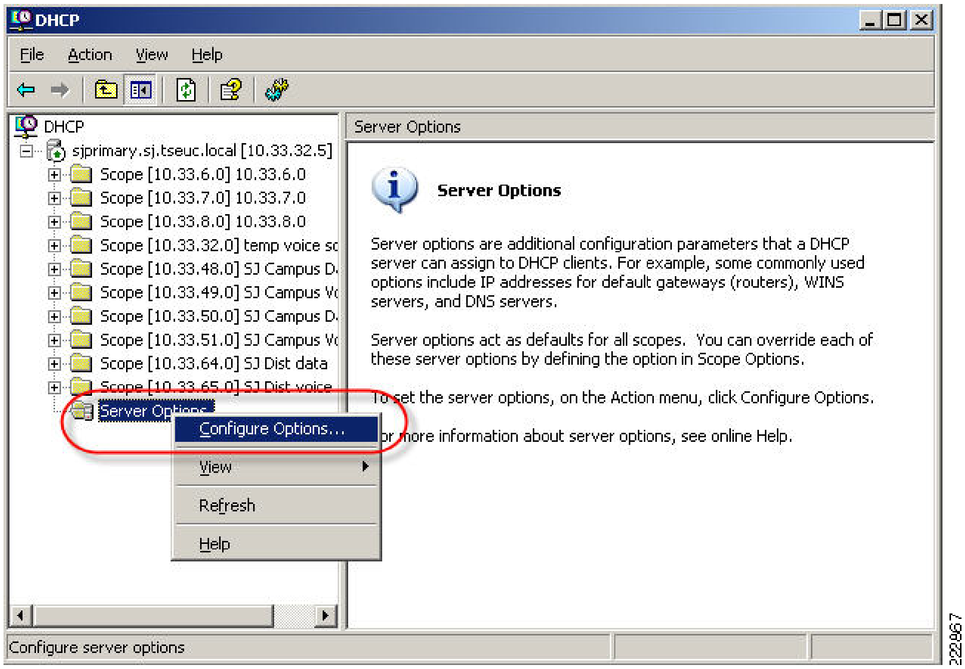
Description: CUCM IP Address

Value

IP Address: 10 . 33 . 32 . 20

Step 5 Configure the DHCP server to pass the newly defined option 150 to all DHCP clients. Select **Server Options**, then click **Configure Options**. See Figure 10-8.

Figure 10-8 Choosing DHCP Server Configuration Options



DHCP
sjprimary.sj.tseuc.local [10.33.32.5]
Scope [10.33.6.0] 10.33.6.0
Scope [10.33.7.0] 10.33.7.0
Scope [10.33.8.0] 10.33.8.0
Scope [10.33.32.0] temp voice sc
Scope [10.33.48.0] SJ Campus D
Scope [10.33.49.0] SJ Campus Vc
Scope [10.33.50.0] SJ Campus D
Scope [10.33.51.0] SJ Campus Vc
Scope [10.33.64.0] SJ Dist data
Scope [10.33.65.0] SJ Dist voice
Server Options

Server Options

Server Options

Server options are additional configuration parameters that a DHCP server can assign to DHCP clients. For example, some commonly used options include IP addresses for default gateways (routers), WINS servers, and DNS servers.

Server options act as defaults for all scopes. You can override each of these server options by defining the option in Scope Options.

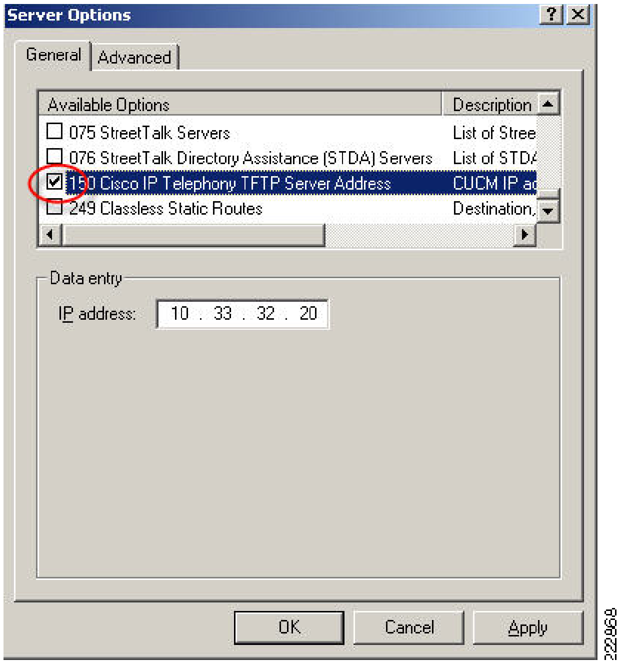
To set the server options, on the Action menu, click Configure Options.

For more information about server options, see online Help.

Configure server options

Step 6 Select your newly created class from the drop-down menu, check your newly created option 150, and click **OK**. See Figure 10-9.

Figure 10-9 Choosing Option 150 from Server Options

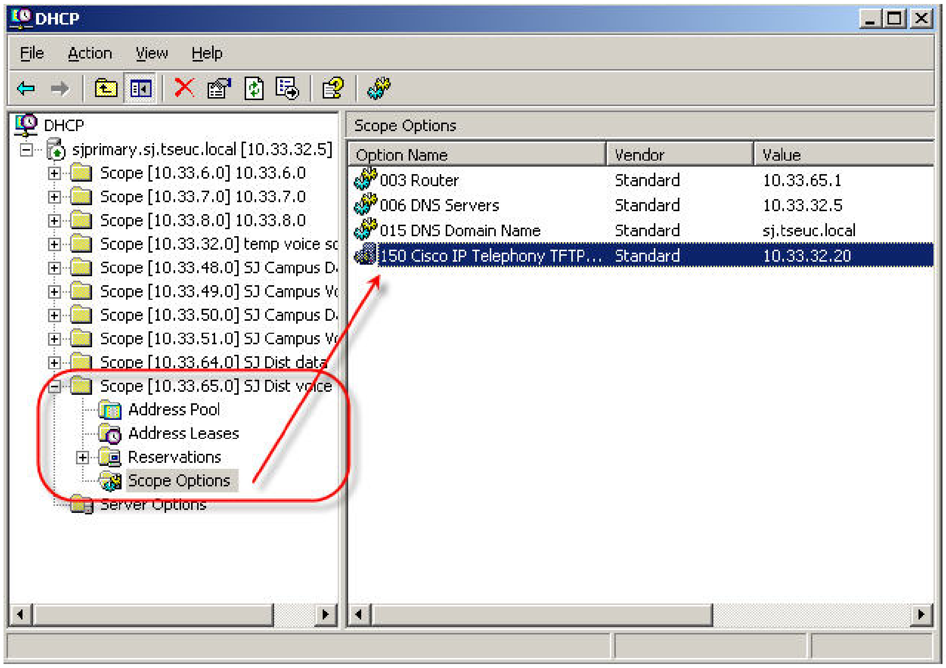


Available Options	Description
☐ 075 StreetTalk Servers	List of Stree
☐ 076 StreetTalk Directory Assistance (STDA) Servers	List of STDA
☑ 150 Cisco IP Telephony TFTP Server Address	CUCM IP ad
☐ 249 Classless Static Routes	Destination,

Data entry
IP address: 10 . 33 . 32 . 20

Step 7 Select a DHCP scope and verify that option 150 now shows up in the *Scope Options* window. See Figure 10-10.

Figure 10-10 DHCP Scope Options Window


DHCP
File Action View Help
DHCP
sjprimary.sj.tseuc.local [10.33.32.5]
Scope [10.33.6.0] 10.33.6.0
Scope [10.33.7.0] 10.33.7.0
Scope [10.33.8.0] 10.33.8.0
Scope [10.33.32.0] temp voice sc
Scope [10.33.48.0] SJ Campus D
Scope [10.33.49.0] SJ Campus Vo
Scope [10.33.50.0] SJ Campus D
Scope [10.33.51.0] SJ Campus Vo
Scope [10.33.64.0] SJ Dist data
Scope [10.33.65.0] SJ Dist voice
Address Pool
Address Leases
Reservations
Scope Options
Server Options
Scope Options
222969

Option Name	Vendor	Value
003 Router	Standard	10.33.65.1
006 DNS Servers	Standard	10.33.32.5
015 DNS Domain Name	Standard	sj.tseuc.local
150 Cisco IP Telephony TFTP...	Standard	10.33.32.20

Configuring the DNS with Cisco Unified Communications Manager Entries

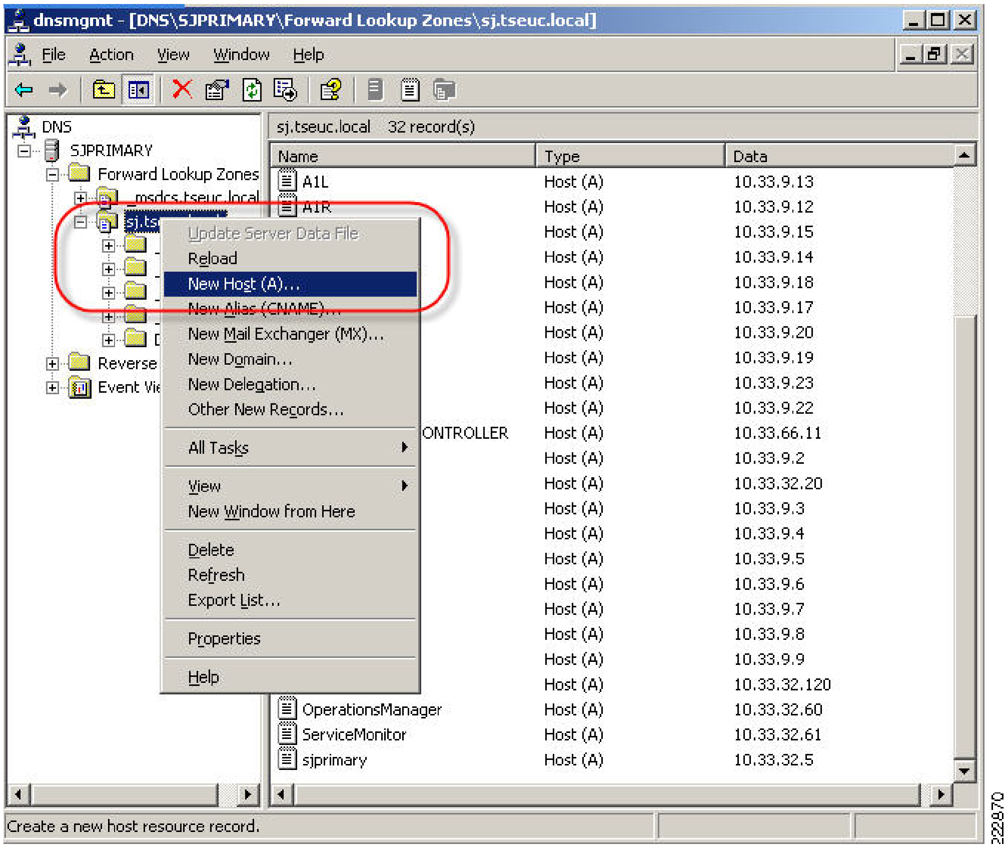
An Cisco IP phone (including the Cisco Unified Wireless IP Phone 7921) uses DHCP option 150 to learn the IP address of an associated TFTP server. An Cisco IP phone downloads its configuration file from the TFTP server. That configuration file contains the name of the Cisco Unified Communications Manager publisher and subscribers. The Cisco IP phone uses DNS to resolve a Cisco Unified Communications Manager name into an IP address that can be used with IP telephony registration messages.

If Cisco IP phones have already been deployed, the DNS configuration will already be complete, and this step can be skipped.

The following steps must be completed once for the Cisco Unified Communications Manager publisher, and once for each of the Cisco Unified Communications Manager subscribers.

Step 1 From the DNS server console, right-click the relevant forward lookup zone, and select **New Host (A)...** See Figure 10-11.

Figure 10-11 New Host (A)



sj.tseuc.local 32 record(s)

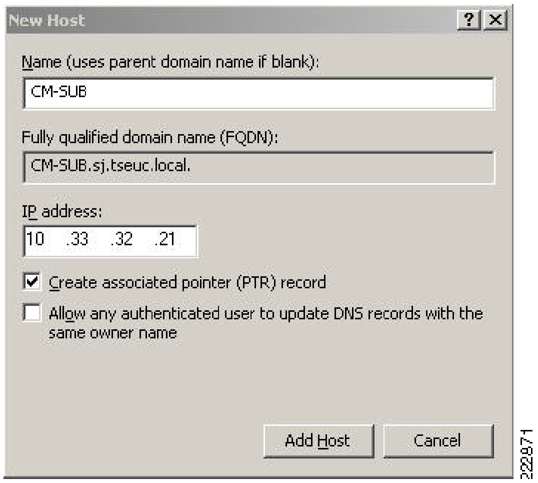
Name	Type	Data
A1L	Host (A)	10.33.9.13
A1R	Host (A)	10.33.9.12
	Host (A)	10.33.9.15
	Host (A)	10.33.9.14
	Host (A)	10.33.9.18
	Host (A)	10.33.9.17
	Host (A)	10.33.9.20
	Host (A)	10.33.9.19
	Host (A)	10.33.9.23
	Host (A)	10.33.9.22
ONTROLLER	Host (A)	10.33.66.11
	Host (A)	10.33.9.2
	Host (A)	10.33.32.20
	Host (A)	10.33.9.3
	Host (A)	10.33.9.4
	Host (A)	10.33.9.5
	Host (A)	10.33.9.6
	Host (A)	10.33.9.7
	Host (A)	10.33.9.8
	Host (A)	10.33.9.9
	Host (A)	10.33.32.120
OperationsManager	Host (A)	10.33.32.60
ServiceMonitor	Host (A)	10.33.32.61
sjprimary	Host (A)	10.33.32.5

Create a new host resource record.

Step 2 Fill out the *Name* and *IP address* of the Cisco Unified Communications Manager publisher server or subscriber server and click **Add Host**. See Figure 10-12.

The "Cisco Unified Communications Manager Base Configuration" section on page 10-10 describes how to determine the Cisco Unified Communications Manager name from Cisco Unified Communications Manager administration.

Figure 10-12 Entering New Host Name



Name (uses parent domain name if blank):
CM-SUB

Fully qualified domain name (FQDN):
CM-SUB.sj.tseuc.local.

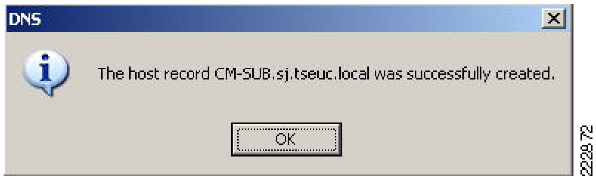
IP address:
10 .33 .32 .21

☑ Create associated pointer (PTR) record

□ Allow any authenticated user to update DNS records with the same owner name

Step 3 Click **OK** to acknowledge the success message. See Figure 10-13.

Figure 10-13 Acknowledging Successful Host Record Creation

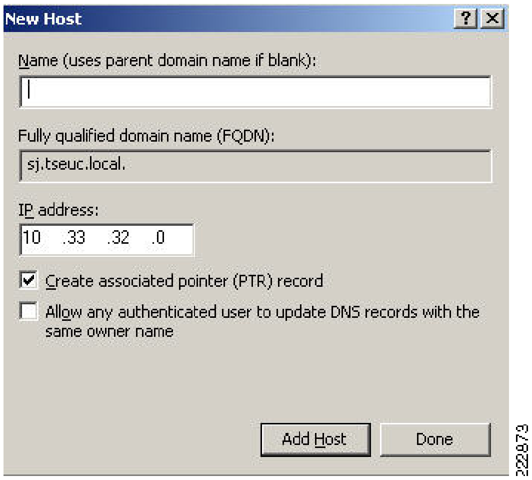


DNS

The host record CM-SUB.sj.tseuc.local was successfully created.

Step 4 Either, fill out the *Name* and *IP address* of the next Cisco Unified Communications Manager publisher server or subscriber server and click **Add Host**, or click **Done** to exit DNS configuration. See Figure 10-14.

Figure 10-14 Entering Cisco Unified Communications Manager Publisher Information



New Host

Name (uses parent domain name if blank):

Fully qualified domain name (FQDN): sj.tseuc.local.

IP address: 10 .33 .32 .0

☑ Create associated pointer (PTR) record

□ Allow any authenticated user to update DNS records with the same owner name

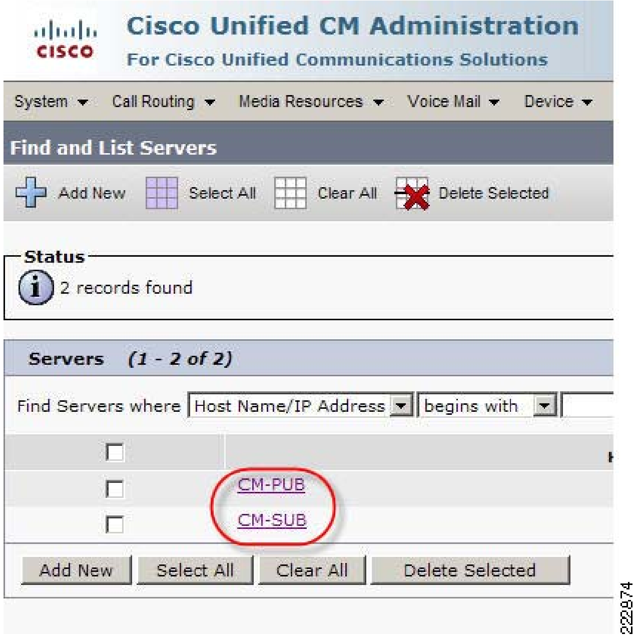
Cisco Unified Communications Manager Base Configuration

This section assumes a Cisco Unified Communications Manager installation pre-exists and provides procedures for verifying the necessary settings to enable a Cisco Unified Wireless IP Phone 7921 to successfully operate.

Verifying Cisco Unified Communications Manager Name

You must know the Cisco Unified Communications Manager server name in order to ensure that it is correctly configured in the DNS server as described in the "Configuring the DNS with Cisco Unified Communications Manager Entries" section on page 10-8. From Cisco Unified Communications Manager administration window, navigate to *System* > *Server* > *Find*. By leaving all the *Find* fields blank, the system will display all Cisco Unified Communications Manager names known to the system. See Figure 10-15.

Figure 10-15 Verifying Cisco Unified Communications Manager Server Names



Status

2 records found

Servers (1 - 2 of 2)

□ CM-PUB

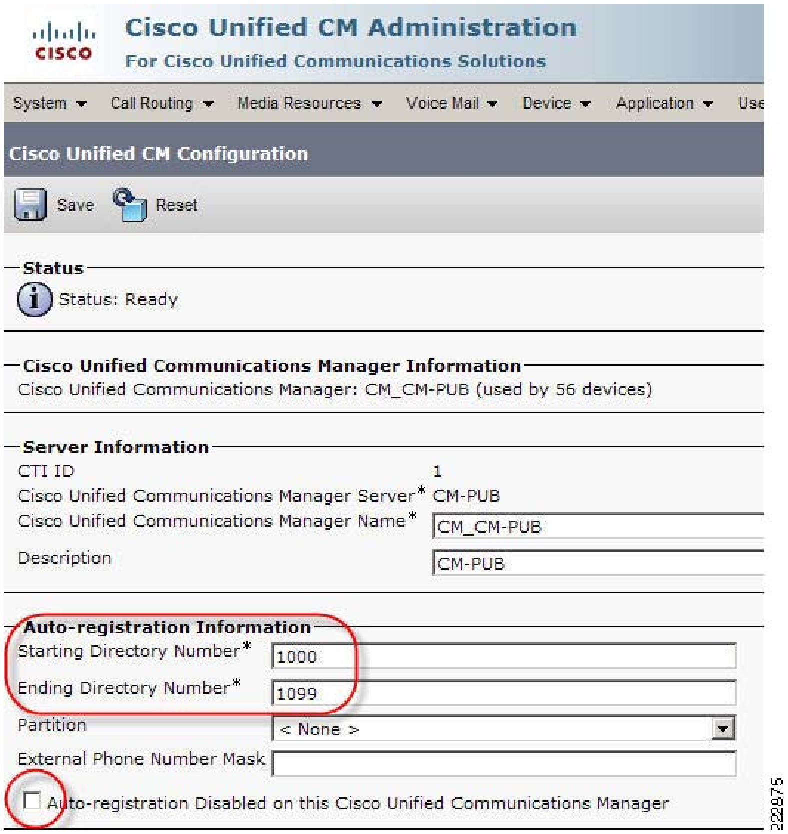
□ CM-SUB

Verifying Auto-Registration Enabled

The simplest way to enable Cisco Unified Wireless IP Phone 7921 registration to a Cisco Unified Communications Manager is to enable auto-registration. To verify or enable auto-registration, navigate to *System* > *Cisco Unified CM* > *Find*. When the *Find* action completes, click the relevant Cisco Unified Communications Manager name and verify that auto-registration is enabled on that Cisco Unified Communications Manager. See Figure 10-16.

In production environments, auto-registration is often disabled and phones are added by explicitly defining each phone in Cisco Unified Communications Manager. Follow the procedures established at your site for adding phones.

Figure 10-16 Cisco Unified Communications Manager Auto Registration:


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
System
Call Routing
Media Resources
Voice Mail
Device
Application
Use
Cisco Unified CM Configuration
Save
Reset
222975

Status

Status: Ready

Cisco Unified Communications Manager Information

Cisco Unified Communications Manager: CM_CM-PUB (used by 56 devices)

Server Information

CTI ID 1

Cisco Unified Communications Manager Server* CM-PUB

Cisco Unified Communications Manager Name* CM_CM-PUB

Description CM-PUB

Auto-registration Information

Starting Directory Number* 1000

Ending Directory Number* 1099

Partition < None >

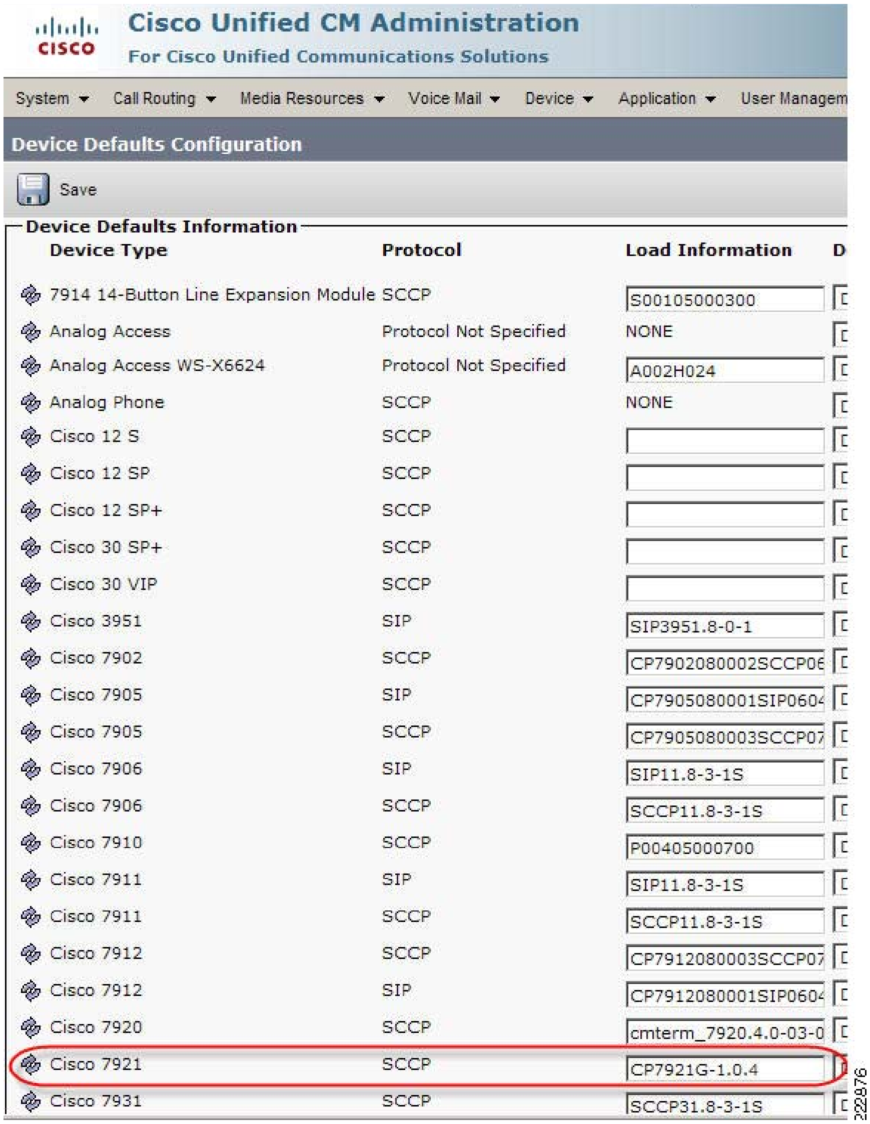
External Phone Number Mask

□ Auto-registration Disabled on this Cisco Unified Communications Manager

Verifying Cisco Unified Wireless IP Phone 7921 Firmware

The Cisco Unified Wireless IP Phone 7921 updates its firmware from the Cisco Unified Communications Manager TFTP server. Customers are strongly encouraged to run the most recent release of Cisco Unified Wireless IP Phone 7921 firmware. The current release on Cisco.com can be determined by going to http://www.cisco.com, logging in, and navigating to *Support* > *Download Software* > *Voice Software* > *Cisco Unified Wireless IP Phone Firmware*. Make a note of the most recent version of firmware available on Cisco.com, and ensure the same version is loaded in the Cisco Unified Communications Manager by navigating on Cisco Unified Communications Manager to *Device* > *Device Settings* > *Device Defaults*. See Figure 10-17.

Figure 10-17 Cisco Unified Communications Manager Device Defaults


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
System
Call Routing
Media Resources
Voice Mail
Device
Application
User Managem
Device Defaults Configuration
Save
222876

Device Defaults Information

Device Type	Protocol	Load Information	D
7914 14-Button Line Expansion Module	SCCP	S00105000300	
Analog Access	Protocol Not Specified	NONE	
Analog Access WS-X6624	Protocol Not Specified	A002H024	
Analog Phone	SCCP	NONE	
Cisco 12 S	SCCP		
Cisco 12 SP	SCCP		
Cisco 12 SP+	SCCP		
Cisco 30 SP+	SCCP		
Cisco 30 VIP	SCCP		
Cisco 3951	SIP	SIP3951.8-0-1	
Cisco 7902	SCCP	CP7902080002SCCP06	
Cisco 7905	SIP	CP7905080001SIP0604	
Cisco 7905	SCCP	CP7905080003SCCP07	
Cisco 7906	SIP	SIP11.8-3-1S	
Cisco 7906	SCCP	SCCP11.8-3-1S	
Cisco 7910	SCCP	P00405000700	
Cisco 7911	SIP	SIP11.8-3-1S	
Cisco 7911	SCCP	SCCP11.8-3-1S	
Cisco 7912	SCCP	CP7912080003SCCP07	
Cisco 7912	SIP	CP7912080001SIP0604	
Cisco 7920	SCCP	cmterm_7920.4.0-03-0	
Cisco 7921	SCCP	CP7921G-1.0.4	
Cisco 7931	SCCP	SCCP31.8-3-1S	

Cisco Unified Wireless IP Phone 7921 Base Configuration

Baseline configuration for the IP phone consist of two procedures:

- Resetting the IP Phone, page 10-13
- Configuring a WLAN Profile, page 10-14

Resetting the IP Phone

If necessary, reset the Cisco Unified Wireless IP Phone 7921 to factory defaults. The factory default option erases all user-defined entries in Network Profiles, Phone Settings, and Call History. To erase the local configuration, follow these steps:

Step 1 Press the **Navigation Button** downwards to enter *SETTINGS* mode

Step 2 Navigate to and select *Phone Settings*.

Step 3 Press ****2** on the keypad. The phone briefly displays this prompt: *Restore to Default?*

Step 4 Press the **Yes** softkey to confirm or **No** to cancel. The phone resets after selecting *Yes*

Configuring a WLAN Profile

The following procedure summarizes the process of configuring the WLAN profile:

Step 1 Press the **Navigation Button** downwards to enter *SETTINGS* mode

Step 2 Navigate to and select *Network Profiles* (pressing the number adjacent to a menu item is equivalent to selecting that item).

Step 3 Unlock the IP phone's configuration menu by pressing ****#.** The padlock icon on the top-right of the screen will change from closed to open.

Step 4 Navigate to the profile you want to change and press the **Change** softkey.

Step 5 Navigate to and select *Profile Name*.

Step 6 Use the IP phone's keypad to enter a profile name. Normally this name will match the corresponding WLAN profile name defined on the Cisco Wireless LAN Controller (Cisco WLC).

Step 7 Navigate to and select *WLAN Configuration*.

Step 8 Navigate to and select *SSID*.

Step 9 Use the IP phone's keypad to enter a SSID name (normally this name will match the corresponding WLAN SSID name defined on the Cisco WLC).

Step 10 Press the **Back** softkey until the **Exit** softkey appears.

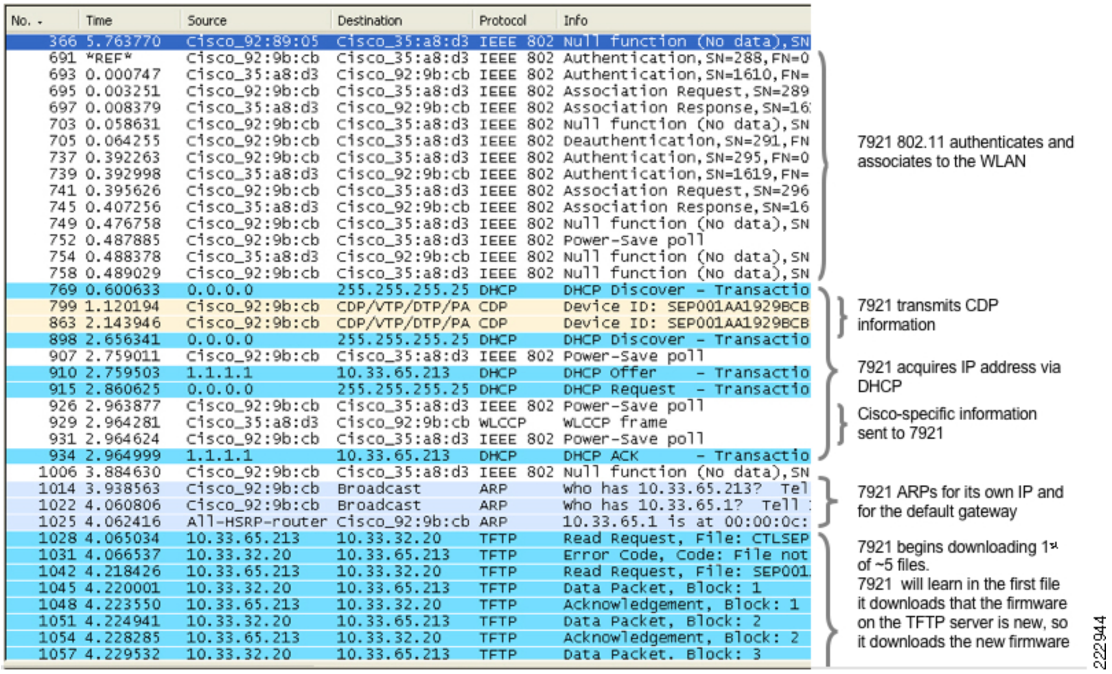
Step 11 Press the **Exit** softkey.

Trace Analysis for a Base Configuration

This section presents annotated sections of a trace of a Cisco Unified Wireless IP Phone 7921 being connected to a network for the first time. Five distinct sections of this trace are examined—highlighting the different stages of the connection. See Figure 10-18. The first section shows the initial connection and the start of the TFTP download.

Because this is the first time the Cisco Unified Wireless IP Phone 7921 has connected, its firmware is out of date. One of the first files the phone downloads contains the name of the firmware image that the Cisco Unified Wireless IP Phone 7921 should be running. The Cisco Unified Wireless IP Phone 7921 will see this and will download the specified firmware image. Because of the need to download a new firmware image, the TFTP process takes longer than it would if the Cisco Unified Wireless IP Phone 7921 was already running the correct firmware.

Figure 10-18 Initial Cisco Unified Wireless IP Phone 7921 Connect Trace (Part 1)



```
No. -   Time      Source           Destination      Protocol   Info
 366 5.763770     Cisco_92:89:05   Cisco_35:a8:d3   IEEE 802   Null function (No data),SN
 691 *REF*        Cisco_92:9b:cb   Cisco_35:a8:d3   IEEE 802   Authentication,SN=288,FN=0
 693 0.000747     Cisco_35:a8:d3   Cisco_92:9b:cb   IEEE 802   Authentication,SN=1610,FN=
 695 0.003251     Cisco_92:9b:cb   Cisco_35:a8:d3   IEEE 802   Association Request,SN=289
 697 0.008379     Cisco_35:a8:d3   Cisco_92:9b:cb   IEEE 802   Association Response,SN=16
 703 0.058631     Cisco_92:9b:cb   Cisco_35:a8:d3   IEEE 802   Null function (No data),SN
 705 0.064255     Cisco_92:9b:cb   Cisco_35:a8:d3   IEEE 802   Deauthentication,SN=291,FN
 737 0.392263     Cisco_92:9b:cb   Cisco_35:a8:d3   IEEE 802   Authentication,SN=295,FN=0
 739 0.392998     Cisco_35:a8:d3   Cisco_92:9b:cb   IEEE 802   Authentication,SN=1619,FN=
 741 0.395626     Cisco_92:9b:cb   Cisco_35:a8:d3   IEEE 802   Association Request,SN=296
 745 0.407256     Cisco_35:a8:d3   Cisco_92:9b:cb   IEEE 802   Association Response,SN=16
 749 0.476758     Cisco_92:9b:cb   Cisco_35:a8:d3   IEEE 802   Null function (No data),SN
 752 0.487885     Cisco_92:9b:cb   Cisco_35:a8:d3   IEEE 802   Power-Save poll
 754 0.488378     Cisco_35:a8:d3   Cisco_92:9b:cb   IEEE 802   Null function (No data),SN
 758 0.489029     Cisco_92:9b:cb   Cisco_35:a8:d3   IEEE 802   Null function (No data),SN
 769 0.600633     0.0.0.0          255.255.255.25   DHCP       DHCP Discover - Transactio
 799 1.120194     Cisco_92:9b:cb   CDP/VTP/DTP/PA   CDP        Device ID: SEP001AA1929BCB
 863 2.143946     Cisco_92:9b:cb   CDP/VTP/DTP/PA   CDP        Device ID: SEP001AA1929BCB
 898 2.656341     0.0.0.0          255.255.255.25   DHCP       DHCP Discover - Transactio
 907 2.759011     Cisco_92:9b:cb   Cisco_35:a8:d3   IEEE 802   Power-Save poll
 910 2.759503     1.1.1.1          10.33.65.213     DHCP       DHCP Offer    - Transactio
 915 2.860625     0.0.0.0          255.255.255.25   DHCP       DHCP Request  - Transactio
 926 2.963877     Cisco_92:9b:cb   Cisco_35:a8:d3   IEEE 802   Power-Save poll
 929 2.964281     Cisco_35:a8:d3   Cisco_92:9b:cb   WLCCP      WLCCP frame
 931 2.964624     Cisco_92:9b:cb   Cisco_35:a8:d3   IEEE 802   Power-Save poll
 934 2.964999     1.1.1.1          10.33.65.213     DHCP       DHCP ACK      - Transactio
1006 3.884630     Cisco_92:9b:cb   Cisco_35:a8:d3   IEEE 802   Null function (No data),SN
1014 3.938563     Cisco_92:9b:cb   Broadcast        ARP        Who has 10.33.65.213?  Tel
1022 4.060806     Cisco_92:9b:cb   Broadcast        ARP        Who has 10.33.65.1?  Tell
1025 4.062416     All-HSRP-router  Cisco_92:9b:cb   ARP        10.33.65.1 is at 00:00:0c:
1028 4.065034     10.33.65.213     10.33.32.20      TFTP       Read Request, File: CTLSEP
1031 4.066537     10.33.32.20      10.33.65.213     TFTP       Error Code, Code: File not
1042 4.218426     10.33.65.213     10.33.32.20      TFTP       Read Request, File: SEP001
1045 4.220001     10.33.32.20      10.33.65.213     TFTP       Data Packet, Block: 1
1048 4.223550     10.33.65.213     10.33.32.20      TFTP       Acknowledgement, Block: 1
1051 4.224941     10.33.32.20      10.33.65.213     TFTP       Data Packet, Block: 2
1054 4.228285     10.33.65.213     10.33.32.20      TFTP       Acknowledgement, Block: 2
1057 4.229532     10.33.32.20      10.33.65.213     TFTP       Data Packet. Block: 3
```

7921 802.11 authenticates and associates to the WLAN

7921 transmits CDP information

7921 acquires IP address via DHCP

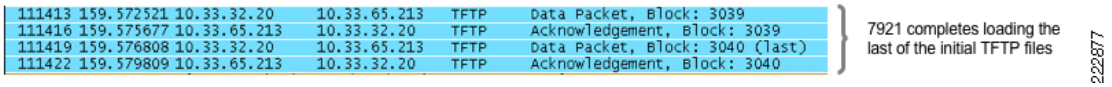
Cisco-specific information sent to 7921

7921 ARPs for its own IP and for the default gateway

7921 begins downloading 1st of ~5 files.
7921 will learn in the first file it downloads that the firmware on the TFTP server is new, so it downloads the new firmware

Figure 10-19 illustrates the end of the initial TFTP download sequence. At this point five TFTP files containing the Cisco Unified Wireless IP Phone 7921 configuration and firmware have been downloaded.

Figure 10-19 Initial Cisco Unified Wireless IP Phone 7921 Connect Trace (Part 2)

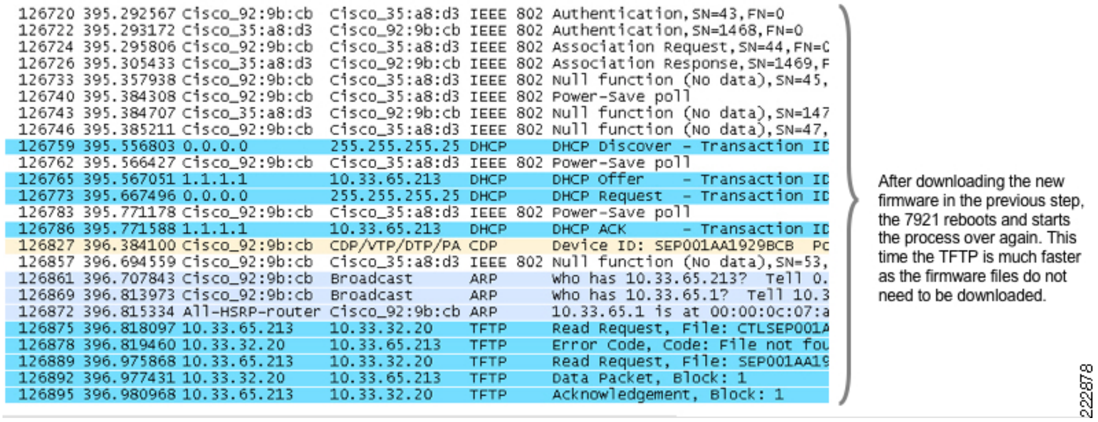


```
111413 159.572521 10.33.32.20     10.33.65.213   TFTP     Data Packet, Block: 3039
111416 159.575677 10.33.65.213    10.33.32.20    TFTP     Acknowledgement, Block: 3039
111419 159.576808 10.33.32.20     10.33.65.213   TFTP     Data Packet, Block: 3040 (last)
111422 159.579809 10.33.65.213    10.33.32.20    TFTP     Acknowledgement, Block: 3040
```

7921 completes loading the last of the initial TFTP files

Figure 10-20 illustrates that the Cisco Unified Wireless IP Phone 7921 has downloaded and installed the new firmware, and then rebooted. The TFTP download in this case is much shorter and quicker.

Figure 10-20 Initial Cisco Unified Wireless IP Phone 7921 Connect Trace (Part 3)

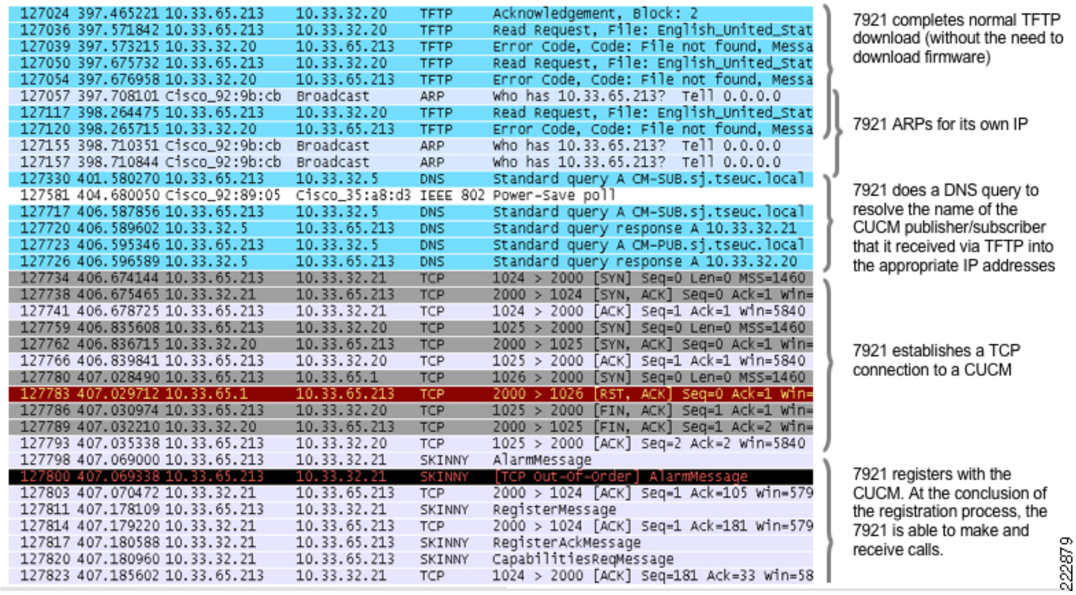


```
126720 395.292567 Cisco_92:9b:cb   Cisco_35:a8:d3  IEEE 802 Authentication,SN=43,FN=0
126722 395.293172 Cisco_35:a8:d3   Cisco_92:9b:cb  IEEE 802 Authentication,SN=1468,FN=0
126724 395.295806 Cisco_92:9b:cb   Cisco_35:a8:d3  IEEE 802 Association Request,SN=44,FN=C
126726 395.305433 Cisco_35:a8:d3   Cisco_92:9b:cb  IEEE 802 Association Response,SN=1469,F
126733 395.357938 Cisco_92:9b:cb   Cisco_35:a8:d3  IEEE 802 Null function (No data),SN=45,
126740 395.384308 Cisco_92:9b:cb   Cisco_35:a8:d3  IEEE 802 Power-Save poll
126743 395.384707 Cisco_35:a8:d3   Cisco_92:9b:cb  IEEE 802 Null function (No data),SN=147
126746 395.385211 Cisco_92:9b:cb   Cisco_35:a8:d3  IEEE 802 Null function (No data),SN=47,
126759 395.556803 0.0.0.0          255.255.255.25  DHCP     DHCP Discover - Transaction ID
126762 395.566427 Cisco_92:9b:cb   Cisco_35:a8:d3  IEEE 802 Power-Save poll
126765 395.567051 1.1.1.1          10.33.65.213    DHCP     DHCP Offer    - Transaction ID
126773 395.667496 0.0.0.0          255.255.255.25  DHCP     DHCP Request  - Transaction ID
126783 395.771178 Cisco_92:9b:cb   Cisco_35:a8:d3  IEEE 802 Power-Save poll
126786 395.771588 1.1.1.1          10.33.65.213    DHCP     DHCP ACK      - Transaction ID
126827 396.384100 Cisco_92:9b:cb   CDP/VTP/DTP/PA  CDP      Device ID: SEP001AA1929BCB  Pc
126857 396.694559 Cisco_92:9b:cb   Cisco_35:a8:d3  IEEE 802 Null function (No data),SN=53,
126861 396.707843 Cisco_92:9b:cb   Broadcast       ARP      Who has 10.33.65.213?  Tell 0.
126869 396.813973 Cisco_92:9b:cb   Broadcast       ARP      Who has 10.33.65.1?  Tell 10.3
126872 396.815334 All-HSRP-router  Cisco_92:9b:cb  ARP      10.33.65.1 is at 00:00:0c:07:a
126875 396.818097 10.33.65.213     10.33.32.20     TFTP     Read Request, File: CTLSEP001A
126878 396.819460 10.33.32.20      10.33.65.213    TFTP     Error Code, Code: File not fou
126889 396.975868 10.33.65.213     10.33.32.20     TFTP     Read Request, File: SEP001AA19
126892 396.977431 10.33.32.20      10.33.65.213    TFTP     Data Packet, Block: 1
126895 396.980968 10.33.65.213     10.33.32.20     TFTP     Acknowledgement, Block: 1
```

After downloading the new firmware in the previous step, the 7921 reboots and starts the process over again. This time the TFTP is much faster as the firmware files do not need to be downloaded.

Figure 10-21 illustrates the conclusion of the normal TFTP sequence, the ARPs verifying that the IP address is unique, and a DNS lookup to resolve the name to IP address of the Cisco Unified Communications Manager publisher and subscriber that learned via the TFTP configuration file. The Cisco Unified Wireless IP Phone 7921 then starts a TCP connection to the subscriber Cisco Unified Communications Manager and begins the phone registration process (shown here as the *skinny* protocol).

Figure 10-21 Initial Cisco Unified Wireless IP Phone 7921 Connect Trace (Part 4)



```
127024 397.465221 10.33.65.213     10.33.32.20      TFTP      Acknowledgement, Block: 2
127036 397.571842 10.33.65.213     10.33.32.20      TFTP      Read Request, File: English_United_Stat
127039 397.573215 10.33.32.20      10.33.65.213     TFTP      Error Code, Code: File not found, Messa
127050 397.675732 10.33.65.213     10.33.32.20      TFTP      Read Request, File: English_United_Stat
127054 397.676958 10.33.32.20      10.33.65.213     TFTP      Error Code, Code: File not found, Messa
127057 397.708101 Cisco_92:9b:cb   Broadcast        ARP       Who has 10.33.65.213?  Tell 0.0.0.0
127117 398.264475 10.33.65.213     10.33.32.20      TFTP      Read Request, File: English_United_Stat
127120 398.265715 10.33.32.20      10.33.65.213     TFTP      Error Code, Code: File not found, Messa
127155 398.710351 Cisco_92:9b:cb   Broadcast        ARP       Who has 10.33.65.213?  Tell 0.0.0.0
127157 398.710844 Cisco_92:9b:cb   Broadcast        ARP       Who has 10.33.65.213?  Tell 0.0.0.0
127330 401.580270 10.33.65.213     10.33.32.5       DNS       Standard query A CM-SUB.sj.tseuc.local
127581 404.680050 Cisco_92:89:05   Cisco_35:a8:d3   IEEE 802  Power-Save poll
127717 406.587856 10.33.65.213     10.33.32.5       DNS       Standard query A CM-SUB.sj.tseuc.local
127720 406.589602 10.33.32.5       10.33.65.213     DNS       Standard query response A 10.33.32.21
127723 406.595346 10.33.65.213     10.33.32.5       DNS       Standard query A CM-PUB.sj.tseuc.local
127726 406.596589 10.33.32.5       10.33.65.213     DNS       Standard query response A 10.33.32.20
127734 406.674144 10.33.65.213     10.33.32.21      TCP       1024 > 2000 [SYN] Seq=0 Len=0 MSS=1460
127738 406.675465 10.33.32.21      10.33.65.213     TCP       2000 > 1024 [SYN, ACK] Seq=0 Ack=1 Win=
127741 406.678725 10.33.65.213     10.33.32.21      TCP       1024 > 2000 [ACK] Seq=1 Ack=1 Win=5840
127759 406.835608 10.33.65.213     10.33.32.20      TCP       1025 > 2000 [SYN] Seq=0 Len=0 MSS=1460
127762 406.836715 10.33.32.20      10.33.65.213     TCP       2000 > 1025 [SYN, ACK] Seq=0 Ack=1 Win=
127766 406.839841 10.33.65.213     10.33.32.20      TCP       1025 > 2000 [ACK] Seq=1 Ack=1 Win=5840
127780 407.028490 10.33.65.213     10.33.65.1       TCP       1026 > 2000 [SYN] Seq=0 Len=0 MSS=1460
127783 407.029712 10.33.65.1       10.33.65.213     TCP       2000 > 1026 [RST, ACK] Seq=0 Ack=1 Win=
127786 407.030974 10.33.65.213     10.33.32.20      TCP       1025 > 2000 [FIN, ACK] Seq=1 Ack=1 Win=
127789 407.032210 10.33.32.20      10.33.65.213     TCP       2000 > 1025 [FIN, ACK] Seq=1 Ack=2 Win=
127793 407.035338 10.33.65.213     10.33.32.20      TCP       1025 > 2000 [ACK] Seq=2 Ack=2 Win=5840
127798 407.069000 10.33.65.213     10.33.32.21      SKINNY    AlarmMessage
127800 407.069338 10.33.65.213     10.33.32.21      SKINNY    [TCP Out-Of-Order] AlarmMessage
127803 407.070472 10.33.32.21      10.33.65.213     TCP       2000 > 1024 [ACK] Seq=1 Ack=105 Win=579
127811 407.178109 10.33.65.213     10.33.32.21      SKINNY    RegisterMessage
127814 407.179220 10.33.32.21      10.33.65.213     TCP       2000 > 1024 [ACK] Seq=1 Ack=181 Win=579
127817 407.180588 10.33.32.21      10.33.65.213     SKINNY    RegisterAckMessage
127820 407.180960 10.33.32.21      10.33.65.213     SKINNY    CapabilitiesReqMessage
127823 407.185602 10.33.65.213     10.33.32.21      TCP       1024 > 2000 [ACK] Seq=181 Ack=33 Win=58
```

7921 completes normal TFTP download (without the need to download firmware)
7921 ARPs for its own IP
7921 does a DNS query to resolve the name of the CUCM publisher/subscriber that it received via TFTP into the appropriate IP addresses
7921 establishes a TCP connection to a CUCM
7921 registers with the CUCM. At the conclusion of the registration process, the 7921 is able to make and receive calls.
222879

Cisco Unified Wireless IP Phone 7921 Security

The Cisco Unified Wireless IP Phone 7921 supports the following WLAN security options:

- Security protocols
  - Wi-Fi Protected Access (WPA) Versions 1 and 2; Personal and Enterprise
- Authentication
  - Lightweight Extensible Authentication Protocol (LEAP) Authentication
  - Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
  - WEP/WPA/WPA2 Shared Key
- Encryption
  - Wired Equivalent Privacy (WEP)
  - Temporal Key Integrity Protocol (TKIP)
  - Advanced Encryption Standard (AES)
- Fast roaming protocol
  - Cisco Centralized Key Management (CCKM)

The remainder of the Cisco Unified Wireless IP Phone 7921 security section provided in this chapter focuses on the items listed that comprise the current best practice recommendations for secure Cisco Unified Wireless IP Phone 7921 deployments. More information on other Cisco Unified Wireless IP Phone 7921 security options is available in the product documentation available at http://www.cisco.com.

Controller WLAN Security Configuration

The optimal configuration for the controller configuration for the WLAN supporting Cisco Unified Wireless IP Phone 7921s is for the WPA security protocol with TKIP encryption and IEEE 802.1X with CCKM key management.

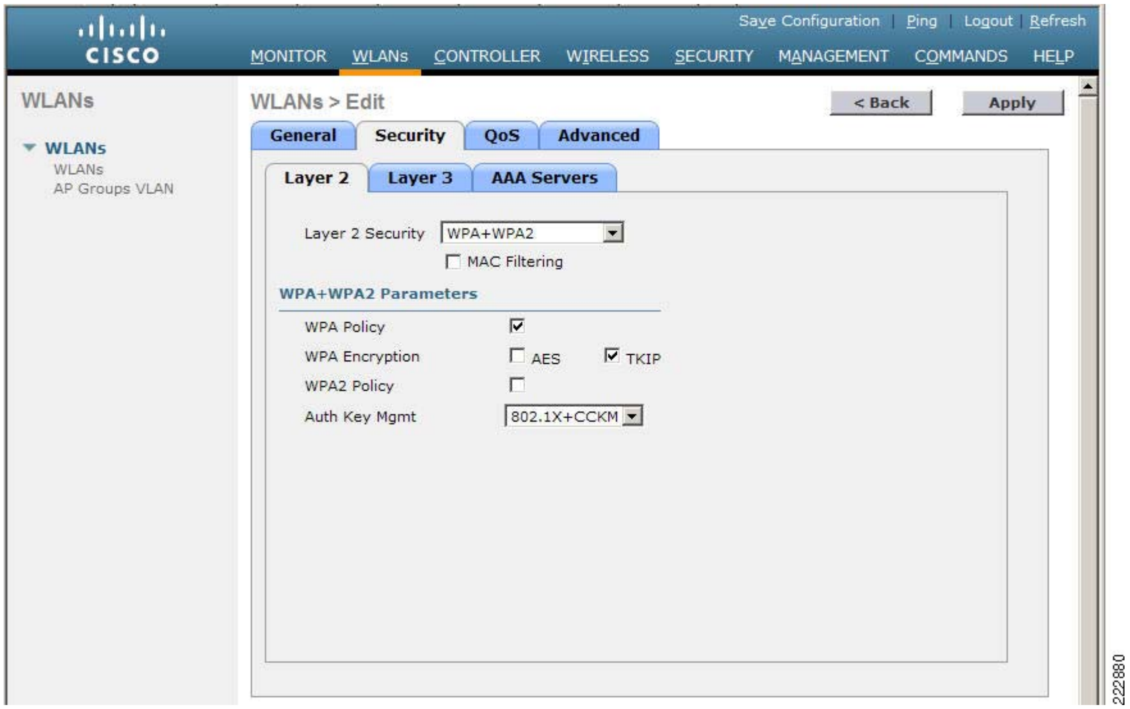
The combination of WPA, TKIP, IEEE 802.1X/CCKM provides the strongest supported authentication, encryption, and key management with CCKM for fast secure roaming between APs. Chapter 5, "Voice over WLAN Roaming," provides additional details addressing CCKM and describes why it is necessary to achieve voice handset roam times between APs in less than the ITU G.114 recommended maximum delay of 150 msec.

Note Cisco Unified Wireless IP Phone 7921s do not support WPA2 with TKIP encryption.

Note Cisco Unified Wireless IP Phone 7921s support WPA2 with AES encryption, but CCKM is not supported in this combination. Even though CCKM can be configured, and the Cisco Unified Wireless IP Phone 7921s appear to connect successfully, CCKM will not be used when roaming between APs in this combination.

The recommended configuration is shown Figure 10-22.

Figure 10-22 Cisco WLC Security Layer 2 Recommended Configuration



Layer 2 Security WPA+WPA2

☐ MAC Filtering

WPA+WPA2 Parameters

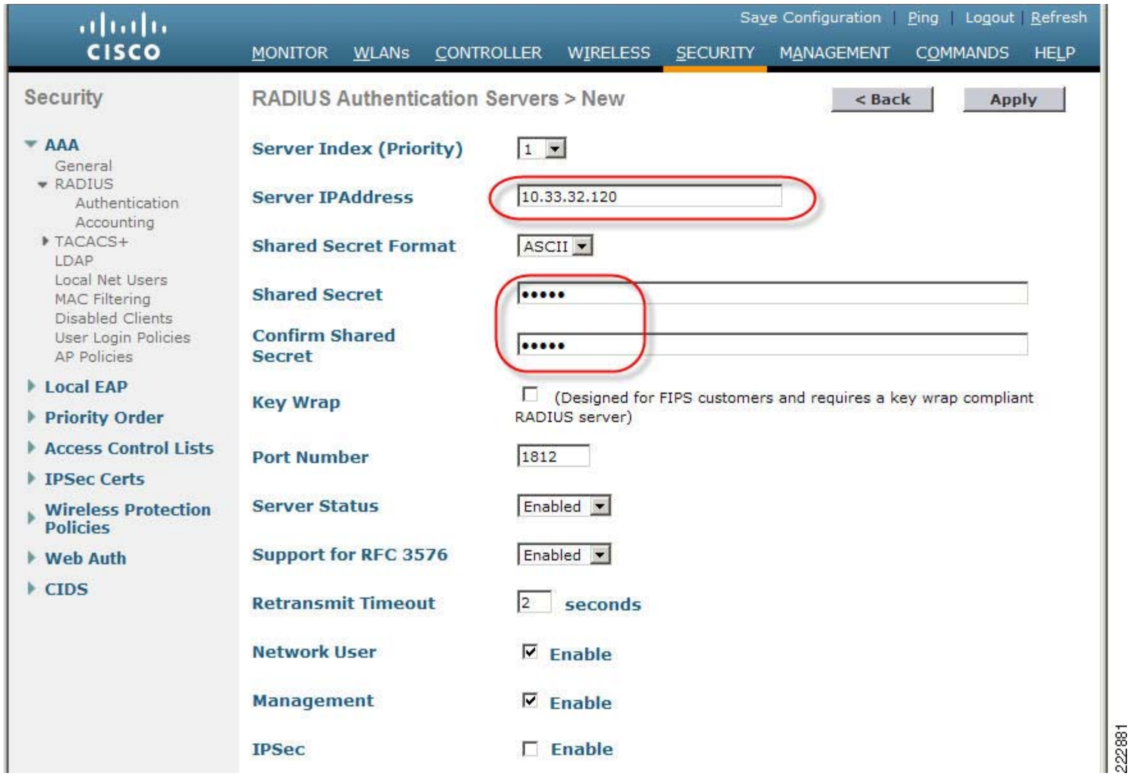
WPA Policy	☑	
WPA Encryption	☐ AES	☑ TKIP
WPA2 Policy	☐	
Auth Key Mgmt	802.1X+CCKM	

The recommended configuration uses IEEE 802.1X key management; that necessitates a RADIUS server for authentication. RADIUS server information is added to the controller by navigating *Security > RADIUS > Authentication*.

Cisco WLAN Controllers also support a mode known as *Local EAP*. When you enable Local EAP, the controller serves as the authentication server and the local user database, thereby removing dependence on an external authentication server. Local EAP is designed for use in remote offices that must maintain connectivity to wireless clients when the remote external authentication server is lost.

Figure 10-23 shows a RADIUS server definition being added to a controller. In Figure 10-23, the *Server IP Address* field is the IP address of the external RADIUS server. The shared secret is defined on both the controller and the RADIUS server; it is used to secure communications between the two. Chapter 4, "Voice over WLAN Security," provides details about configuring the Cisco ACS server to act as the external RADIUS server for wireless LAN EAP authentication.

Figure 10-23 Adding a RADIUS server to the Controller

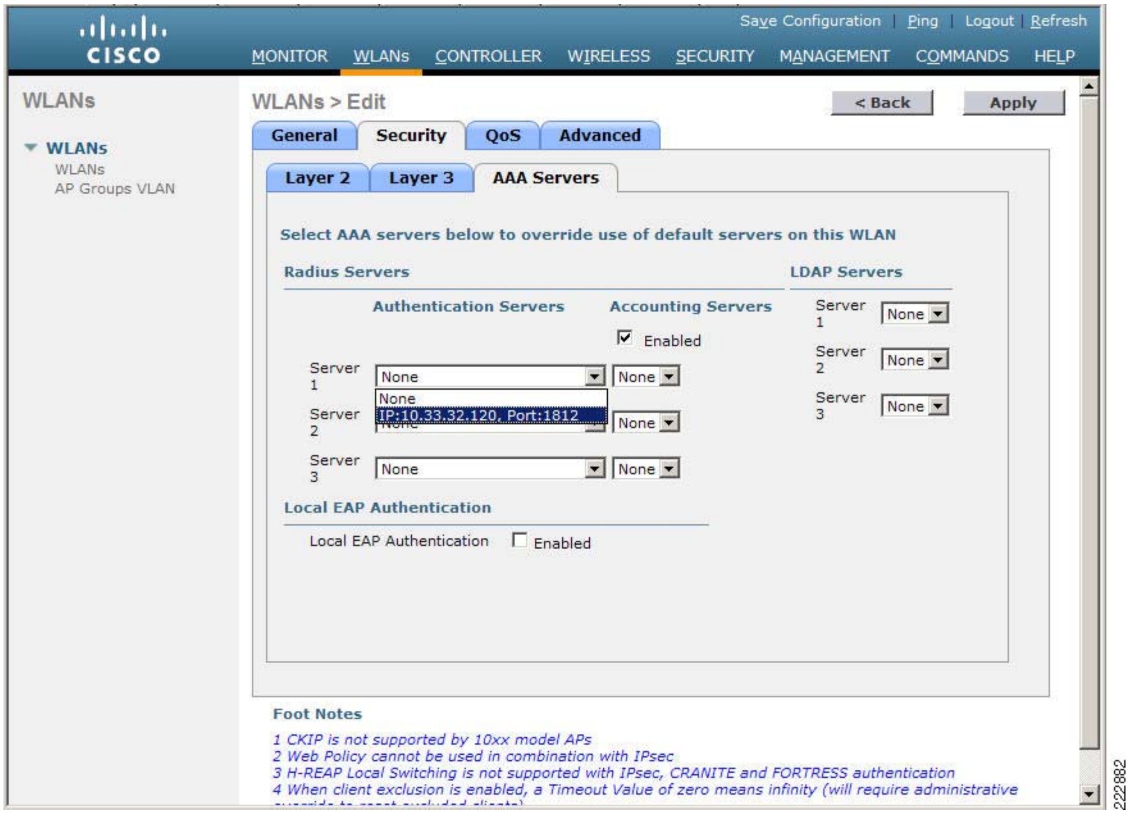


RADIUS Authentication Servers > New

Server Index (Priority)	1
Server IPAddress	10.33.32.120
Shared Secret Format	ASCII
Shared Secret	•••••
Confirm Shared Secret	•••••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Retransmit Timeout	2 seconds
Network User	☑ Enable
Management	☑ Enable
IPSec	□ Enable

Once the external RADIUS server definition has been added to the controller, the RADIUS server can be selected from the drop-down box for use by individual WLANs. Figure 10-24 shows a RADIUS server being selected from the *WLANs* > *Security* > *AAA Servers* tab.

Figure 10-24 Selecting Cisco WLC Security AAA Servers


cisco
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
< Back
Apply
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers
222882

WLANs > Edit

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

Radius Servers

Authentication Servers / Accounting Servers

☑ Enabled

Server 1: None (None / IP:10.33.32.120, Port:1812) — None

Server 2: None — None

Server 3: None — None

LDAP Servers

Server 1: None

Server 2: None

Server 3: None

Local EAP Authentication

Local EAP Authentication □ Enabled

Foot Notes

1 CKIP is not supported by 10xx model APs
2 Web Policy cannot be used in combination with IPsec
3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication
4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)

Setting the WLAN Controller IEEE 802.1X Timeout for EAP-FAST

When using EAP-FAST, the IEEE 802.1X timeout on the controller must be increased (default = 2 seconds) in order for the client to obtain the PAC via automatic provisioning. The default timeout on the Cisco ACS server is 20 seconds, which is the recommended value. To change the IEEE 802.1X timeout on the Cisco Wireless LAN controller, connect using Telnet or SSH to the controller and enter the following command:

```
(Cisco Controller)> config advanced eap request-timeout 20

(Cisco Controller)> show advanced eap
 EAP-Identity-Request Timeout (seconds)........... 1
 EAP-Identity-Request Max Retries................ 20
 EAP Key-Index for Dynamic WEP.................... 0
 EAP-Request Timeout (seconds)................... 20
 EAP-Request Max Retries.......................... 2
```

Cisco Unified Communications Manager Security Configuration

The Cisco Unified Wireless IP Phone 7921G supports the following voice security features:

- Certificates
- Image authentication
- Device authentication

- File authentication
- Signaling authentication
- Secure Cisco Unified SRST
- Media encryption (SRTP)

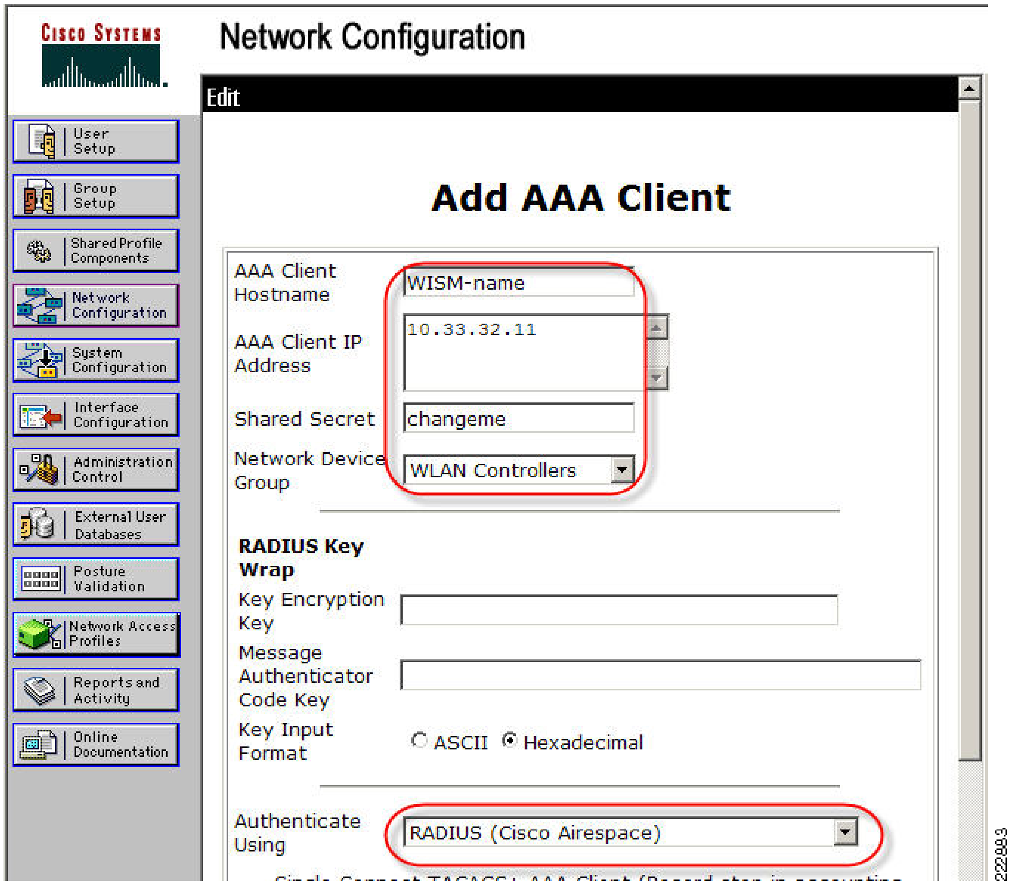
The Cisco Unified Communications Manager provides these available voice security features. For more information, refer to the Cisco Unified Communications Manager documentation at http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Network infrastructure Security Configuration

EAP-FAST authenticates to a RADIUS server. In this section, we configure the Cisco ACS server to support EAP-FAST authentication.

Every network device performing EAP authentication must be defined to the ACS as an *AAA Client*. On the ACS, we define the controller as an AAA Client by navigating *Network Configuration* > (select a group if device groups are being used) > *Add Entry*. Figure 10-25 shows an example of a controller being defined on the ACS.

Figure 10-25 Cisco ACS Configuration—Adding NAS



Network Configuration

Edit

Add AAA Client

AAA Client Hostname: WISM-name

AAA Client IP Address: 10.33.32.11

Shared Secret: changeme

Network Device Group: WLAN Controllers

RADIUS Key Wrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format: ○ ASCII ● Hexadecimal

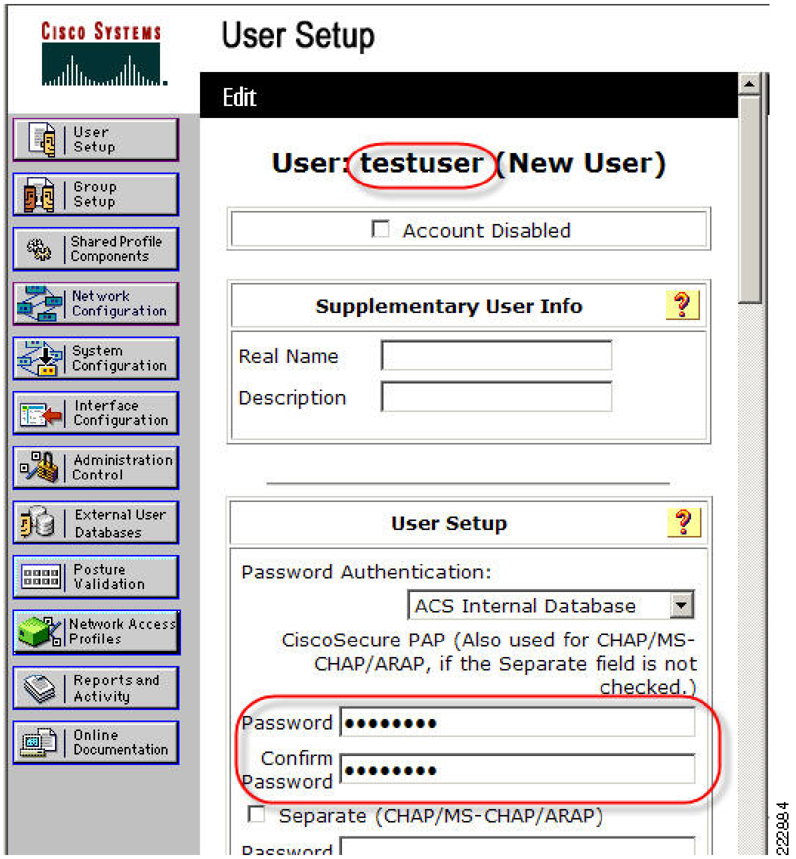
Authenticate Using: RADIUS (Cisco Airspace)

Every Cisco Unified Wireless IP Phone 7921 using EAP-FAST is configured with a *userid* and a *password*.

It is possible to configure multiple Cisco Unified Wireless IP Phone 7921s with the same userid and password. This is useful for small test deployments, but should be avoided in productions deployments where the loss of a single phone could require all deployed phones to be reconfigured.

Figure 10-26 shows a Cisco Unified Wireless IP Phone 7921s userid and password being configured on the ACS. This is done by navigating *User Setup* > (enter the name of the new user being added) > *Add/Edit*.

Figure 10-26 ACS Configuration—Adding a User



User: testuser (New User)

□ Account Disabled

Supplementary User Info

Real Name

Description

User Setup

Password Authentication:

ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password ••••••••

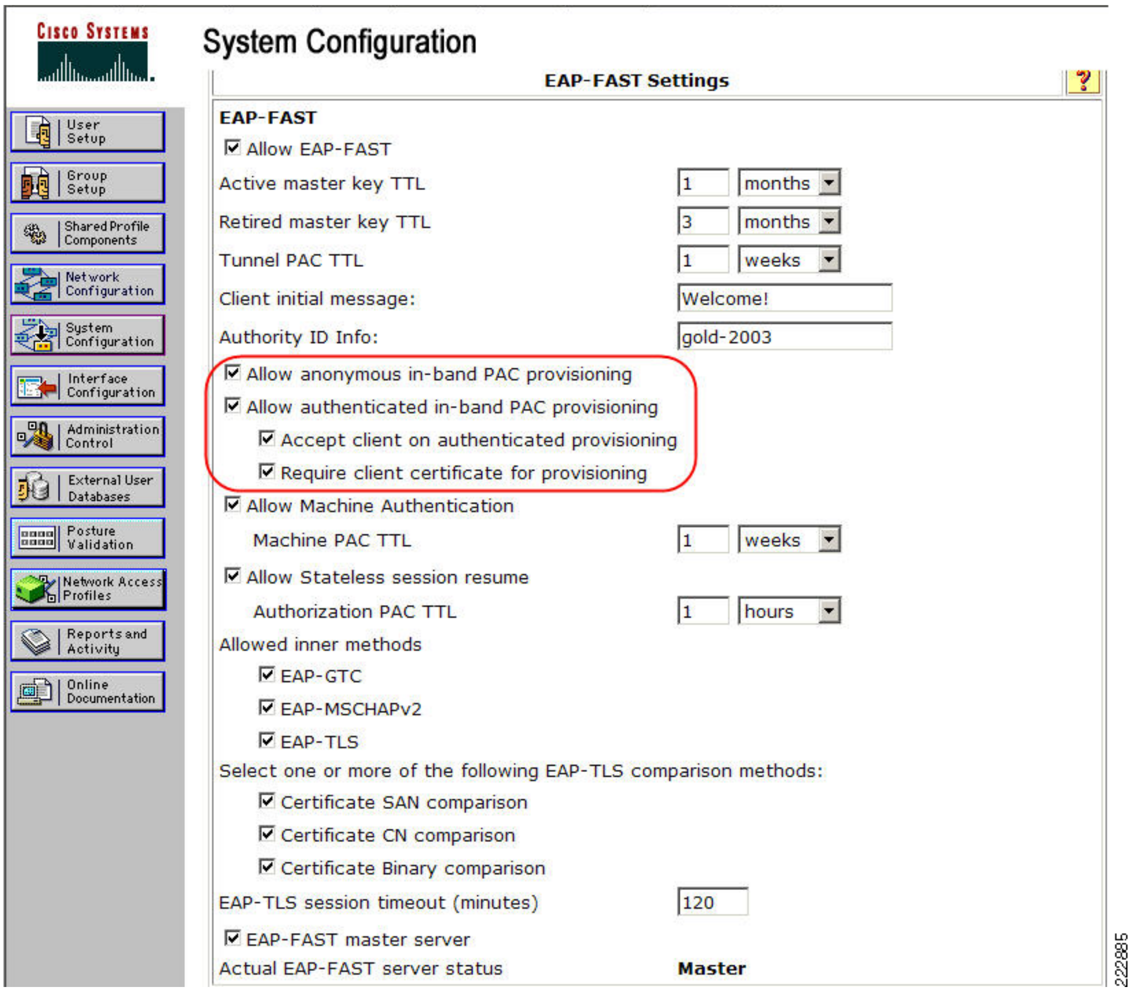
Confirm Password ••••••••

□ Separate (CHAP/MS-CHAP/ARAP)

Password

The ACS must also be configured to explicitly support EAP-FAST authentication. The Cisco Unified Wireless IP Phone 7921G currently supports only automatic provisioning of the Protected Access Credential (PAC), so *Anonymous In-Band PAC Provisioning* must be enabled. EAP-FAST is configured by navigating *System Configuration* > *Global Authentication Setup* > *EAP-FAST Configuration*. See Figure 10-27.

Figure 10-27 ACS Configuration—EAP-FAST Settings



System Configuration

EAP-FAST Settings

EAP-FAST

☑ Allow EAP-FAST

Active master key TTL: 1 months

Retired master key TTL: 3 months

Tunnel PAC TTL: 1 weeks

Client initial message: Welcome!

Authority ID Info: gold-2003

☑ Allow anonymous in-band PAC provisioning

☑ Allow authenticated in-band PAC provisioning

- ☑ Accept client on authenticated provisioning
- ☑ Require client certificate for provisioning

☑ Allow Machine Authentication

- Machine PAC TTL: 1 weeks

☑ Allow Stateless session resume

- Authorization PAC TTL: 1 hours

Allowed inner methods

- ☑ EAP-GTC
- ☑ EAP-MSCHAPv2
- ☑ EAP-TLS

Select one or more of the following EAP-TLS comparison methods:

- ☑ Certificate SAN comparison
- ☑ Certificate CN comparison
- ☑ Certificate Binary comparison

EAP-TLS session timeout (minutes): 120

☑ EAP-FAST master server

Actual EAP-FAST server status: **Master**

Cisco Unified Wireless IP Phone 7921 Security Configuration

The "Cisco Unified Wireless IP Phone 7921 Base Configuration" section on page 10-13 covered resetting a Cisco Unified Wireless IP Phone 7921 to factory defaults (if necessary) and adding a new WLAN Profile. Follow the instructions in that section to create a new WLAN profile for a EAP-FAST WLAN. This section focuses on configuring EAP-FAST.

Configure a WLAN Profile to use EAP-FAST Authentication

Cisco Unified Wireless IP Phone 7921s can be configured to use EAP-FAST with a specific userid and password as described in the following procedure.

Step 1 Press the **Navigation Button** downwards to enter *SETTINGS* mode

Step 2 Navigate to and select **Network Profiles** (pressing the number adjacent to a menu item is equivalent to selecting that item).

Step 3 Unlock the phones configuration menu by pressing **#. The padlock icon on the top-right of the screen will change from closed to open.

Step 4 Navigate to the profile you want to change and press the **Change** softkey.

Step 5 Navigate to and select **WLAN Configuration**.

Step 6 Navigate to and select **Security Mode**.

Step 7 Navigate to and select **EAP-FAST**.

Step 8 Press the **Save** soft-key.

Step 9 Navigate to and select **UserName**.

Step 10 Use the IP phone's keypad to enter a *username* (press the **Select** button to enter).

Step 11 Navigate to and select **Password**.

Step 12 Use the IP phone's keypad to enter a *password* (press the select button to enter).

Step 13 Press the **Back** softkey until *Network Profiles* re-appears.

Step 14 Select the newly added profile for EAP-FAST and de-select the old profile.

Step 15 Press the **Back** softkey until the **Exit** softkey appears.

Step 16 Press the **Exit** softkey,

Cisco Unified Wireless IP Phone 7921 RF Considerations

A well-designed and effectively deployed RF environment is critical for a successful VoWLAN implementation. A wireless network that appears to function well for data traffic might provide unsatisfactory coverage for a voice deployment. This is because data applications can often tolerate packet delays or recover from packet loss that would be disruptive to a voice call.

Refer to the datasheet at the following URL for Cisco Unified Wireless IP Phone 7921 RF specifications:

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

Chapter 3, "Voice over WLAN Radio Frequency Design," provides general RF deployment guidance as well as voice call capacity information. In particular, the following general VoWLAN guidelines, as stated in the RF design for voice, are applicable to the Cisco Unified Wireless IP Phone 7921:

- VoWLAN networks require overlaps of about 20 percent (for 2.4 GHz), and about 15 percent (for 5 GHz), where a WLAN data design might use an AP cell overlap of 5-to-10 percent.
- The recommended VoWLAN cell boundary recommendation is -67 dBm, while a WLAN data cell boundary might be acceptable at lower power levels.

Choosing Between IEEE 802.11b/g and IEEE 802.11a

It is a common customer requirement to deploy voice on the relatively interference-free IEEE 802.11a 5 GHz frequency band (see Chapter 3, "Voice over WLAN Radio Frequency Design," for more details). There are two ways in which voice can be restricted to just one frequency band (IEEE 802.11a or just IEEE 802.11b/g).

- By configuring the phone to use one frequency band

- By configuring the WLAN on the controller to support only one frequency band

Configuration guidance for these two option is provided in the sections that follow.

The recommended method used to limit the Cisco Unified Wireless IP Phone 7921 operation to a single frequency band is to leave the phones at their default setting and to configure the WLAN on the controller—or Cisco Wireless Control System (WCS)—to operate on the required frequency band.

Cisco Unified Wireless IP Phone 7921 RF Configuration

The Cisco Unified Wireless IP Phone 7921 is enabled for all IEEE 802.11 frequency bands (IEEE 802.11b/g and IEEE 802.11a) by default. The frequency band used can be changed with the following procedure:

Step 1 Press the **Navigation Button** downwards to enter *SETTINGS* mode.

Step 2 Navigate to and select **Network Profiles** (pressing the number adjacent to a menu item is equivalent to selecting that item).

Step 3 Unlock the phones configuration menu by pressing ****#**. The padlock icon on the top-right of the screen will change from closed to open.

Step 4 Navigate to the profile you want to change and press the **Change** softkey.

Step 5 Navigate to and select **WLAN Configuration**.

Step 6 Navigate to and select **802.11 Mode**.

Step 7 Navigate to and select the mode option you wish to use.

Step 8 Press the **Save** soft-key.

Step 9 Press the **Back** softkey until the **Exit** softkey appears.

Step 10 Press the **Exit** softkey.

The available options for IEEE 802.11 mode are shown in Table 10-1

Table 10-1 Available IEEE 802.11 Mode Options

IEEE 802.11 Mode	Description
IEEE 802.11b/g	Always use only IEEE 802.11b/g
IEEE 802.11a	Always use only IEEE 802.11a
Auto-b/g	Use IEEE 802.11b/g if available, fallback to IEEE 802.11a if not
Auto-a	Use IEEE 802.11a if available, fallback to IEEE 802.11b/g if not
Auto-RSSI	Use whatever frequency band has the strongest RSSI

Behavior in Presence of 2.4 GHz IEEE 802.11 b/g and 5 GHz

If the Cisco Unified Wireless IP Phone 7921 is enabled for both IEEE 802.11b/g and IEEE 802.11a, and receives beacons on both of these frequency bands for the voice SSID (assuming there is sufficient admission control capacity on each frequency band), the following notes apply.

On Cisco Unified Wireless IP Phone 7921 initial association:

- If the default Auto-RSSI is enabled, the phone will associate to the radio (and therefore frequency band) it acquires having the strongest Receive Signal Strength Indicator (RSSI).
- If Auto-b/g or Auto-a is enabled, the phone will associate to the frequency band specified and will fall back to the non-specified frequency band only if the specified frequency is unavailable
- If IEEE 802.11-b/g or IEEE 802.11-a is enabled, the phone will only associate to the frequency band specified.

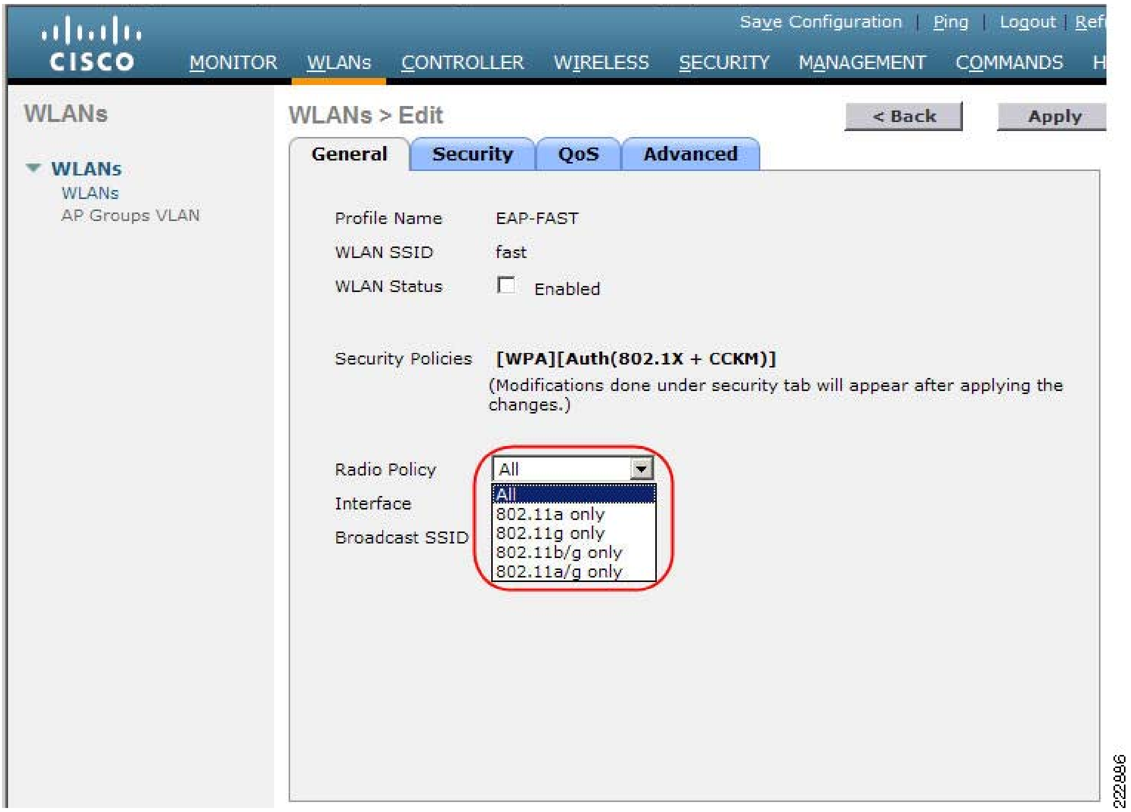
On Cisco Unified Wireless IP Phone 7921 roam:

- Once the phone has associated to an AP on a particular frequency band, it will only scan for and roam to APs on the same frequency band.
- If the Cisco Unified Wireless IP Phone 7921 has moved beyond the boundaries of the frequency band it initially associated with and cannot roam to another AP on that frequency band, then the Cisco Unified Wireless IP Phone 7921 will become disassociated and will begin the association process again (looking on both frequency bands).

WLAN RF—Controller Configuration

The recommended way to limit the Cisco Unified Wireless IP Phone 7921 operation to a single frequency band (such as IEEE 802.11a or IEEE 802.11b/g) is to leave the phone at its default setting and to configure the WLAN on the controller (or Cisco WCS) to operate on a single frequency band. Figure 10-28 shows the options available to restrict a voice VLAN to specific frequency ranges.

Figure 10-28 VLAN Radio Policy



WLANs > Edit

Profile Name EAP-FAST

WLAN SSID fast

WLAN Status □ Enabled

Security Policies [WPA][Auth(802.1X + CCKM)]

(Modifications done under security tab will appear after applying the changes.)

Radio Policy All

Interface

Broadcast SSID

All
802.11a only
802.11g only
802.11b/g only
802.11a/g only

Cisco Unified Wireless IP Phone 7921 QoS

A well-designed and effectively deployed QoS implementation is critical for a successful VoWLAN deployment. A wireless network that appears to function well for data traffic might well provide unsatisfactory performance for a voice deployment. This is because data applications can often tolerate packet delays or recover from packet loss that would be disruptive to a voice call.

Chapter 2, "WLAN Quality of Service," provides general QoS deployment guidance.

Cisco Unified Wireless IP Phone 7921 QoS Configuration

The Cisco Unified Wireless IP Phone 7921 supports the following QoS related protocols and standards;

- IEEE 802.11e/Wi-Fi Multimedia (WMM)
- Traffic Specification (TSPEC)
- Enhanced Distributed Channel Access (EDCA)
- QoS Basic Service Set (QBSS)
- Unscheduled automatic power-save delivery (U-APSD)
- Power-save mode

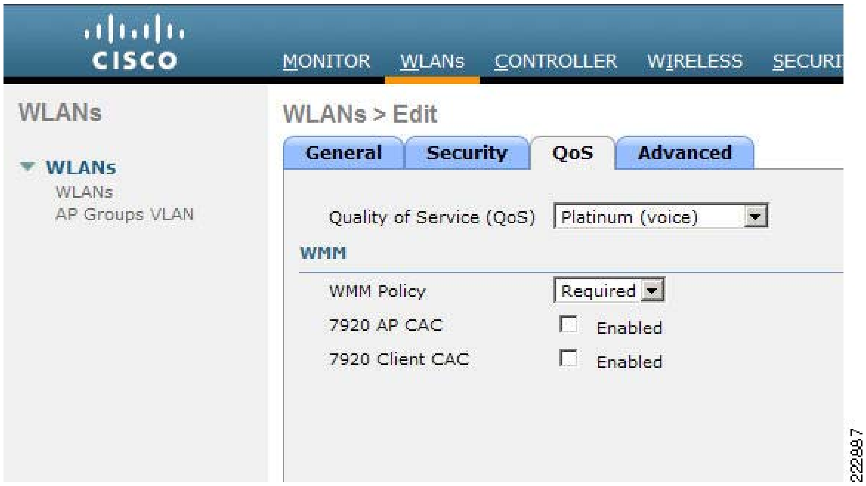
All of these features are enabled by default on the phone and will be used if enabled on the AP to which the phone associates. The QoS chapter provides more details about each of these.

Cisco WLC QoS configuration

A dedicated voice VLAN should be defined on the controller for all VoIP handsets including the Cisco Unified Wireless IP Phone 7921. The voice VLAN should be configured for the highest possible QoS by editing the VLAN and selecting the QoS tab.

As shown in Figure 10-29, in the *Quality of Service (QoS)* drop-down box *Platinum (voice)* should be selected. If only WMM-capable voice handsets, such as the Cisco Unified Wireless IP Phone 7921, are to be deployed, then the *WMM Policy* drop-down box should be set to *Required*. If there will be a mix of Cisco Unified Wireless IP Phone 7921 and nonWMM-capable devices, such as the Cisco Unified Wireless IP Phone 7920, then the WMM policy should be set to *Optional*.

Figure 10-29 Cisco WLC WLAN QoS Policy Options



WLANs > Edit

Quality of Service (QoS) Platinum (voice)

WMM

WMM Policy Required

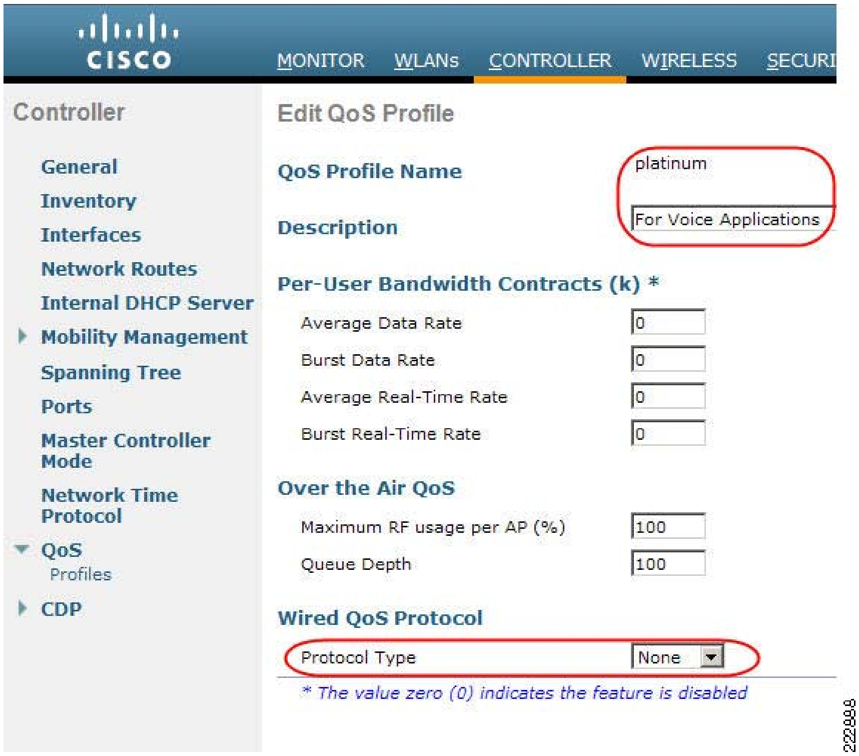
7920 AP CAC □ Enabled

7920 Client CAC □ Enabled

For each of the four QoS Profiles (*Bronze*, *Silver*, *Gold*, and *Platinum*) that can be selected for a given WLAN, there is a controller-wide option to change the characteristics of that profile.

Figure 10-30 shows an example of a *QoS Profile* edit screen. In most deployments, these settings should not be changed and the default configuration shown here should be used. More information on these options is available in the Chapter 2, "WLAN Quality of Service."

Figure 10-30 Cisco WLC Edit QoS Profile



Edit QoS Profile

QoS Profile Name platinum

Description For Voice Applications

Per-User Bandwidth Contracts (k) *

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

Over the Air QoS

Maximum RF usage per AP (%)	100
Queue Depth	100

Wired QoS Protocol

Protocol Type None

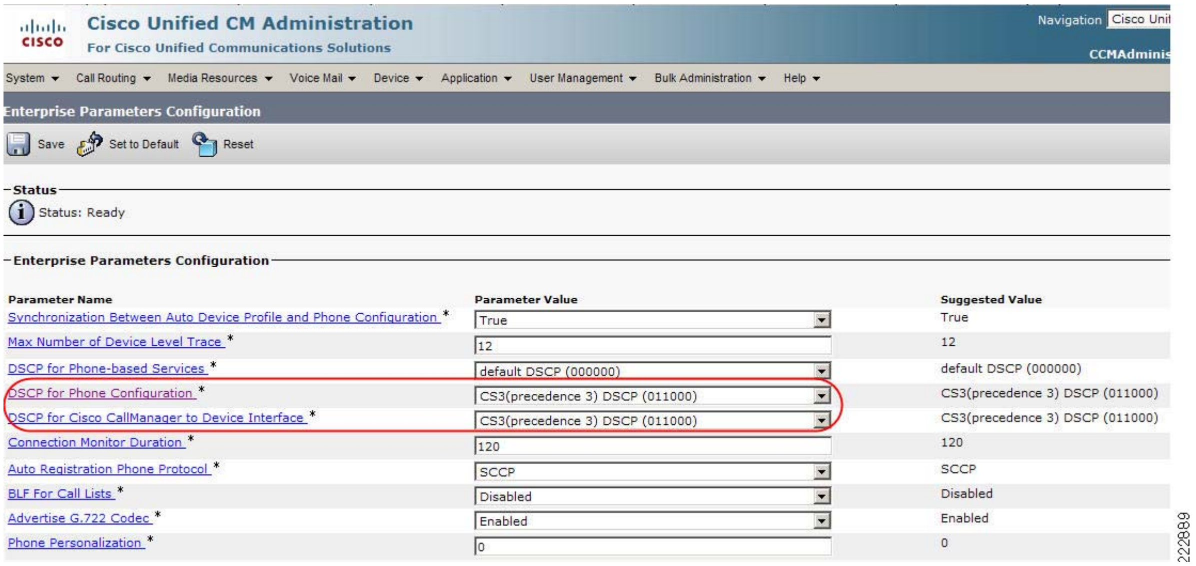
** The value zero (0) indicates the feature is disabled*

Cisco Unified Communications Manager QoS Configuration

The default Cisco Unified Communications Manager configuration contains the recommended values for Cisco Unified Communications Manager voice signaling QoS. The following relevant settings are shown in Figure 10-31 and are appropriate for most deployments:

- *DSCP for Phone Configuration*—This parameter specifies the Differentiated Service Code Point (DSCP) IP classification for any phone configuration, including any TFTP, DNS, or DHCP access necessary for phone configuration.
- *DSCP for Cisco Unified Communications Manager to Device Interface*—This parameter specifies the DSCP IP classification for protocol control interfaces used in Cisco Unified Communications Manager-to-device communications.

Figure 10-31 Cisco Unified Communications Manager QoS Parameters



Status

Status: Ready

Enterprise Parameters Configuration

Parameter Name	Parameter Value	Suggested Value
Synchronization Between Auto Device Profile and Phone Configuration *	True	True
Max Number of Device Level Trace *	12	12
DSCP for Phone-based Services *	default DSCP (000000)	default DSCP (000000)
DSCP for Phone Configuration *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
DSCP for Cisco CallManager to Device Interface *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
Connection Monitor Duration *	120	120
Auto Registration Phone Protocol *	SCCP	SCCP
BLF For Call Lists *	Disabled	Disabled
Advertise G.722 Codec *	Enabled	Enabled
Phone Personalization *	0	0

Infrastructure QoS Configuration

This section shows sample QoS configurations for switch interfaces used in the campus network. More configuration details for all the switches and routers used in this design guide is available in the Appendix , "Voice over WLAN Campus Test Architecture," testing section of this guide.

Table 10-2 shows interface commands on a Cisco 3750G access-layer switch used to connect an IP Phone. The Auto-QoS configuration statement is shown in red and the statements generated by Auto-QoS follow it.

Table 10-2 Cisco 3750G—Wired IP Phone Port Configuration

Commands	Comments

`interface GigabitEthernet2/0/3`
`description IP phone 7960`
	Interface configuration mode and description.

`switchport access vlan 50`
`switchport mode access`
	Define access VLAN for data VLAN.

Table 10-2 Cisco 3750G—Wired IP Phone Port Configuration (continued)

Commands	Comments
`switchport voice vlan 51`	Define Voice VLAN.

`switchport port-security maximum 2`
`switchport port-security`
`switchport port-security aging time 2`
`switchport port-security violation restrict`
`switchport port-security aging type inactivity`
	Define Port Security features.

`spanning-tree portfast`	Spanning tree port configuration.
`auto qos voip cisco-phone`	Auto-QoS statement entered on all voice ports

`srr-queue bandwidth share 10 10 60 20`
`srr-queue bandwidth shape 10 0 0 0`
`queue-set 2`
`mls qos trust device cisco-phone`
`mls qos trust cos`
	Platform-specific QoS statements generated by the Auto-QoS statement that is in red in the preceding line.

Table 10-3 shows interface commands on a Cisco 4503 access-layer switch used to connect an AP. The Auto-QoS configuration statement is shown in red and the statements generated by Auto-QoS follow it.

Table 10-3 Cisco 4503—AP Port

Commands	Comments

`interface FastEthernet2/16`
`description ports connected to APs in Isolation Boxes`
	Interface configuration mode and description.

`switchport access vlan 48`
`switchport mode access`
	Define access VLAN for data VLAN all APs go on the access VLAN.

`auto qos voip trust`	Auto-QoS statement entered on all AP ports.
`qos trust dscp` **Note**—The **mls qos trust dscp** command is the equivalent command format for a 3750 switch.	The Auto-QoS statement above sets the switch port to trust Layer-2 CoS. For nonrouted ports, the CoS value of the incoming packet is trusted. For routed ports, the DSCP value of the incoming packet is trusted. This **qos trust dscp** command overrides that and sets the port to trust Layer-3 DSCP instead. The link between the AP and the switch port is not trunked and does not mark Layer-2 CoS.

`tx-queue 3`
`bandwidth percent 33`
`priority high`
`shape percent 33`
`service-policy output autoqos-voip-policy`
	Platform-specific QoS statements generated by the Auto-QoS statement shown in red in preceding line.

Table 10-4 shows interface commands on a Cisco 4503 access-layer switch used as an uplink port to a distribution-layer switch. The Auto-QoS configuration statement is shown in red and the statements generated by Auto QoS follow it.

Table 10-4 Cisco 4503 Uplink Port to Distribution Layer

Commands	Comments

`interface TenGigabitEthernet1/1`
`description A4L to D3L`
	Interface configuration mode and description.

`no switchport`
`ip address 10.33.3.10 255.255.255.252`
`ip hello-interval eigrp 100 1`
`ip hold-time eigrp 100 3`
`ip authentication mode eigrp 100 md5`
`ip authentication key-chain eigrp 100`
`eigrp-chain`
`ip pim sparse-mode`
`logging event link-status`
`load-interval 30`
`carrier-delay msec 0`
	Interface configuration unrelated to QoS.

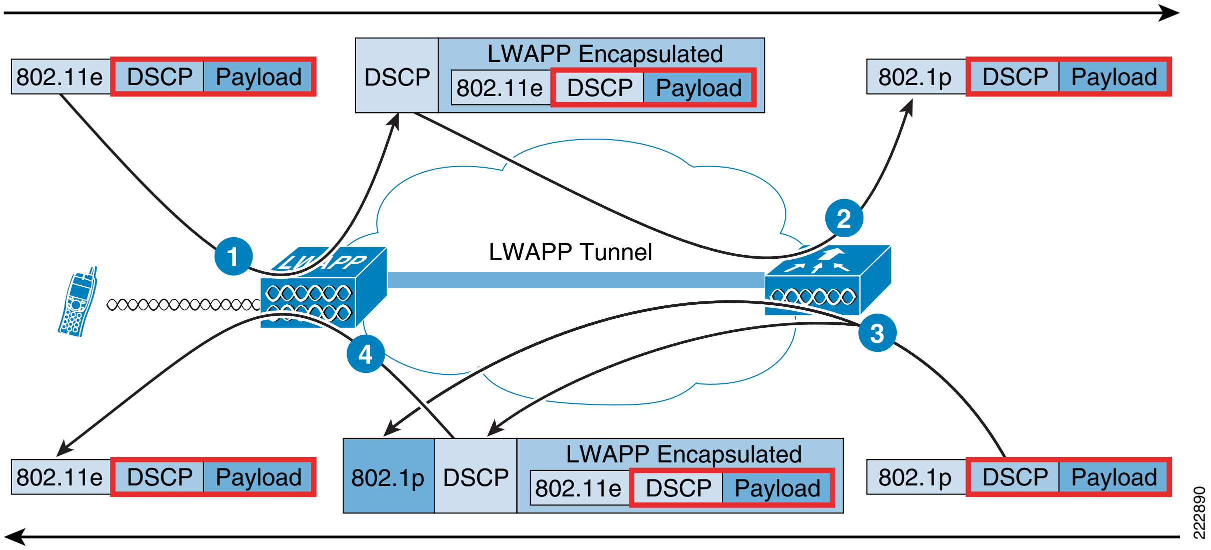
`auto qos voip trust`	

`qos trust dscp`
`tx-queue 3`
`bandwidth percent 33`
`priority high`
`shape percent 33`
`service-policy output autoqos-voip-policy`
	Platform-specific QoS statements generated by the Auto-QoS statement that is in red in the line above
	Note—Because this is a Layer-3 port, the **auto qos voip trust** command sets **qos trust dscp** not **qos trust cos** as it did in Table 10-3.

End-to-End QoS Mapping

In the centralized WLAN architecture, WLAN data is tunneled between the AP and the wireless LAN controller via LWAPP. In order to maintain the original QoS classification across this tunnel, the QoS settings of the encapsulated data packet must be appropriately mapped to the Layer 2 (IEEE 802.1p) and Layer 3 (IP DSCP) fields of the outer tunnel packet. See Figure 10-32.

Figure 10-32 End-to-end QoS Packet Marking Mappings



The original IP packet DSCP and user-data—sent by the WLAN client to the AP or received by the controller from the wired network infrastructure—are transmitted unaltered across the LWAPP tunnel between the AP and the controller. The Layer-2 and Layer-3 QoS markings are only changed on the headers that encapsulate the original IP packet. Table 10-5 provides additional marker mapping elaboration for the numbered labels in Figure 10-32.

Table 10-5 End-to-end QoS Packet Marking Mappings

Label Number[1]	From	To	Outbound UP (IEEE 802.1p/IEEE 802.11e) Mapping	Outbound IP DSCP Mapping
1	AP	Controller	N/A (APs do not support IEEE 802.1Q / IEEE 802.1p tags on the wired interface).	*WMM Client (such as Cisco Unified Wireless IP Phone 7921)*—Police the IEEE 802.11e UP value to ensure it does not exceed the maximum value allowed for the QoS policy assigned to that client; translate the value to the DSCP value. *Regular Client*—Use the IEEE 802.11e UP value for the QoS policy assigned to that client's WLAN; translate the value to the DSCP value.
2	Controller	Ethernet Switch	Translate the DSCP value of the incoming LWAPP packet to the IEEE 802.1p UP value. **Note**—The AP has policed the upstream DSCP (when it mapped from IEEE 802.1p UP to DSCP)	N/A (The original/encapsulated DSCP value is preserved) **Note**—The DSCP is un-policed; it is whatever was set by the WLAN client.
3	Controller	AP	Translate the DSCP value of the incoming packet to the Cisco Architecture for Voice, Video and Integrated Data (AVVID) IEEE 802.1p UP value. **Note**—The QoS profile is used to police the maximum IEEE 802.1p value that can be set	Copy the DSCP value from the incoming packet. **Note**—No policing is performed here; it is assumed that traffic was policed at ingress to the network.
4	AP	Wireless Client	*WMM Client (such as Cisco Unified Wireless IP Phone 7921)*—Translate the DSCP value of the incoming LWAPP packet to the IEEE 802.11e UP value. Police the value to ensure it does not exceed the maximum value allowed for the WLAN QoS policy assigned to the WLAN the client belongs to. Place packet in the IEEE 802.11 Tx queue appropriate for the UP value. *Regular Client*—Place packet in the default IEEE 802.11 Tx queue for the WLAN QoS policy assigned to that client.	N/A (original/encapsulated DSCP value is preserved).

1. Refer to Figure 10-32.

Table 10-6 provides the translations that occur between IEEE 802.11e/IEEE 802.1p UP values and IP DSCP values. Because Cisco AVVID defines the translation from IEEE 802.1 UP to IP DSCP, and the IEEE defines the translation from IP DSCP to IEEE 802.11e UP, two different sets of translations must be used.

Table 10-6 QoS Packet Marking Translations

Cisco AVVID IEEE 802.1p UP-Based Traffic Type	Cisco AVVID IP DSCP	Cisco AVVID IEEE 802.1p UP	IEEE 802.11e UP	Notes
Network Control	–	7	–	Reserved for network control only
Inter-Network Control	48	6	7 (AC_VO)	LWAPP control
Voice	46 (EF)	5	6 (AC_VO)	*Controller*—Platinum QoS profile
Video	34 (AF41)	4	5 (AC_VI)	*Controller*—Gold QoS profile
Voice Control	26 (AF31)	3	4 (AC_VI)	–
Best Effort	0 (BE)	0	3 (AC_BE) 0 (AC_BE)	*Controller*— Silver QoS profile –
Transaction Data	18 (AF21)	2	2 (AC_BK)	–
Bulk Data	10 (AF11)	1	1 (AC_BK)	*Controller*— Bronze QoS profile.

Cisco Unified Wireless IP Phone 7921 Troubleshooting

This section will focus on troubleshooting that is specific to the Cisco Unified Wireless IP Phone 7921G. For additional troubleshooting information, refer to Chapter 9, “Voice over WLAN Troubleshooting and Management Tools.”

Configuration Checklist

When configuring your wireless LAN controller, use the following guidelines:

Step 1 Set the QoS policy to *Platinum*.

Step 2 Enable WMM to enable QoS and the ability to use U-APSD.

Step 3 Disable DHCP address assignment required.

Step 4 Ensure *Aggressive Load Balancing* is disabled.

Step 5 If you have clients from other regions that will attempt to associate with the WLAN, enable World Mode (IEEE 802.11d).

Verify Coverage with Cisco Unified Wireless IP Phone 7921G

Chapter 9, "Voice over WLAN Troubleshooting and Management Tools," covers the management of the RF deployment using the Cisco WCS, Cisco WLC, as well as using third-party site-survey and WLAN analysis tools. This section describes how the Cisco Unified Wireless IP Phone 7921G can be used to validate the RF design provided by those tools.

Wireless LAN performance varies from client device to client device. A client with a strong transmit signal and a high receiver sensitivity will perform better in marginal WLAN coverage than a client with weaker radio characteristics. For this reason, it is recommended that WLAN coverage is validated with the actual device you intend to use (in addition to using professional site survey tools such as *AirMagnet Survey* and *Cisco Cisco Spectrum Expert Analysis*).

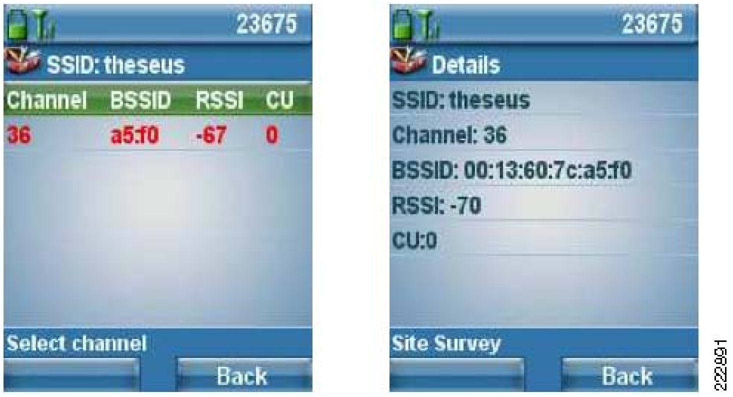
After the initial deployment of wireless phones in the WLAN, it is a good practice to perform site surveys at regular intervals to verify that the APs are providing adequate coverage and that wireless phones can roam from one AP to another without audio problems. You should use the Cisco Unified Wireless IP Phone 7921G to verify that the signal range and transmission power provide adequate coverage for roaming phones.

Access the *Site Survey* menu on the phone by pressing **Settings** > **Status** > **Site Survey**

Note When not in a call, the Cisco Unified Wireless IP Phone 7921G only scans other non-associated channels when the current signal lowers to a certain threshold, so you might see the AP with which it is associated in the list. To see all APs, place a call from the Cisco Unified Wireless IP Phone 7921G to a wired IP phone where scanning occurs constantly while the phone call is active.

Figure 10-33 shows an example display output from a Cisco Unified Wireless IP Phone 7921.

Figure 10-33 Cisco Unified Wireless IP Phone 7921 Site Survey Screen Capture



SSID: theseus

Channel	BSSID	RSSI	CU
36	a5:f0	-67	0

Details

SSID: theseus
Channel: 36
BSSID: 00:13:60:7c:a5:f0
RSSI: -70
CU:0

Cisco Unified Wireless IP Phone 7921 coverage statistics can also be viewed by using Telnet to connect to the Cisco Unified Wireless IP Phone 7921.

Cisco Unified Wireless IP Phone 7921 Web Page Access

You can access the web page for any Cisco Unified Wireless IP Phone 7921G that is connected to the WLAN. Be sure the phone is powered on and connected. To access the web page for the Cisco Unified Wireless IP Phone 7921G follow these steps:

- Enabling or Disabling IP Phone Web Access from Cisco Unified Communications Manager, page 10-35
- Access the Cisco Unified Wireless IP Phone 7921s Web Pages, page 10-35

These procedure are summarized in the brief sections that follow.

Enabling or Disabling IP Phone Web Access from Cisco Unified Communications Manager

Web access for IP phones is enabled by default on Cisco Unified Communications Manager. The following steps are required to disable or re-enable web access.

Step 1 Navigate to the *Phone Configuration* web page in Cisco Unified Communications Manager Administration and set the *Web Access* field to *Read Only* or *Disabled*.

Step 2 Reset the phone from Cisco Unified Communications Manager to implement the change in web access policy.

Access the Cisco Unified Wireless IP Phone 7921s Web Pages

Step 1 Obtain the IP address of the Cisco Unified Wireless IP Phone 7921G using one of these methods:

a. Search for the phone in Cisco Unified Communications Manager by choosing *Devices* > *Phones*. Phones registered with Cisco Unified Communications Manager display the IP address on the *Find* and *List Phones* web page and at the top of the *Phone Configuration* web page.

b. On the Cisco Unified Wireless IP Phone 7921G, press **Settings** > **Device Information** > **Network Configuration** and then scroll to the *IP Address* option.

Step 2 Open a web browser and enter the following URL, where *IP_address* is the IP address of the Cisco Unified IP Phone: **https://***IP-address*

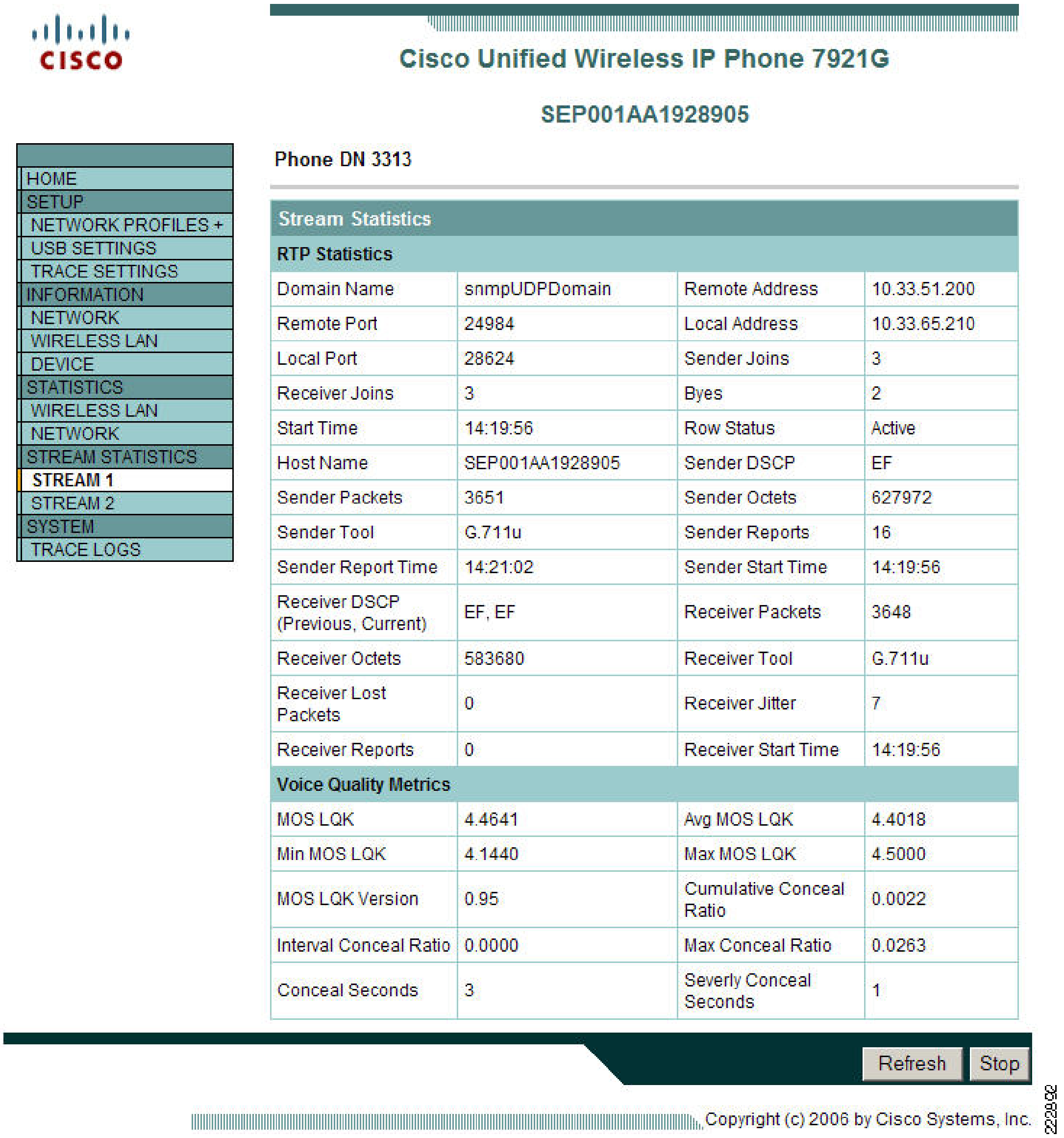
Note When the *Security Alert* dialog box displays a notice to accept the Trust Certificate, click **Yes** or **Always** to accept the application.

Step 3 Log in to the web pages with the username *admin* and enter the password *Cisco* for the phone web pages.

Step 4 View the informational pages and changes to configurable pages as needed.

Figure 10-34 provides an example display showing some of the information that is available from the Cisco Unified Wireless IP Phone 7921 web pages.

Figure 10-34 Cisco Unified Wireless IP Phone 7921 Stream Statistics



Cisco Unified Wireless IP Phone 7921G

SEP001AA1928905

Phone DN 3313

Stream Statistics

RTP Statistics			
Domain Name	snmpUDPDomain	Remote Address	10.33.51.200
Remote Port	24984	Local Address	10.33.65.210
Local Port	28624	Sender Joins	3
Receiver Joins	3	Byes	2
Start Time	14:19:56	Row Status	Active
Host Name	SEP001AA1928905	Sender DSCP	EF
Sender Packets	3651	Sender Octets	627972
Sender Tool	G.711u	Sender Reports	16
Sender Report Time	14:21:02	Sender Start Time	14:19:56
Receiver DSCP (Previous, Current)	EF, EF	Receiver Packets	3648
Receiver Octets	583680	Receiver Tool	G.711u
Receiver Lost Packets	0	Receiver Jitter	7
Receiver Reports	0	Receiver Start Time	14:19:56
Voice Quality Metrics			
MOS LQK	4.4641	Avg MOS LQK	4.4018
Min MOS LQK	4.1440	Max MOS LQK	4.5000
MOS LQK Version	0.95	Cumulative Conceal Ratio	0.0022
Interval Conceal Ratio	0.0000	Max Conceal Ratio	0.0263
Conceal Seconds	3	Severly Conceal Seconds	1

Copyright (c) 2006 by Cisco Systems, Inc.

References

Please see the following publications for additional information:

- *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

- *Wireless LAN Controller Documentation*
  http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html
- *Cisco Wireless Control System Configuration Guide*
  http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

CHAPTER 11

Voice over WLAN Vocera Implementation

Vocera Overview

The Vocera Communications System enables wireless voice communication that users control with naturally spoken commands. The system is primarily targeted at hospitals, hotels, retail stores, and other in-building environments where mobile workers must stay in contact to perform their jobs. The Vocera Communications System consists of two key components:

- Vocera System Software—Controls and manages call activity
- Vocera Communications Badge—A lightweight, wearable, voice-controlled communication device that operates over a wireless LAN (IEEE 802.11b/g)

The Vocera Badge is briefly discussed in this chapter with minimum configurations required to integrate it with Cisco Unified Communications Manager.

The *Vocera User Guide*, *Configuration Guide*, and *Infrastructure Planning Guide* can be found at http://www.vocera.com/documentation/default.aspx

Note The first Badge release by Vocera is the B1000A and is the subject of this design guide. Vocera has since announced the Vocera Communications Badge B2000 with an improved wireless radio which will support WiFi Multimedia (WMM). This announcement occurred as this design guide was in the process of being released so no testing has been done on the new B2000 Badge.

Vocera System Software

The Vocera System Software platform runs on a standard Windows server and contains the system intelligence, including managing calls call connections, and user profiles, as well as the Nuance speech recognition and voice-print verification software. The Administrative Console allows system administrators to set global preferences and permissions for users. User preferences are configured on the server via browser-based Administration and User Consoles.

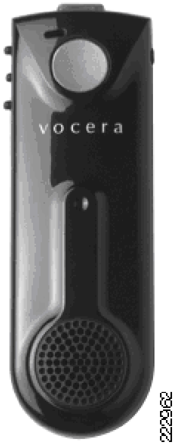
The Vocera versions used for this design guide are as follows:

- Vocera Server 4.0 [Build 1279]
- Vocera Telephony Server 4.0 [Build 1279]
- Vocera Badge V4.0 1273

Vocera Communications Badge

The Vocera Communications Badge is a small, lightweight, wearable, wireless device that provides a voice-controlled user interface to the Vocera Communications System. The Vocera Communications Badge enables instant, hands-free conversations among people throughout the workplace. It contains a speaker, microphone, wireless radio, and a backlit LCD that shows caller ID, text messages and alerts. A Vocera Communications Badge is shown in Figure 11-1.

Figure 11-1 Vocera Communications Badge



Vocera Architecture

This section addresses the following Vocera architecture topics:

- Main Components, page 11-2
- Badge Overview, page 11-3
- Badge-to-Badge Communication, page 11-4
- Badge Telephony Communication, page 11-4
- Vocera Broadcast, page 11-5
- Badge Location Function, page 11-6

Main Components

Primary Vocera system components consist of the following elements:

- *Vocera Server Program*—Provides the central system functionality, and calls on the other components for specific services.
- *Embedded MySQL Database*—Stores user profiles (which contain personal information and Badge settings), group and location information, and system settings.
- *Nuance*^{TM} *Speech Recognition, Verifier, and Vocalizer Software*—Provides the speech recognition, voiceprint authentication, and text-to-speech engines used by the Vocera voice interface.

- *Apache/Tomcat Web Serve*—Hosts the browser-based Administration Console and User Console applications.

Software Utilities

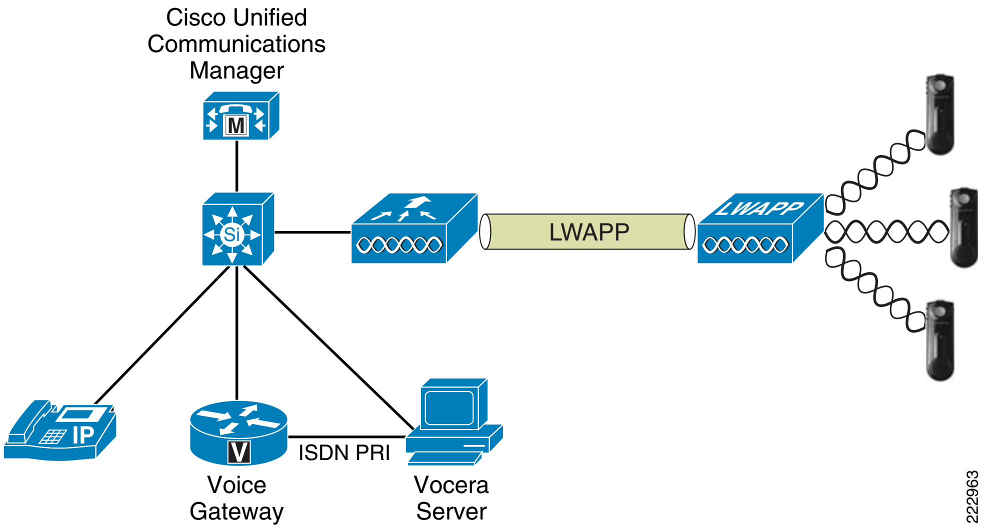
The Vocera system software includes the following utilities:

- *Badge Properties Editor*—Allows setting values for Badge properties so the Vocera Badges can connect to the wireless network.
- *Badge Configuration Utility*—Downloads the properties set with the Badge Properties Editor, as well as any firmware upgrades, to the Badges.
- *Vconfig Utility*—Provides interactive setting of individual properties and to download individual firmware components to a Badge.

The Vocera system can be a standalone communications system with Badge-to-Badge communication only. Typically the system is installed in conjunction with a PBX to allow hardphone (wired)-to-Vocera Badge communications, as well as access through the PBX to the Public Switched Telephone Network (PSTN). For this communication to take place, an Intel Dialogic board must be installed in the Vocera System Server. For this design guide an Intel Dialogic D/480JCT-1T1 (North America, T1/PRI) was used. For a list of other supported analog and digital integrations refer to the Vocera Datasheet.

A high level diagram is shown in Figure 11-2.

Figure 11-2 Vocera Architecture Diagram



Badge Overview

The Badges are centrally maintained by the Vocera Server from a single configuration file for all Badges. The Badge does not have a keyboard, so this single configuration file is uploaded to all Badges. The Badge does not maintain a static DN or ID (as a typical phone would have). Instead, each Badge defines its identity when a user logs in. As a necessary consequence of this centralized management, all Badge properties, including the SSID and security settings that allow it to connect to the network, must be the same. In turn, all APs to which the Vocera Badge can connect must also share the same SSID and security settings.

The Vocera Badge supports the following wireless networks, and authentication and encryption capabilities:

- *Wireless Network Support*—IEEE 802.11b/g wireless network with multicast and UDP unicast packet delivery
- *Authentication*—Types supported include the following:
  - Open
  - Wi-Fi Protected Access-Pre-shared Key (WPA-PSK)
  - WPA-Protected Extensible Authentication Protocol (PEAP)
  - Lightweight Extensible Authentication Protocol (LEAP)
- *Encryption*—Types supported include the following:
  - 64/128 bit Wired Equivalent Privacy (WEP)
  - Temporal Key Integrity Protocol (TKIP)
  - Message Integrity Check (MIC)
  - Cisco Temporal Key Integrity Protocol (CKIP)

Note Vocera supports Autonomous and Lightweight Access Point Protocol (LWAPP). Refer to the "Vocera IP Phone Deployment" chapter in *Cisco Unified Wireless Network Infrastructure* for more information on deploying Vocera in a Wireless Network.

Badge-to-Badge Communication

When one Vocera user calls another user, the Badge first contacts the Vocera Server which looks up the IP address of the callee's Badge and contacts the Badge user to ask the user if he/she can take a call. If the callee accepts the call, the Vocera Server will notify the calling Badge of the callee Badge's IP address to setup direct communication between the Badges with no further server intervention. All communication with the Vocera Server uses the G.711 CODEC and all Badge-to-Badge communication uses a Vocera proprietary CODEC.

Badge Telephony Communication

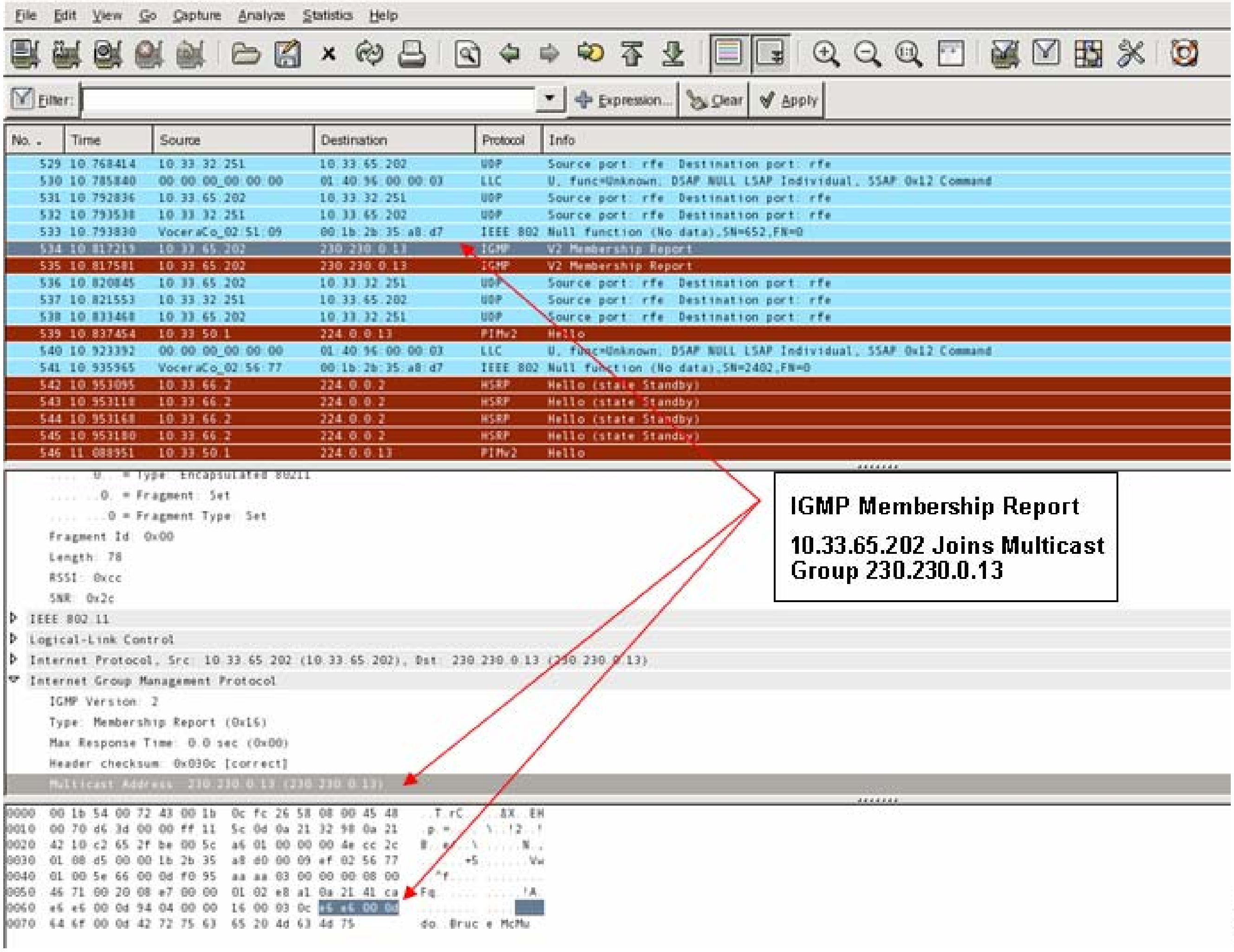
When the Vocera Telephony Server is installed and setup with a connection to a PBX, a user is able to call internal extensions off of the PBX or outside telephone lines. Vocera allows users to make calls by either saying the numbers (five, six, three, two) or by creating an address book entry in the Vocera database for the person or function at that number (for example, pharmacy, home, pizza) the Vocera server determines the number that is being called, either by intercepting the numbers in the extension or by looking up the name in the database and selecting the number. The Vocera Server then passes that information to the Vocera Telephone Server which connects to the PBX and generates the appropriate telephony signaling (ex. DTMF). All media is via UDP using g711, but call signaling between the Vocera Server (VS) and Vocera Telephony Server (VTS) is via a TCP connection between the two. Once a call is established, media between the VS and VTS or between the badge and VTS is g711 via UDP.

Vocera Broadcast

A Vocera Badge user can call and communicate to a group of Vocera Badges at the same time by using the **broadcast** command. When a user broadcasts to a group, the users Badge sends the command to the Vocera Server who looks up the members of a group, determines which members of the group are active, assigns a multicast address to use for this broadcast session, and sends a message to each active user's Badge instructing it to join the multicast group with the assigned multicast address. More information on Vocera Multicast in an LWAPP environment can be found at "Vocera IP Phone Deployment" chapter in *Cisco Unified Wireless Network Infrastructure*.

Filtering a trace on IGMP Protocol allows you to see the Membership Report of a device joining the multicast group. Figure 11-3 illustrates the Badge with an IP Address of 10.33.65.202 joins Multicast Group 230.230.0.13 (hex e6 e6 00 0d).

Figure 11-3 Vocera Badge Joining Multicast Group



```
No. .  Time        Source              Destination         Protocol   Info
   529 10.768414   10.33.32.251        10.33.65.202        UDP        Source port: rfe  Destination port: rfe
   530 10.785840   00:00:00_00:00:00   01:40:96:00:00:03   LLC        U, func=Unknown; DSAP NULL LSAP Individual, SSAP 0x12 Command
   531 10.792836   10.33.65.202        10.33.32.251        UDP        Source port: rfe  Destination port: rfe
   532 10.793538   10.33.32.251        10.33.65.202        UDP        Source port: rfe  Destination port: rfe
   533 10.793830   VoceraCo_02:51:09   00:1b:2b:35:a8:d7   IEEE 802   Null function (No data),SN=652,FN=0
   534 10.817219   10.33.65.202        230.230.0.13        IGMP       V2 Membership Report
   535 10.817581   10.33.65.202        230.230.0.13        IGMP       V2 Membership Report
   536 10.820845   10.33.65.202        10.33.32.251        UDP        Source port: rfe  Destination port: rfe
   537 10.821553   10.33.32.251        10.33.65.202        UDP        Source port: rfe  Destination port: rfe
   538 10.833468   10.33.65.202        10.33.32.251        UDP        Source port: rfe  Destination port: rfe
   539 10.837454   10.33.50.1          224.0.0.13          PIMv2      Hello
   540 10.923392   00:00:00_00:00:00   01:40:96:00:00:03   LLC        U, func=Unknown; DSAP NULL LSAP Individual, SSAP 0x12 Command
   541 10.935965   VoceraCo_02:56:77   00:1b:2b:35:a8:d7   IEEE 802   Null function (No data),SN=2402,FN=0
   542 10.953095   10.33.66.2          224.0.0.2           HSRP       Hello (state Standby)
   543 10.953118   10.33.66.2          224.0.0.2           HSRP       Hello (state Standby)
   544 10.953168   10.33.66.2          224.0.0.2           HSRP       Hello (state Standby)
   545 10.953180   10.33.66.2          224.0.0.2           HSRP       Hello (state Standby)
   546 11.088951   10.33.50.1          224.0.0.13          PIMv2      Hello
```

```
    .... .0.. = Type: Encapsulated 80211
    .... ..0. = Fragment: Set
    .... ...0 = Fragment Type: Set
    Fragment Id: 0x00
    Length: 78
    RSSI: 0xcc
    SNR: 0x2c
▷ IEEE 802.11
▷ Logical-Link Control
▷ Internet Protocol, Src: 10.33.65.202 (10.33.65.202), Dst: 230.230.0.13 (230.230.0.13)
▽ Internet Group Management Protocol
    IGMP Version: 2
    Type: Membership Report (0x16)
    Max Response Time: 0.0 sec (0x00)
    Header checksum: 0x030c [correct]
    Multicast Address: 230.230.0.13 (230.230.0.13)
```

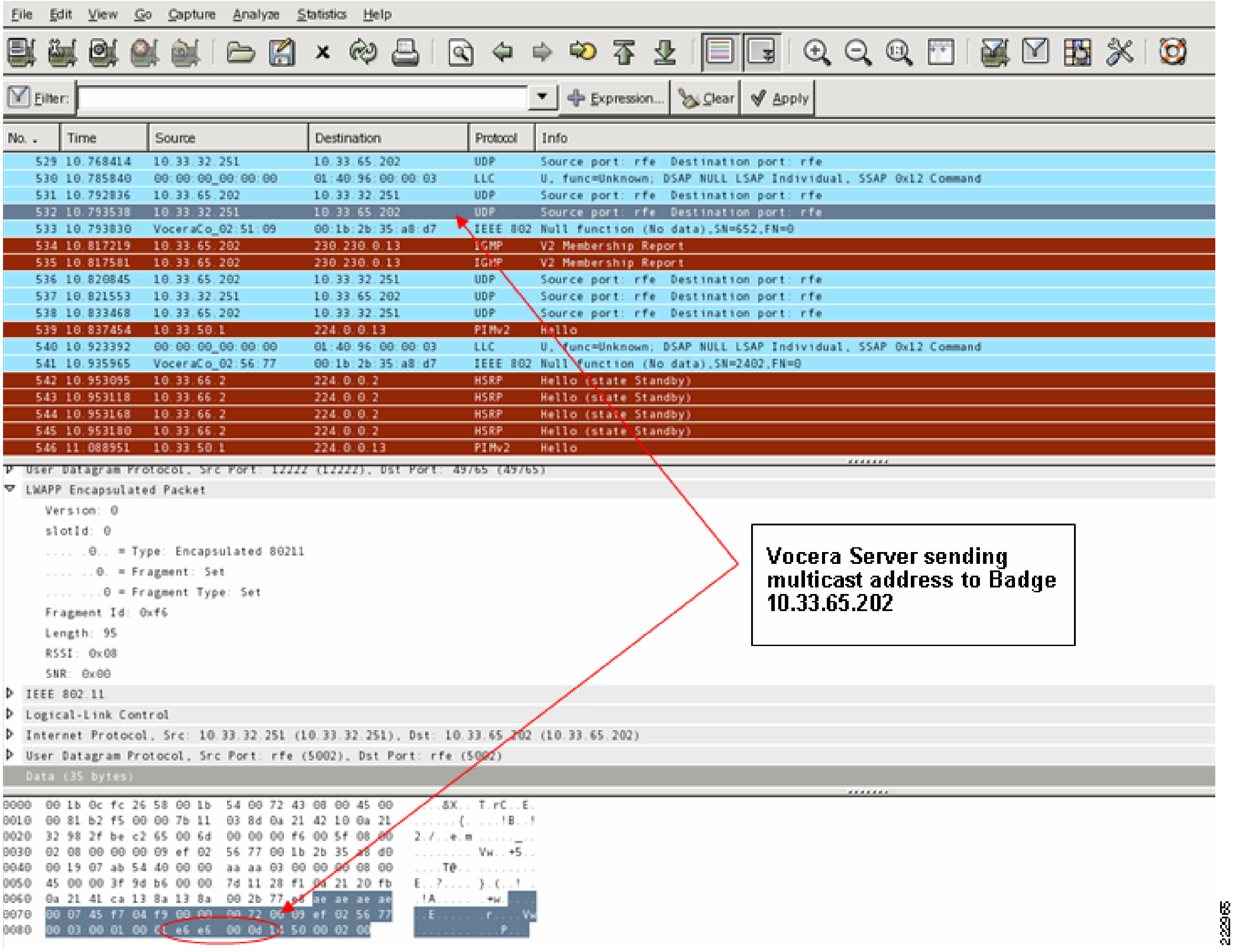
```
0000  00 1b 54 00 72 43 00 1b  0c fc 26 58 08 00 45 48   ..T.rC.. ..&X..EH
0010  00 70 d6 3d 00 00 ff 11  5c 0d 0a 21 32 98 0a 21   .p.=.... \..!2..!
0020  42 10 c2 65 2f be 00 5c  a6 01 00 00 00 4e cc 2c   B..e/..\ .....N.,
0030  01 08 d5 00 00 1b 2b 35  a8 d0 00 09 ef 02 56 77   ......+5 ......Vw
0040  01 00 5e 66 00 0d f0 95  aa aa 03 00 00 00 08 00   ..^f.... ........
0050  46 71 00 20 08 e7 00 00  01 02 e8 a1 0a 21 41 ca   Fq...... .....!A.
0060  e6 e6 00 0d 94 04 00 00  16 00 03 0c e6 e6 00 0d   ........ ........
0070  64 6f 00 0d 42 72 75 63  65 20 4d 63 4d 75         do..Bruc e McMu
```

IGMP Membership Report

10.33.65.202 Joins Multicast Group 230.230.0.13

After locating the Membership Report of a specific Badge joining the multicast group, look earlier in the trace for the occurrence of the Vocera Server as the source and the Badge in question as the destination. See Figure 11-4. In this example the Badge is 10.33.65.202 and the Vocera Server is 10.33.32.251. In the data you will see the occurrence of e6 e6 00 0d (hex representation of the multicast address 230.230.0.13).

Figure 11-4 Vocera Server Sending Multicast Address to Vocera Badge


File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
Vocera Server sending multicast address to Badge 10.33.65.202
222965

No. .	Time	Source	Destination	Protocol	Info
529	10.768414	10.33.32.251	10.33.65.202	UDP	Source port: rfe Destination port: rfe
530	10.785840	00:00:00_00:00:00	01:40:96:00:00:03	LLC	U, func=Unknown; DSAP NULL LSAP Individual, SSAP 0x12 Command
531	10.792836	10.33.65.202	10.33.32.251	UDP	Source port: rfe Destination port: rfe
532	10.793538	10.33.32.251	10.33.65.202	UDP	Source port: rfe Destination port: rfe
533	10.793830	VoceraCo_02:51:09	00:1b:2b:35:a8:d7	IEEE 802	Null function (No data),SN=652,FN=0
534	10.817219	10.33.65.202	230.230.0.13	IGMP	V2 Membership Report
535	10.817581	10.33.65.202	230.230.0.13	IGMP	V2 Membership Report
536	10.820845	10.33.65.202	10.33.32.251	UDP	Source port: rfe Destination port: rfe
537	10.821553	10.33.32.251	10.33.65.202	UDP	Source port: rfe Destination port: rfe
538	10.833468	10.33.65.202	10.33.32.251	UDP	Source port: rfe Destination port: rfe
539	10.837454	10.33.50.1	224.0.0.13	PIMv2	Hello
540	10.923392	00:00:00_00:00:00	01:40:96:00:00:03	LLC	U, func=Unknown; DSAP NULL LSAP Individual, SSAP 0x12 Command
541	10.935965	VoceraCo_02:56:77	00:1b:2b:35:a8:d7	IEEE 802	Null function (No data),SN=2402,FN=0
542	10.953095	10.33.66.2	224.0.0.2	HSRP	Hello (state Standby)
543	10.953118	10.33.66.2	224.0.0.2	HSRP	Hello (state Standby)
544	10.953168	10.33.66.2	224.0.0.2	HSRP	Hello (state Standby)
545	10.953180	10.33.66.2	224.0.0.2	HSRP	Hello (state Standby)
546	11.088951	10.33.50.1	224.0.0.13	PIMv2	Hello

```
▷ User Datagram Protocol, Src Port: 12222 (12222), Dst Port: 49765 (49765)
▽ LWAPP Encapsulated Packet
    Version: 0
    slotId: 0
    .... .0.. = Type: Encapsulated 80211
    .... ..0. = Fragment: Set
    .... ...0 = Fragment Type: Set
    Fragment Id: 0xf6
    Length: 95
    RSSI: 0x08
    SNR: 0x00
▷ IEEE 802.11
▷ Logical-Link Control
▷ Internet Protocol, Src: 10.33.32.251 (10.33.32.251), Dst: 10.33.65.202 (10.33.65.202)
▷ User Datagram Protocol, Src Port: rfe (5002), Dst Port: rfe (5002)
  Data (35 bytes)
```

```
0000  00 1b 0c fc 26 58 00 1b  54 00 72 43 08 00 45 00   ....&X.. T.rC..E.
0010  00 81 b2 f5 00 00 7b 11  03 8d 0a 21 42 10 0a 21   ......{. ...!B..!
0020  32 98 2f be c2 65 00 6d  00 00 00 f6 00 5f 08 00   2./..e.m ....._..
0030  02 08 00 00 00 09 ef 02  56 77 00 1b 2b 35 a8 d0   ........ Vw..+5..
0040  00 19 07 ab 54 40 00 00  aa aa 03 00 00 00 08 00   ....T@.. ........
0050  45 00 00 3f 9d b6 00 00  7d 11 28 f1 0a 21 20 fb   E..?.... }.(..! .
0060  0a 21 41 ca 13 8a 13 8a  00 2b 77 e8 ae ae ae ae   .!A..... .+w.....
0070  00 07 45 f7 04 f9 00 00  00 72 00 09 ef 02 56 77   ..E..... .r....Vw
0080  00 03 00 01 00 00 e6 e6  00 0d 1b 50 00 02 00      ........ ..P...
```

Badge Location Function

The Vocera Server keeps track of the AP to which each active Badge is associated as each Badge will send a 30 second keepalive to the server with the associated BSSID. This allows the Vocera system to roughly estimate the location of a Badge user. This function has a relatively low degree of accuracy because a Badge might not be associated to the AP to which it is closest. A more accurate solution for finding the location of a device is the Cisco Location-Based Services (LBS).

WLAN Controller Base Configuration

This section addresses creating a Voice WLAN.

Create Voice WLAN

Creating a WLAN with the minimum necessary configuration needed to test Vocera connectivity can be done in the following steps on the controller GUI.

Step 1 Click the **WLANs** tab in the controller GUI.

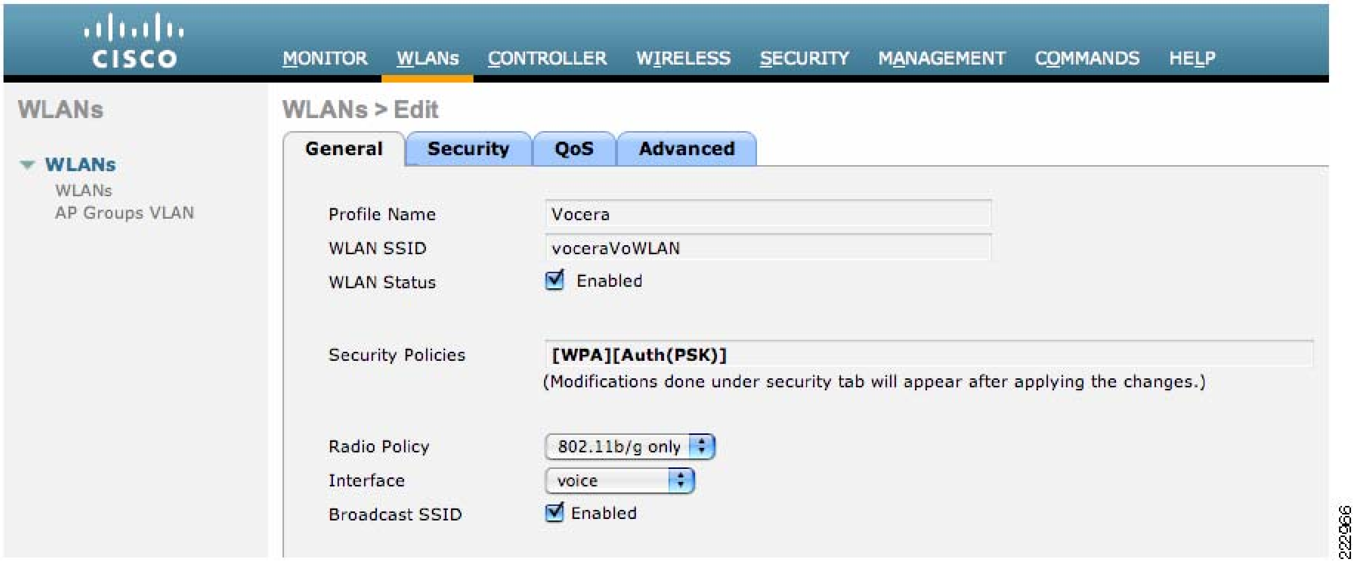
Step 2 Click the **New** button at the top-right corner of the page.

Step 3 Define a *profile name* and *SSID* (often the same string is used for both) for the new WLAN.

Step 4 Click **Apply**.

Step 5 The *WLANs > Edit* page loads. See Figure 11-5.

Figure 11-5 WLANs > Edit Page



Profile Name Vocera
WLAN SSID voceraVoWLAN
WLAN Status ☑ Enabled
Security Policies [WPA][Auth(PSK)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy 802.11b/g only
Interface voice
Broadcast SSID ☑ Enabled

Step 6 Check the *WLAN Status* box to signal that this new WLAN should be enabled.

Step 7 Change the *Interface* drop-down box to point to a user-defined dynamic interface (you must have predefined a dynamic interface; do not use the management interface).

Step 8 Click the **Security** tab.

Step 9 Change the *Layer-2 Security* drop-down box to **WPA-PSK**.

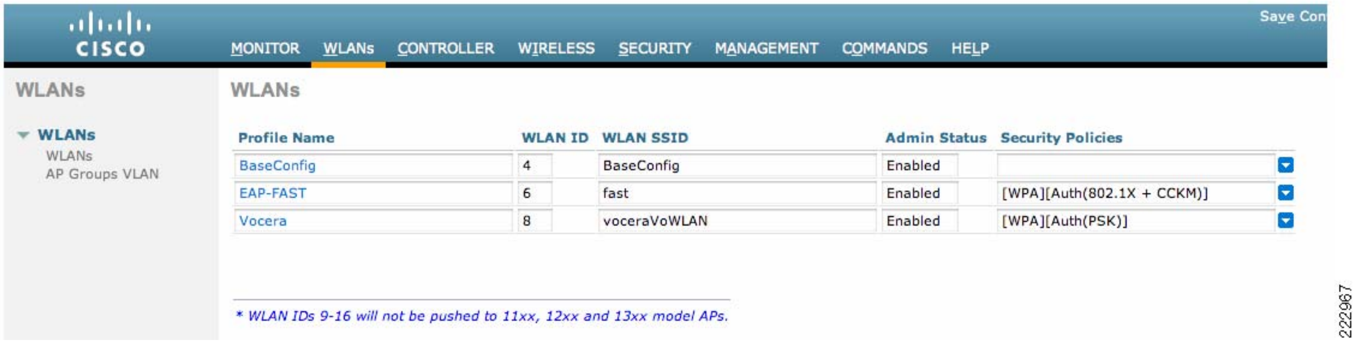
Step 10 Click the **QoS** tab.

Step 11 Change the *Quality of Service (QoS)* drop-down box to **Platinum (voice)**.

Step 12 Click the **Apply** button at the top-right corner of the page.

When the base controller WLAN configuration is complete, the WLAN page should look similar to the page shown in Figure 11-6.

Figure 11-6 WLANs Page with Vocera VoWLAN



WLANs

Profile Name	WLAN ID	WLAN SSID	Admin Status	Security Policies
BaseConfig	4	BaseConfig	Enabled	
EAP-FAST	6	fast	Enabled	[WPA][Auth(802.1X + CCKM)]
Vocera	8	voceraVoWLAN	Enabled	[WPA][Auth(PSK)]

* WLAN IDs 9-16 will not be pushed to 11xx, 12xx and 13xx model APs.

Vocera Configuration

This section addresses Vocera Server and Vocera Badge configuration.

Server and Badge Configuration

Since the Vocera Badge has no keyboard for the entry of network settings, the computer running the Vocera Badge Configuration Utility must have specific TCP/IP properties defined. This computer must also be connected to an Isolated Access Point with a specific SSID.

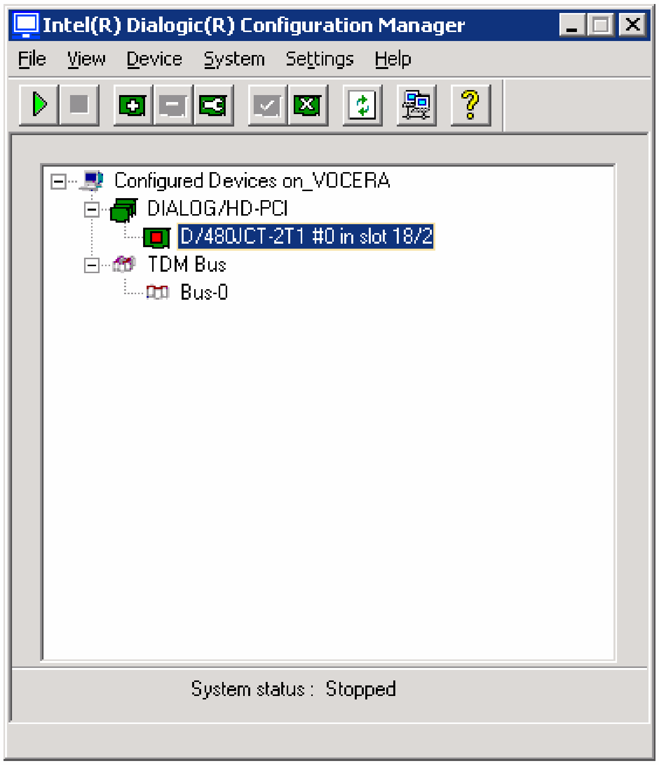
Refer to the *Vocera Configuration Guide* for information on specific TCP/IP and SSID properties required for the Isolated Access Point.

Vocera Telephony Integration

The hardware required to integrate Vocera with a PBX differs according to whether you perform an analog or a digital integration. A digital integration with Cisco Unified Communications Manager is suggested as it provides a higher density of channels than an analog integration. Specific Intel Dialogic boards are supported by Vocera and can be found in the *Vocera Configuration Guide*.

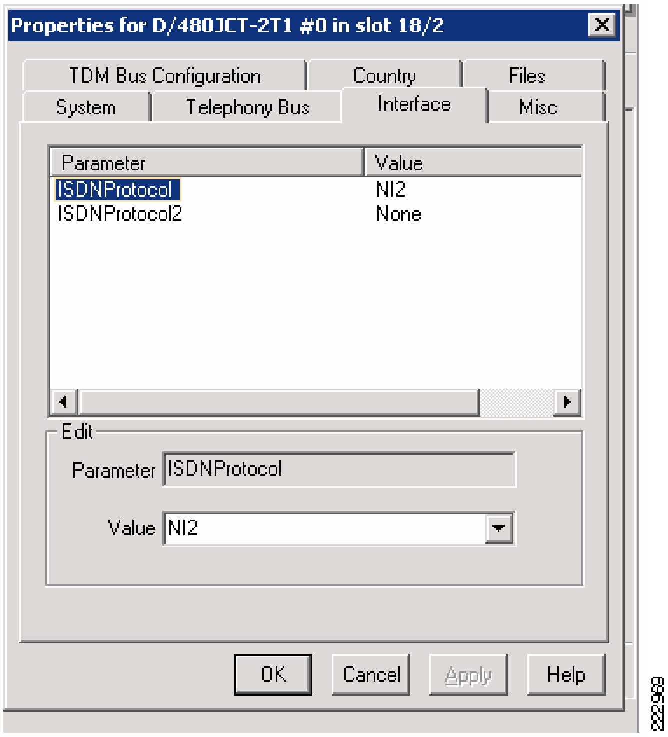
For this design guide the Intel® Dialogic® D/480JCT-2T1 was used with a switch protocol of NI2. Figure 11-7 and Figure 11-8 show the Dialogic settings from the Vocera Intel® Dialogic® Configuration Manager located on the Vocera Server.

Figure 11-7 Vocera Intel® Dialogic® Configuration Manager Screen 1


Intel(R) Dialogic(R) Configuration Manager
File
View
Device
System
Settings
Help
Configured Devices on_VOCERA
DIALOG/HD-PCI
D/480JCT-2T1 #0 in slot 18/2
TDM Bus
Bus-0

System status : Stopped

Figure 11-8 Vocera Intel® Dialogic® Configuration Manager Screen 2



Parameter	Value
ISDNProtocol	NI2
ISDNProtocol2	None

Edit

Parameter ISDNProtocol

Value NI2

DHCP

Vocera does not allow the running of the DHCP server on the Vocera Server computer. Although the DHCP server does not typically require significant system resources, running it on the Vocera Server computer causes significant problems in a clustered environment, including the following:

- Devices may inadvertently receive duplicate IP addresses.
- Badges may not receive an IP address and get stuck displaying *Requesting IP Address*.
- Badges may get invalid and unusable IP address information.

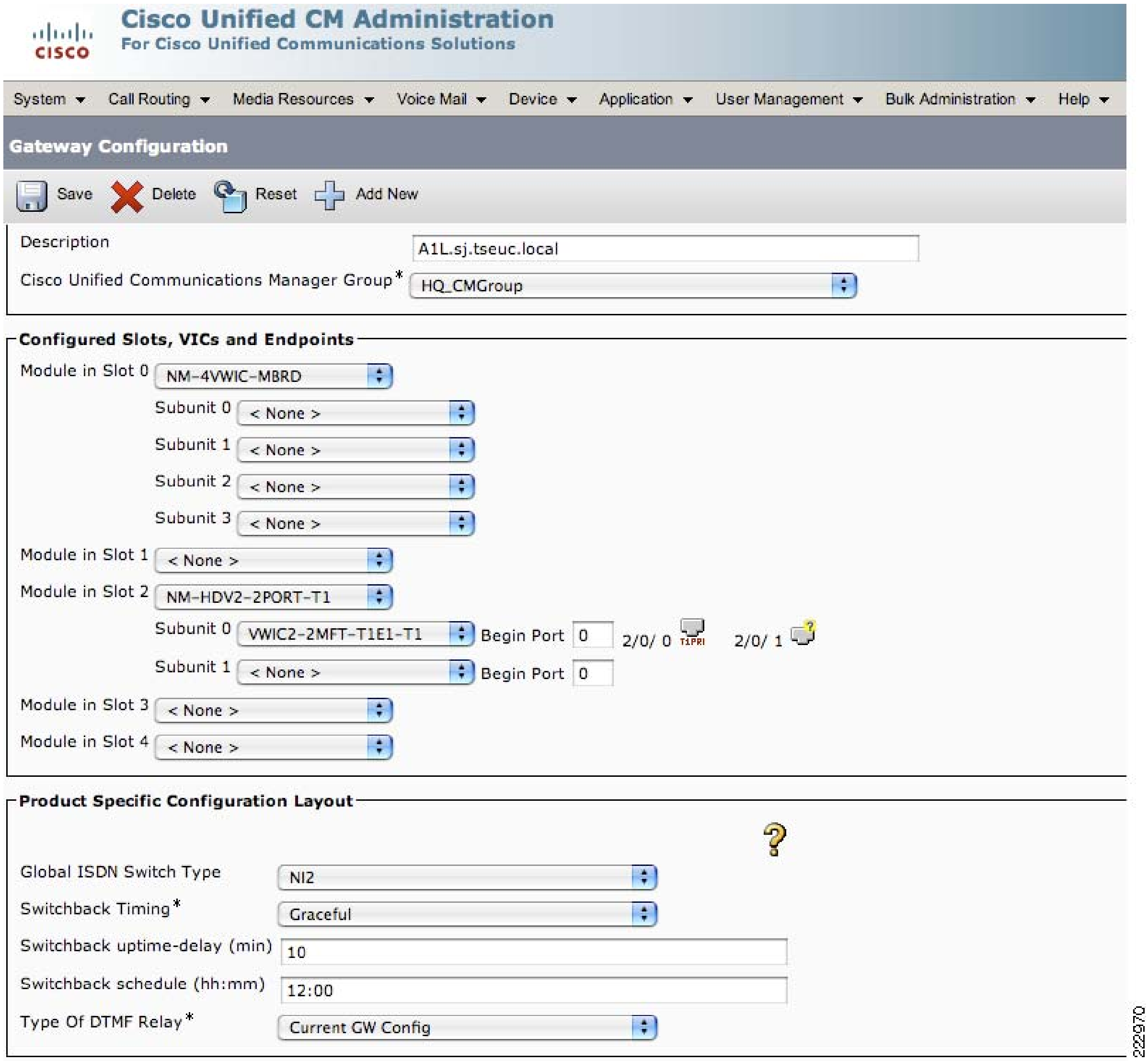
Unlike Cisco IP phones, the DHCP scope does not require option 150 to be set. Option 150 defines the address of the Cisco Unified Communications Manager TFTP Server for Cisco IP phones (Vocera Badges do not communicate directly with Cisco Unified Communications Manager). If DHCP is not used, the Badges will require manual entry of network properties. Since the Badges do not have a keyboard this process is slow and error prone, thus DHCP is highly recommended.

Cisco Unified Communications Manager Configuration

Communication between Cisco Unified Communications Manager and Vocera is accomplished in the same manner as connecting CUCM with a PBX. It is always suggested to use the highest level of integration that both systems can support. For example, if both systems support QSig then this would offer a more robust integration than ISDN or analog integration. In the case of Vocera they only support ISDN or analog integration so ISDN should be used whenever possible.

Figure 11-9 shows the Cisco Unified Manager Communications gateway configuration when using MGCP. The gateway is A1L.sj.tseuc.local with endpoint 2/0/0 (T1PRI) connected to the Vocera Dialogic board.

Figure 11-9 Cisco Unified Communications Manager Gateway Configuration



Gateway Configuration

Description: A1L.sj.tseuc.local

Cisco Unified Communications Manager Group*: HQ_CMGroup

Configured Slots, VICs and Endpoints

Module in Slot 0: NM-4VWIC-MBRD
Subunit 0: < None >
Subunit 1: < None >
Subunit 2: < None >
Subunit 3: < None >

Module in Slot 1: < None >

Module in Slot 2: NM-HDV2-2PORT-T1
Subunit 0: VWIC2-2MFT-T1E1-T1 Begin Port 0 2/0/ 0 2/0/ 1
Subunit 1: < None > Begin Port 0

Module in Slot 3: < None >

Module in Slot 4: < None >

Product Specific Configuration Layout

Global ISDN Switch Type: NI2

Switchback Timing*: Graceful

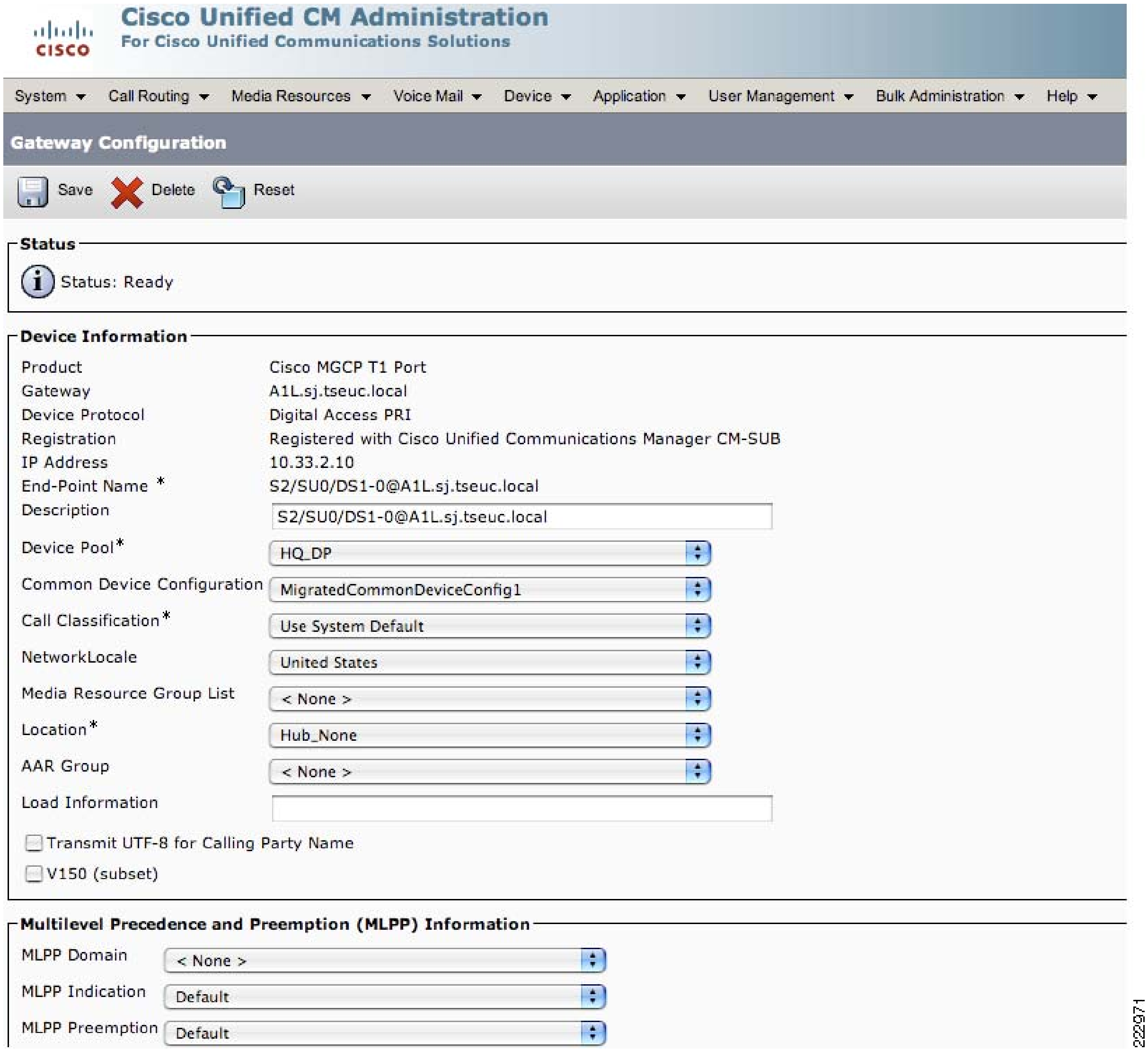
Switchback uptime-delay (min): 10

Switchback schedule (hh:mm): 12:00

Type Of DTMF Relay*: Current GW Config

Figure 11-10 through Figure 11-13 show the endpoint 2/0/0 configuration.

Figure 11-10 Cisco Unified Communications Manager Gateway Configuration (Part 1)



Gateway Configuration

Status

Status: Ready

Device Information

Product	Cisco MGCP T1 Port
Gateway	A1L.sj.tseuc.local
Device Protocol	Digital Access PRI
Registration	Registered with Cisco Unified Communications Manager CM-SUB
IP Address	10.33.2.10
End-Point Name *	S2/SU0/DS1-0@A1L.sj.tseuc.local
Description	S2/SU0/DS1-0@A1L.sj.tseuc.local
Device Pool*	HQ_DP
Common Device Configuration	MigratedCommonDeviceConfig1
Call Classification*	Use System Default
NetworkLocale	United States
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Load Information	

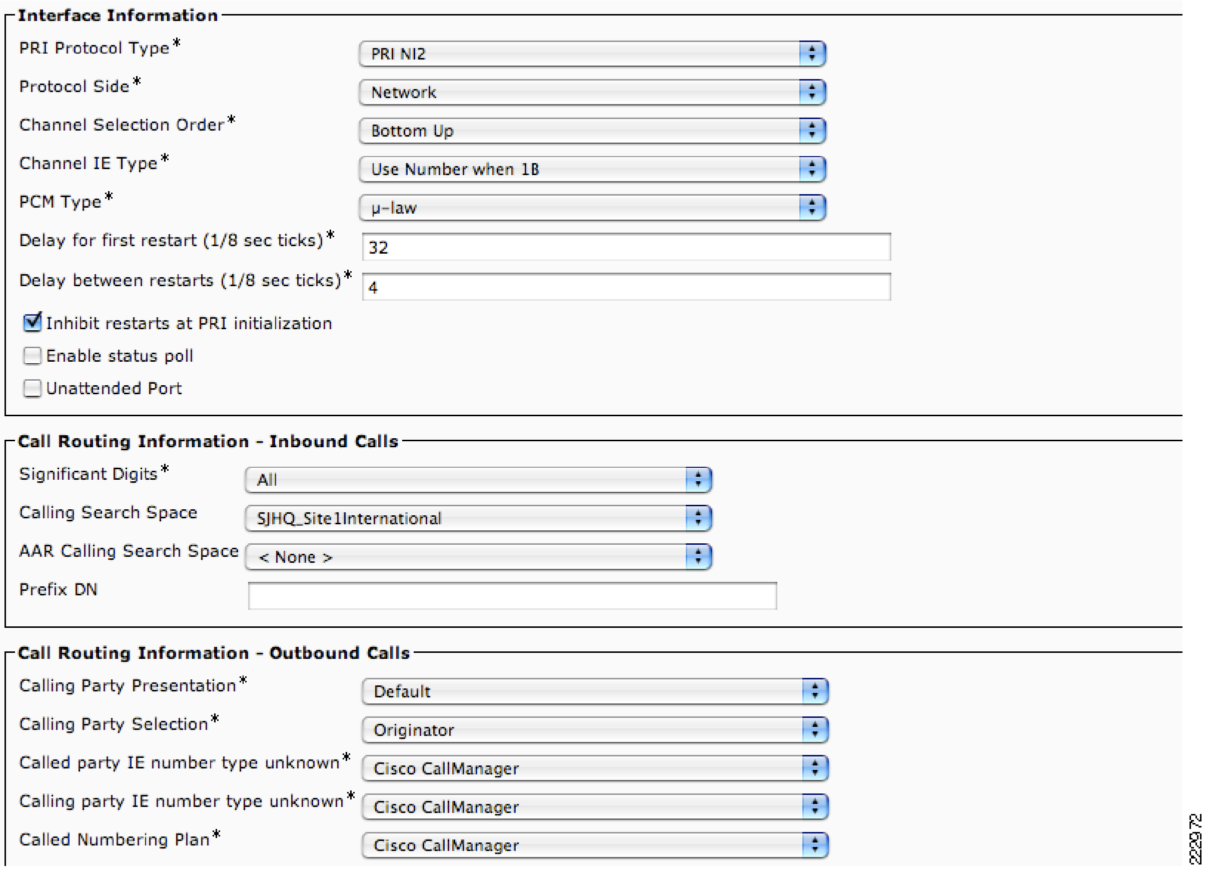
□ Transmit UTF-8 for Calling Party Name

□ V150 (subset)

Multilevel Precedence and Preemption (MLPP) Information

MLPP Domain	< None >
MLPP Indication	Default
MLPP Preemption	Default

Figure 11-11 Cisco Unified Communications Manager Gateway Configuration (Part 2)



Interface Information

PRI Protocol Type*	PRI NI2
Protocol Side*	Network
Channel Selection Order*	Bottom Up
Channel IE Type*	Use Number when 1B
PCM Type*	µ-law
Delay for first restart (1/8 sec ticks)*	32
Delay between restarts (1/8 sec ticks)*	4

☑ Inhibit restarts at PRI initialization
□ Enable status poll
□ Unattended Port

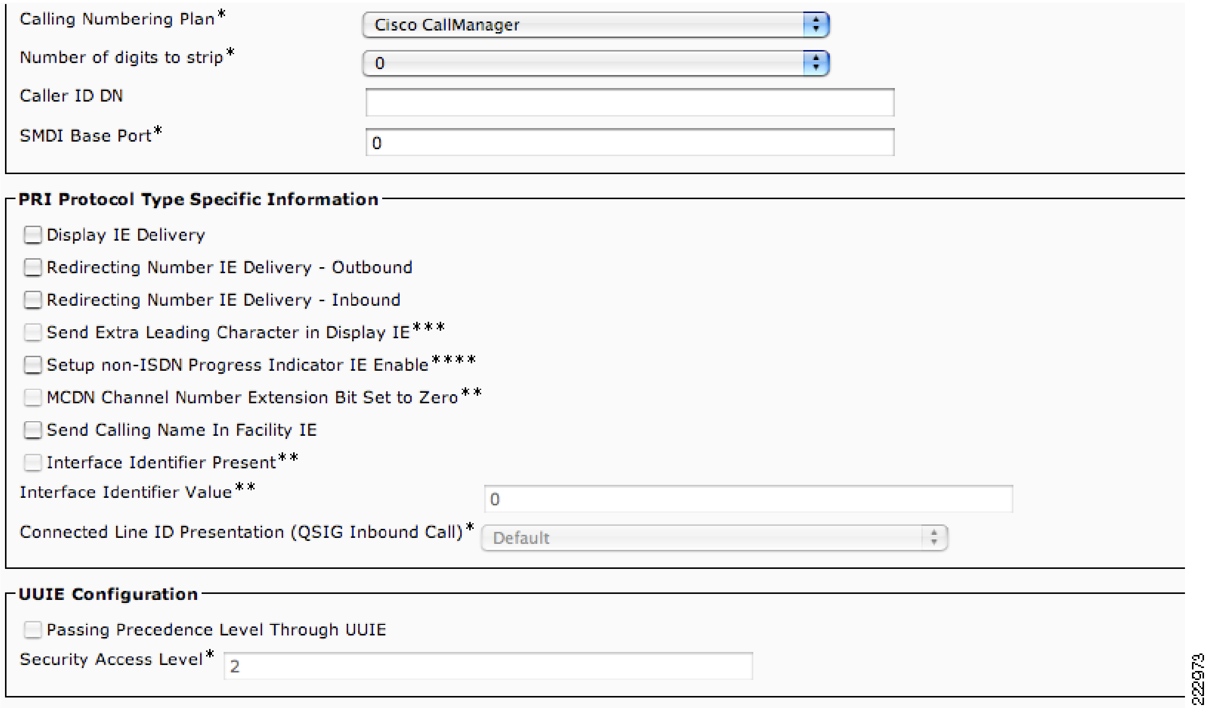
Call Routing Information - Inbound Calls

Significant Digits*	All
Calling Search Space	SJHQ_Site1International
AAR Calling Search Space	< None >
Prefix DN	

Call Routing Information - Outbound Calls

Calling Party Presentation*	Default
Calling Party Selection*	Originator
Called party IE number type unknown*	Cisco CallManager
Calling party IE number type unknown*	Cisco CallManager
Called Numbering Plan*	Cisco CallManager

Figure 11-12 Cisco Unified Communications Manager Gateway Configuration (Part 3)



Calling Numbering Plan* Cisco CallManager
Number of digits to strip* 0
Caller ID DN
SMDI Base Port* 0

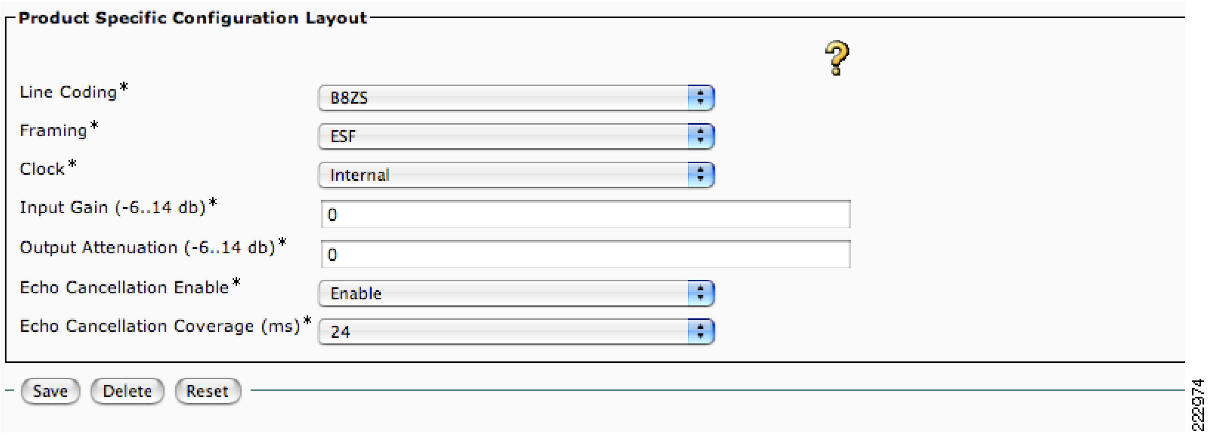
PRI Protocol Type Specific Information

□ Display IE Delivery
□ Redirecting Number IE Delivery - Outbound
□ Redirecting Number IE Delivery - Inbound
□ Send Extra Leading Character in Display IE***
□ Setup non-ISDN Progress Indicator IE Enable****
□ MCDN Channel Number Extension Bit Set to Zero**
□ Send Calling Name In Facility IE
□ Interface Identifier Present**
Interface Identifier Value** 0
Connected Line ID Presentation (QSIG Inbound Call)* Default

UUIE Configuration

□ Passing Precedence Level Through UUIE
Security Access Level* 2

Figure 11-13 Cisco Unified Communications Manager Gateway Configuration (Part 4)



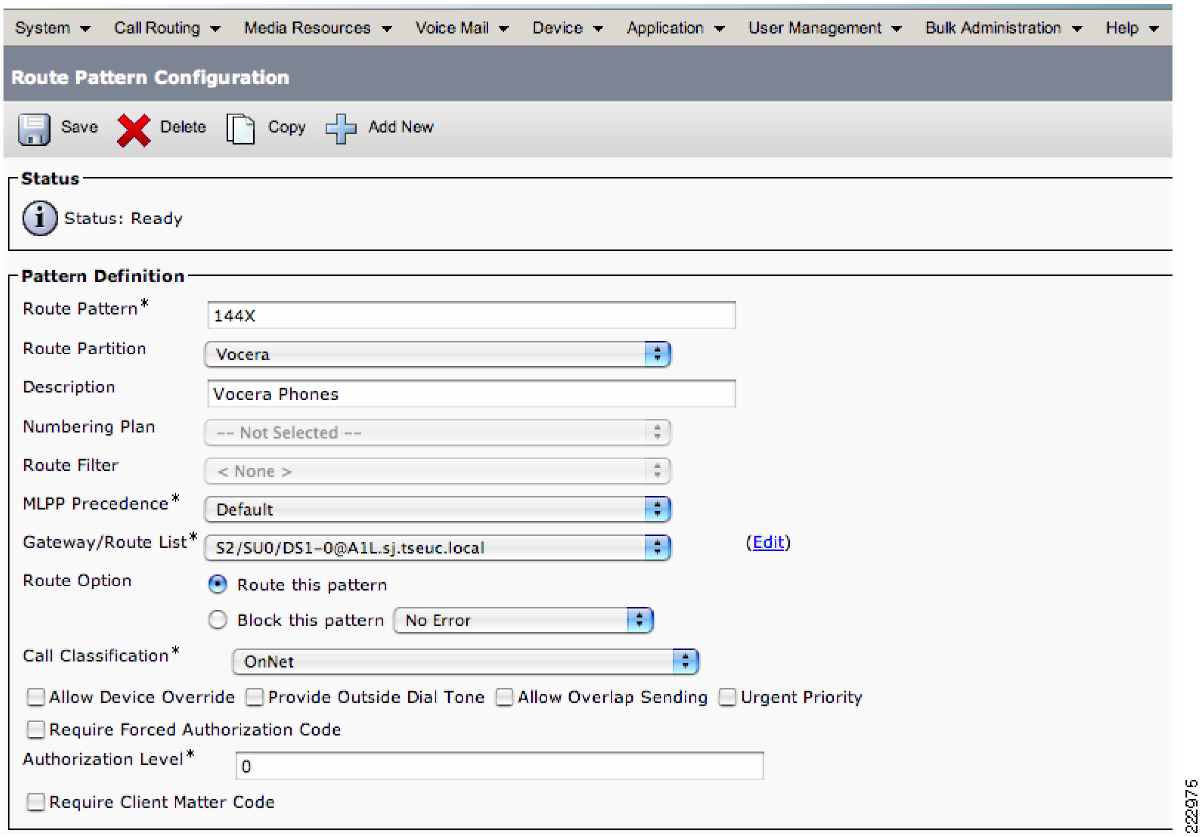
Product Specific Configuration Layout

Line Coding* B8ZS
Framing* ESF
Clock* Internal
Input Gain (-6..14 db)* 0
Output Attenuation (-6..14 db)* 0
Echo Cancellation Enable* Enable
Echo Cancellation Coverage (ms)* 24

Dial Plan and Translation

Vocera Badges are usually deployed for special-purpose areas such as on hospital or retail sales floors. It is suggested that access to the Vocera Badges be restricted by putting the Badges in their own partition that only allows those devices with a need to contact a Vocera Badge the ability to do so. The *Route Pattern Configuration* shown in Figure 11-14 allows all numbers within the range of 1440 to 1449 to be routed to the Vocera Server and assigns the *Vocera* partition.

Figure 11-14 Route Pattern Configuration



Route Pattern Configuration

Status

Status: Ready

Pattern Definition

Route Pattern*	144X
Route Partition	Vocera
Description	Vocera Phones
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
Gateway/Route List*	S2/SU0/DS1-0@A1L.sj.tseuc.local
Route Option	● Route this pattern ○ Block this pattern No Error
Call Classification*	OnNet

□ Allow Device Override □ Provide Outside Dial Tone □ Allow Overlap Sending □ Urgent Priority

□ Require Forced Authorization Code

Authorization Level* 0

□ Require Client Matter Code

Vocera Security

Table 11-1 summarizes the security features supported by Vocera.

Table 11-1 Vocera-supported Security Features

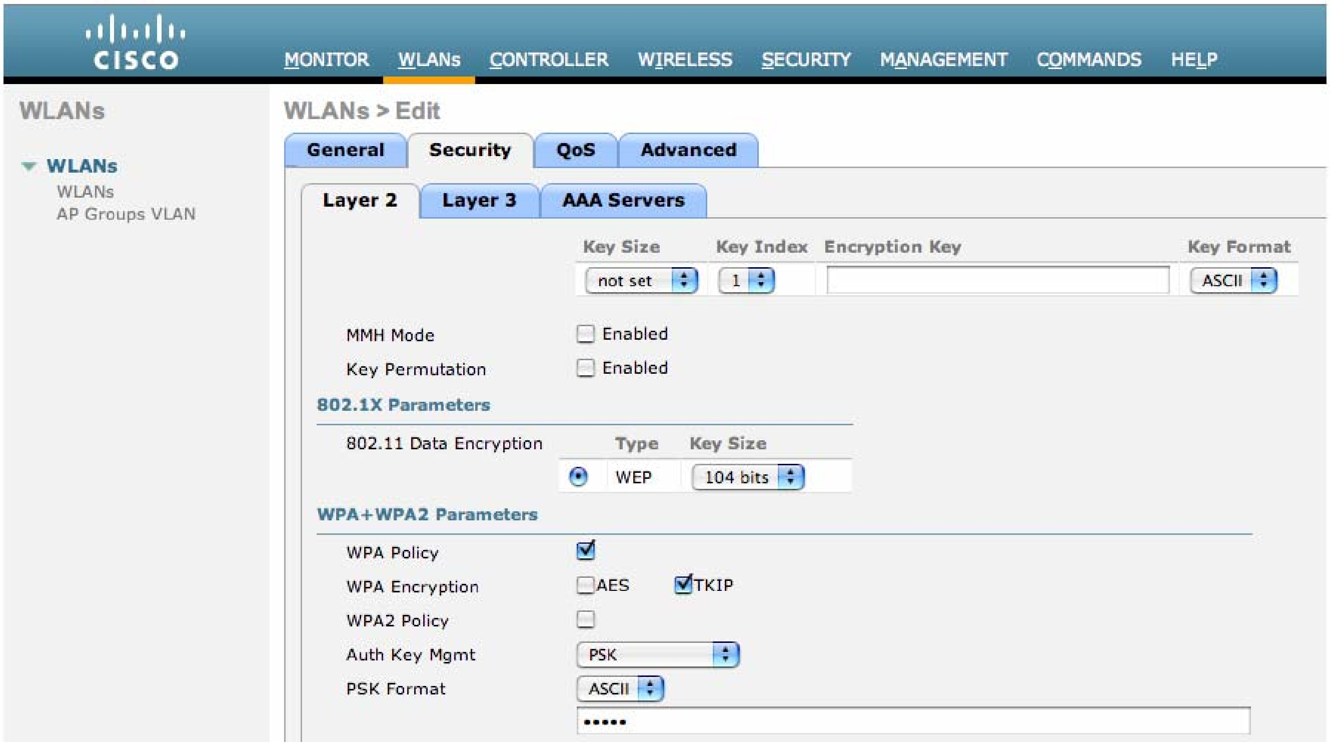
Authentication	Encryption	Message Integrity Check
Open	None, WEP64,WEP128	N/A
LEAP	TKIP-Cisco, WEP64, WEP128	N/A
WPA-PEAP (MS-CHAP v2)	TKIP-WPA	MIC
WPA-PSK	TKIP-WPA	MIC

The LEAP and PEAP protocols typically require each user in a network environment to be authenticated with a unique set of credentials. However, each Badge must have the same security properties so the Vocera Server can automatically update all Badges when necessary. Consequently, Vocera supports device authentication for PEAP and LEAP, not user authentication. All Badges must present the same set of credentials for network authentication.

Applications such as voice running on client devices require fast reassociation when they roam to a different AP to prevent delays and gaps in conversation. Vocera Badges do not support fast, secure roaming so in order to provide fast roaming and a reasonable level of authentication security and encryption, WPA-PSK with TKIP should be used with the Vocera Badge (pre-B2000).

Setting the authentication and encryption is set in the WLC WLAN *Layer 2 Security* tab. Figure 11-15 shows the authentication and encryption setting for the Vocera WLAN.

Figure 11-15 WLAN Security Settings



Key Size	Key Index	Encryption Key	Key Format
not set	1		ASCII

MMH Mode □ Enabled

Key Permutation □ Enabled

802.1X Parameters

802.11 Data Encryption		Type	Key Size
	●	WEP	104 bits

WPA+WPA2 Parameters

WPA Policy ☑

WPA Encryption □ AES ☑ TKIP

WPA2 Policy □

Auth Key Mgmt PSK

PSK Format ASCII

•••••

Vocera Radio Frequency Considerations

Wireless IP telephony networks require careful RF planning. A thorough voice site survey is often required to determine the proper levels of wireless coverage and to identify sources of interference. AP placement and antenna selection choices can be greatly eased with the help of the results of a valid voice site survey. For further information on Vocera RF considerations and configuration please refer to the "Vocera IP Phone Deployment" chapter in *Cisco Unified Wireless Network Infrastructure*.

Vocera QoS

A well-designed and effectively deployed QoS implementation is critical for a successful voice over WLAN deployment. A wireless network that appears to function well for data traffic might provide unsatisfactory performance for a voice deployment. This is because data applications can often tolerate packet delays or recover from packet loss that would be disruptive to a voice call.

Chapter 2, "WLAN Quality of Service," of this document provides general QoS deployment guidance.

Vocera QoS Configuration

VLANs provide a mechanism for segmenting networks into one or more broadcast domains. VLANs are especially important for IP telephony networks, where the typical recommendation is to separate voice and data traffic into different Layer-2 domains. Cisco recommends that you configure separate VLANs for the Vocera Badges from other voice and data traffic. For example, VLANs might consist of the following: a native VLAN for AP management traffic; data VLAN for data traffic; a voice or auxiliary VLAN for voice traffic; and, a VLAN for the Vocera Badges. A separate voice VLAN enables the network to take advantage of Layer-2 marking and provides priority queuing at the Layer-2 access switch port. This ensures that appropriate QoS is provided for various classes of traffic and helps to resolve addressing issues such as IP addressing, security, and network dimensioning. The Vocera Badges use a broadcast feature that utilizes multicast delivery. The use a separate, common voice VLAN ensures that a Badge remains part of the multicast group whenever it roams between controllers. Refer to the “Vocera IP Phone Deployment” chapter in *Cisco Unified Wireless Network Infrastructure*.

Vocera sets the ToS byte in the following ways:

- With a DiffServ Code Point (DSCP) marking of EF (Expedited Forwarding).
- With an IP Precedence marking of 5.

This is not configurable within the Vocera system.

Note The Badge broadcast is sent by the Badge at DSCP EF; when the multicast comes back to the group from the WLC, it is marked best effort. This is a function of the WLC and can have an effect on voice quality.

If your Vocera traffic traverses a WAN circuit, you should make sure the following QoS requirements are met:

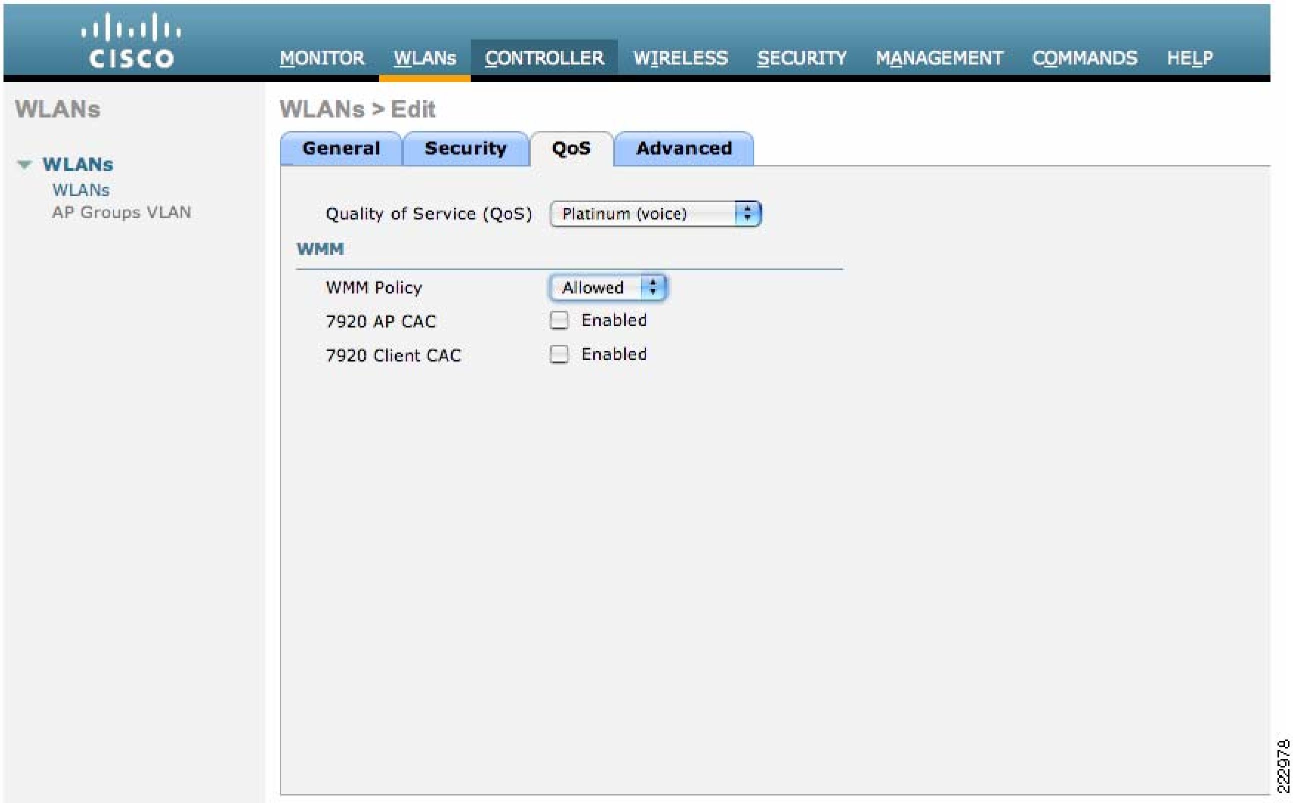
- Enable QoS at all WAN ingress and egress points.
- Make sure routers providing WAN circuits give the highest priority to traffic with a DSCP marking of EF or an IP Precedence of 5.

WLC QoS Configuration

As mentioned in the “Cisco WLC QoS configuration” section on page 10-27, a dedicated voice VLAN should be defined on the controller for all VoIP handsets—that includes Vocera Badges. The voice VLAN should be configured for the highest possible quality of service by editing the VLAN and selecting the QoS tab.

As shown in Figure 11-16, **Platinum (voice)** should be selected on the *Quality of Service (QoS)* drop-down box. Vocera Badges do not support WMM so the WMM Policy drop-down box should be set to **Optional**.

Figure 11-16 WLC QoS Configuration



Quality of Service (QoS): Platinum (voice)

WMM Policy: Allowed

7920 AP CAC □ Enabled

7920 Client CAC □ Enabled

For each of the four QoS Profiles (bronze, silver, gold, platinum) that can be selected for a given WLAN, there is a controller-wide option to change the characteristics of that profile.

In most deployments, these settings should not be changed and the default configuration should be used. More information on these options is available in Chapter 2, "WLAN Quality of Service," of this document.

Infrastructure QoS Configuration

This section shows sample QoS configurations for switch interfaces used in the campus network. More configuration detail for all the switch and routers used in this design guide is available in the Chapter 11, "Voice over WLAN Vocera Implementation."

Table 11-2 summarizes configuration commands for an interface on a Cisco 3750G access-layer switch used to connect an IP phone. The Auto-QoS configuration statement is shown in red and the statements generated by Auto-QoS are shown below it.

Table 11-2 Cisco 3750G —Wired IP Phone Port

Commands	Comments

`interface GigabitEthernet2/0/3`
`description IP phone 7960`
	Interface configuration mode and provide description

`switchport access vlan 50`
`switchport mode access`
	Define access VLAN for data VLAN

Table 11-2 Cisco 3750G —Wired IP Phone Port (continued)

Commands	Comments
`switchport voice vlan 51`	Define Voice VLAN

`switchport port-security maximum 2`
`switchport port-security`
`switchport port-security aging time 2`
`switchport port-security violation restrict`
`switchport port-security aging type inactivity`
	Define Port Security features

`spanning-tree portfast`	Spanning tree port configuration
`auto qos voip cisco-phone`	Auto-QoS statement entered on all voice ports

`srr-queue bandwidth share 10 10 60 20`
`srr-queue bandwidth shape 10 0 0 0`
`queue-set 2`
`mls qos trust device cisco-phone`
`mls qos trust cos`
	Platform-specific QoS statements generated by the Auto-QoS statement that is in red in the line above.

Table 11-3 summarizes configuration commands for an interface on a Cisco 4503 access-layer switch used to connect an AP. The Auto-QoS configuration statement is shown in red and the statements generated by Auto-QoS are shown below it.

Table 11-3 Cisco 4503—Access Point Port

Command	Comments
`interface FastEthernet2/16` (description ports connected to APs in Isolation Boxes)	Interface configuration mode and provide description.

`switchport access vlan 48`
`switchport mode access`
	Define access VLAN for data VLAN all APs go on the access VLAN

`auto qos voip trust`	Auto-QoS statement entered on all AP ports
`qos trust dscp` (**mls qos trust dscp** is the equivalent command format for a Cisco 3750 switch.)	The Auto-QoS statement above sets the switch port to trust Layer-2 CoS (For nonrouted ports, the CoS value of the incoming packet is trusted. For routed ports, the DSCP value of the incoming packet is trusted). This **qos trust dscp** command overrides that and sets the port to trust Layer-3 DSCP instead. The link between the AP and the switch port is not trunked and does not mark L2 CoS

`tx-queue 3`
`bandwidth percent 33`
`priority high`
`shape percent 33`
`service-policy output autoqos-voip-policy`
	Platform-specific QoS statements generated by the Auto-QoS statement that is in red in the line above.

Table 11-4 summarizes configuration commands for an interface on a Cisco 4503 access-layer switch used as an uplink port to a distribution-layer switch. The Auto-QoS configuration statement is shown in red and the statements generated by Auto-QoS are shown below it.

Table 11-4 Cisco 4503 Uplink Port to Distribution Layer

Command	Comments
`interface TenGigabitEthernet1/1`	Interface configuration mode and provide description

`description A4L to D3L`
`no switchport`
`ip address 10.33.3.10 255.255.255.252`
`ip hello-interval eigrp 100 1`
`ip hold-time eigrp 100 3`
`ip authentication mode eigrp 100 md5`
`ip authentication key-chain eigrp 100 eigrp-chain`
`ip pim sparse-mode`
`logging event link-status`
`load-interval 30`
`carrier-delay msec 0`
	Interface configuration unrelated to QoS

`auto qos voip trust`	**Note**—Because this is a Layer-3 port, the **auto qos voip trust** command sets **qos trust dscp** not **qos trust cos** as it did in Table 11-3.
`qos trust dscp`	Platform-specific QoS statements generated by the Auto-QoS statement that is in red in the line above
`tx-queue 3`	

`bandwidth percent 33`
`priority high`
`shape percent 33`
`service-policy output autoqos-voip-policy`	

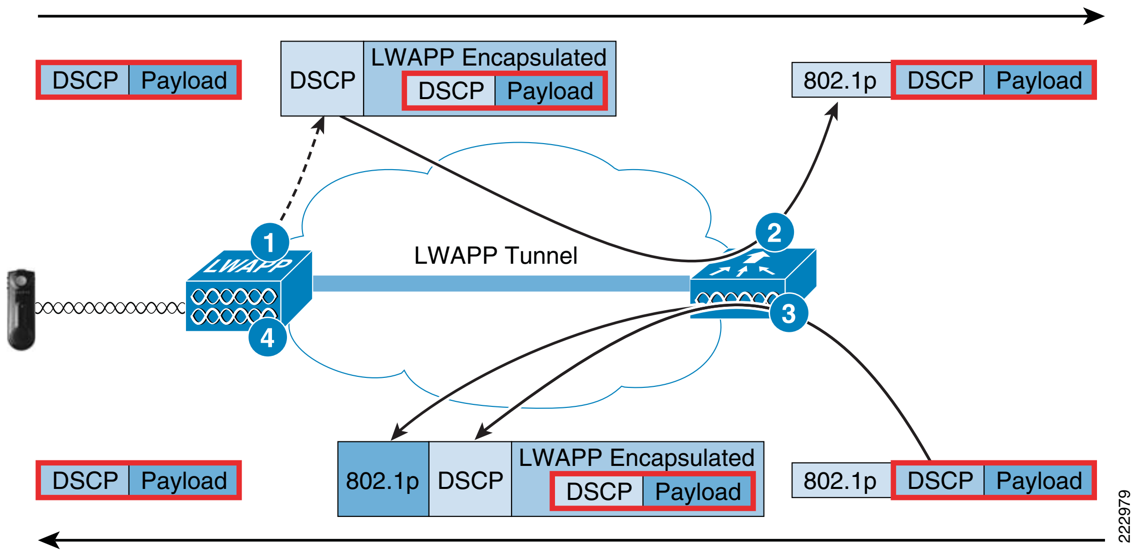
Note Nothing relevant to this topic is configurable within the Vocera devices/products.

End-to-end QoS Mapping

In the centralized WLAN architecture, WLAN data is tunneled between the AP and the WLAN controller via LWAPP. In order to maintain the original QoS classification across this tunnel, the QoS settings of the encapsulated data packet must be appropriately mapped to the Layer-2 (IEEE 802.1p) and Layer-3 (IP DSCP) fields of the outer tunnel packet. See Figure 11-17.

Figure 11-17 and Table 11-5 reference the original Vocera Badge tested for this document. The original Badge does not support WMM for over-the-air QoS, but Vocera has announced a new Badge (the B2000) which will support WMM QoS.

Figure 11-17 End-to-end QoS Packet Marking Mappings



The original IP packet DSCP and user-data sent by the WLAN client to the AP or received by the controller from the wired network infrastructure are transmitted across the LWAPP tunnel between the AP and the controller unaltered; the Layer-2 and Layer-3 QoS markings are only changed on the headers that encapsulate the original IP packet.

Table 11-5 End-to-end QoS Packet Marking Mappings

Mapping Number[1]	From	To	Outbound UP (IEEE 802.1p/IEEE 802.11e) mapping	Outbound IP DSCP mapping
1	Access Point	Controller	N/A (APs do not support IEEE 802.1Q / IEEE 802.1p tags on the wired interface)	**WMM Client:** Police the IEEE 802.11e UP value to ensure it does not exceed the maximum value allowed for the QoS policy assigned to that client; translate the value to the DSCP value. **Regular Client (Vocera Badge):** Use the IEEE 802.11e UP value for the QoS policy assigned to that clients WLAN; translate the value to the DSCP value.
2	Controller	Ethernet Switch	Translate the DSCP value of the incoming LWAPP packet to the IEEE 802.1p UP value. **Note**—The AP has policed the upstream DSCP (when it mapped from IEEE 802.1p UP to DSCP)	N/A (The original/encapsulated DSCP value is preserved) **Note**—The DSCP is un-policed; it is whatever was set by the WLAN client.

Table 11-5 End-to-end QoS Packet Marking Mappings

Mapping Number[1]	From	To	Outbound UP (IEEE 802.1p/IEEE 802.11e) mapping	Outbound IP DSCP mapping
3	Controller	Access Point	Translate the DSCP value of the incoming packet to the AVVID IEEE 802.1p UP value. **Note**—The QoS profile is used to police the maximum IEEE 802.1p value that can be set	Copy the DSCP value from the incoming packet. **Note**—No policing is performed here; it is assumed that traffic was policed at ingress to the network
4	Access Point	Wireless Client	**WMM Client:** Translate the DSCP value of the incoming LWAPP packet to the IEEE 802.11e UP value. Police the value to ensure it does not exceed the maximum value allowed for the WLAN QoS policy assigned to the WLAN the client belongs to. Place packet in the IEEE 802.11 Tx queue appropriate for the UP value. **Regular client (Vocera Badge):** Place packet in the default IEEE 802.11 Tx queue for the WLAN QoS policy assigned to that client.	N/A (original/encapsulated DSCP value is preserved)

[1] Refers to Figure 11-17.

APPENDIX A

Deploying and Operating a Secure Voice over Wireless LAN Solution with Cisco Lifecycle Services

To gain full advantage of converged mobile applications requires blending wired and wireless systems within an infrastructure that is continuously reliable, highly available, and scalable. Wireless network users expect the same level of secure connectivity, reliability, and performance for Voice over Wireless LAN applications as they experience with a wired environment.

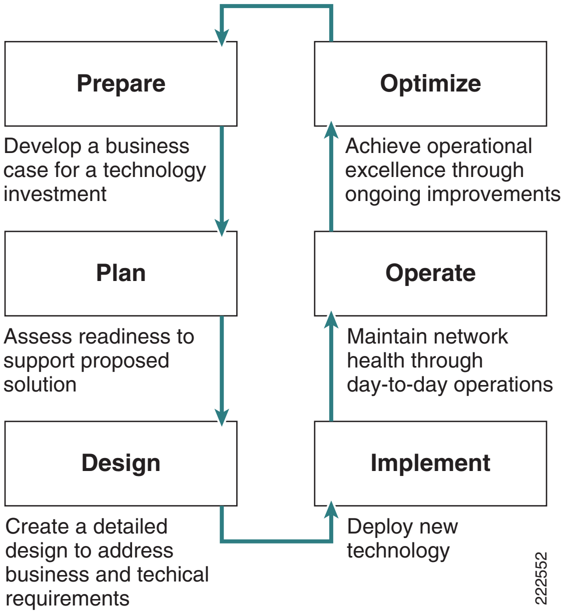
Companies aim to design, build, and operate a voice system that is secure, yet highly available to designated users, and that offers the lowest possible total cost of ownership.

The Cisco Lifecycle Services Approach

The Cisco Lifecycle Services approach defines the minimum set of activities needed, by technology and by network complexity, to help you successfully deploy and operate Cisco Wireless LAN solutions and optimize their performance throughout the lifecycle of your network.

Figure A-1 illustrates the general Cisco Lifecycle Services methodology.

Figure A-1 Lifecycle Services Methodology


Prepare
Develop a business case for a technology investment
Plan
Assess readiness to support proposed solution
Design
Create a detailed design to address business and techical requirements
Implement
Deploy new technology
Operate
Maintain network health through day-to-day operations
Optimize
Achieve operational excellence through ongoing improvements
222552

This approach is based on proven methodologies for planning, designing, implementing, operating, and optimizing the performance of a variety of secure voice and data wireless network solutions and technologies. It creates a framework for defining services that is independent of who performs the service activities—Cisco, partners, or customers themselves—enabling multiple parties to provide the support needed in a coordinated manner. Table A-1 summarizes the lifecycle methodology components summarized in the sections that follow. Each listed recommended activity links to a brief description.

Note Cisco and our Wireless LAN Specialized Partners offer a broad portfolio of end-to-end services based on proven methodologies for deploying and operating a variety of secure voice and data wireless network solutions and technologies. For more information, please see http://www.cisco.com/en/US/products/ps8306/serv_home.html.

Table A-1 Lifecycle Methodology for Cisco Voice over Wireless LAN Solutions

General Tasks	Specific Recommended Activity
Prepare	Wireless LAN Business Requirements Development Wireless LAN Technical Requirements Development Wireless LAN Operations Technology Strategy Development Wireless LAN High Level Design Development
Plan	Wireless LAN Deployment Project Management Architecture Review and Assessment Wireless LAN Operations Readiness Assessment IP Communications over Wireless LAN Assessment Wireless Security Posture Assessment

Table A-1 Lifecycle Methodology for Cisco Voice over Wireless LAN Solutions (continued)

General Tasks	Specific Recommended Activity
Design	Wireless LAN Staff Plan Development Wireless Security Design Development Wireless LAN Detailed Design Development Wireless LAN Detailed Design Validation Wireless LAN Operations Design Development Wireless LAN Staging Plan Development Wireless LAN Implementation Plan Development Wireless LAN Operations Implementation Plan Development Wireless LAN Acceptance Test Plan Development Wireless LAN Migration Plan Development Wireless LAN Site Readiness Assessment (RF Site Survey) Security Implementation Plan Development
Implement	Cisco Security Agent Implementation Security Implementation Engineering Security Network Admission Control Implementation Wireless LAN Staging Wireless Control System Implementation Wireless LAN Controller Implementation Wireless LAN Operations Implementation Wireless LAN Migration Staff Training Wireless LAN Acceptance Test and Network Deployment Verification Audit
Operate	Wireless LAN Systems Monitoring Wireless LAN Incident Management Wireless LAN Problem Management Wireless LAN Change Management Wireless LAN Configuration Management Wireless LAN Supplier Management Wireless LAN Security Administration
Optimize	Wireless LAN Business Requirements Alignment Wireless LAN Technology Assessment Wireless LAN Operations Assessment Wireless Security Assessment

Lifecycle Services Methodology—Prepare Phase

In the *prepare* phase, a company determines a business case and financial rationale to support wireless LAN solution adoption. By carefully anticipating future needs and developing both a technology strategy and a high-level architecture to meet those needs, your business is better equipped to contain costs during deployment and operations.

Cisco recommends the following activities to support successful deployment:

- Wireless LAN Business Requirements Development
- Wireless LAN Technical Requirements Development
- Wireless LAN Operations Technology Strategy Development
- Wireless LAN High Level Design Development

These activities are described briefly in the sections that follow.

Wireless LAN Business Requirements Development

Assess and document the business requirements for end-user voice over wireless LAN service delivery that support the technology investment.

Why: Make sound financial decisions by developing a business case that establishes the financial justification for making a technology change.

Wireless LAN Technical Requirements Development

Analyze your business and voice over wireless LAN service requirements and identify the Cisco advanced technologies that support them. Document a technology strategy.

Why: Improve efficiency throughout the solution lifecycle by aligning your technology strategy to your business goals.

Wireless LAN Operations Technology Strategy Development

Create an operational strategy that defines the people, processes, and tools required to support the operations and management of the technology solution.

Why: Achieve business goals by aligning your operations strategy with your business and technical voice over wireless LAN requirements.

Wireless LAN High Level Design Development

Create a high-level conceptual architecture of your proposed voice over wireless LAN solution that addresses business and technical requirements and creates the foundation for wireless LAN solution deployment. Include specifications for availability, capacity, and security to meet service requirements.

Why: Reduce rework during the design phase by identifying and validating required technologies and features early in the wireless LAN solution lifecycle.

Lifecycle Services Methodology—Plan Phase

Successful wireless LAN deployment depends on an accurate assessment of your company's network, security state, and overall readiness to support the proposed solution. In the *plan* phase, a company ascertains whether it has adequate resources to manage a technology deployment project to completion. To evaluate and improve network security, a company tests for vulnerability to intruders and outside networks.

Cisco recommends the following activities to support successful deployment:

- Wireless LAN Deployment Project Management
- Architecture Review and Assessment
- Wireless LAN Operations Readiness Assessment
- IP Communications over Wireless LAN Assessment
- Wireless Security Posture Assessment
- Wireless Security Design Review

These activities are described briefly in the sections that follow.

Wireless LAN Deployment Project Management

Provide for one or more project managers or program managers to manage the planning, design, and implementation of your deployment project. Develop and implement a project management plan, manage information and resources, and control change.

Why: Reduce risks and resolve problems quickly by using proven project management methodologies and risk mitigation strategies.

Architecture Review and Assessment

Prepare for your technology solution deployment by assessing the readiness of your existing system infrastructure to support a new technology. Analyze the physical and logical configuration of the network, systems availability, systems capacity, quality of service, systems resiliency, security, and integration with existing platforms. Identify network and application modifications that should be made prior to implementation. Prepare for your technology solution deployment with a comprehensive site assessment that evaluates the readiness of your current facilities infrastructure to support the new technology. Identify any physical, environmental, and electrical modifications that should be made prior to implementation.

Why: Reduce deployment costs by analyzing gaps early in the planning process to determine what is needed to support the solution and to improve productivity by identifying and resolving gaps in service-level requirements associated with availability, capacity, and security specifications.

Wireless LAN Operations Readiness Assessment

Prepare for your wireless LAN solution deployment with a comprehensive operations assessment that evaluates the readiness of your current operations and network management infrastructure to support the new technology. Identify any changes to people, processes, and tools that should be made prior to implementation.

Why: Effectively plan and budget for your wireless LAN technology expenditures by gauging your operational preparedness and ability to support current and planned applications and services. Reduce network operations costs by identifying the operational changes required to support the operation and management of the technology solution.

IP Communications over Wireless LAN Assessment

Understand the readiness of the existing wireless LAN to support their proposed IP communications applications, and how migrating the proposed IP communications application may affect the existing wireless LAN / Wired LAN. Assess the readiness of your existing wireless LAN to support your proposed IP communications applications. Appraise the potential effects of migration on the interoperability between the proposed IP communications application and your existing wireless LAN and wired LAN. Review building blueprints and coverage requirements, potential interference sources, noise floor, signal strength, and more.

Why: Avoid costly and disruptive design changes during the implementation phase through early planning of design changes to accommodate IP communications over wireless LAN.

Wireless Security Posture Assessment

Protect your network from inside and outside intruders by assessing system, application, and network device vulnerabilities. Safely simulate activities typical of attacks on your network, without affecting your network. Recommend changes that should be made to the network to help prevent security breaches and reduce risk of attack.

Why: Mitigate network security threats by limiting their ability to do damage. Improve the overall security state of the corporate *trusted* network and the systems and information within it by identifying changes to address vulnerabilities.

Lifecycle Services Methodology—Design Phase

Developing a detailed design is essential to reducing risk, delays, and the total cost of your wireless LAN deployment. A design aligned with business goals and technical requirements can improve network performance while supporting high availability, reliability, security, and scalability. Day-to-day operations and network management processes need to be anticipated, and, when necessary, custom applications are created to integrate new systems into existing infrastructure. The *design* phase can also guide and accelerate successful implementation with plans to stage, configure, test, and validate network operations.

Cisco recommends the following activities:

- Wireless LAN Staff Plan Development
- Wireless Security Design Development
- Wireless LAN Detailed Design Development
- Wireless LAN Detailed Design Validation
- Wireless LAN Operations Design Development
- Wireless LAN Staging Plan Development
- Wireless LAN Implementation Plan Development
- Wireless LAN Operations Implementation Plan Development
- Wireless LAN Acceptance Test Plan Development
- Wireless LAN Migration Plan Development
- Wireless LAN Site Readiness Assessment (RF Site Survey)
- Security Implementation Plan Development

These activities are described briefly in the sections that follow.

Wireless LAN Staff Plan Development

Prepare your staff for wireless LAN solution deployment by using conventional instructional design methodologies to create a staff plan. Determine the technical activities and tasks required to support the voice over wireless solution, measure the ability of functional groups to perform those tasks, and develop a curriculum plan to address skill and knowledge gaps.

Why: Reduce ongoing operating costs by identifying proficiency issues that could affect staff productivity and performance.

Wireless Security Design Development

Develop an in-depth, implementation-ready detailed design for your wireless LAN security solution. Take into consideration your defined business requirements and the associated performance, availability, resiliency, maintainability, resource-capacity, and security criteria used to measure and confirm the delivery of the required services.

Why: Implement advanced security and intrusion detection devices and strategies effectively to keep data private and secure and lower your total cost of ownership.

Wireless LAN Detailed Design Development

Develop an in-depth, implementation-ready detailed design for your wireless LAN solution. Derive the design from availability, capacity, reliability, security, scalability, and performance specifications that align with your business and technical voice over wireless requirements.

Why: Reduce expensive, time-consuming network redesign by creating a well-engineered design early in the network lifecycle.

Wireless LAN Detailed Design Validation

Validate that your detailed design meets your business and technical voice over wireless requirements with an in-depth, detailed test plan and support for test implementation. Include testing of features, functionality, compatibility, and software applications.

Why: Accelerate wireless LAN solution adoption by validating that your design meets end-user service delivery goals.

Wireless LAN Operations Design Development

Prepare your current operations and network management infrastructure to support the new technology with a detailed design of the operations and network management processes and tools for your wireless LAN solution.

Why: Speed migration of the new voice over wireless LAN solution by improving operations preparedness.

Wireless LAN Staging Plan Development

Develop a step-by-step plan for staging the configuration, implementation, and connectivity testing of the voice over wireless LAN solution in a controlled environment that emulates, but does not affect, your production network.

Why: Reduce delays and other problems during staging with a detailed plan that addresses staging requirements including physical, electrical, and environmental conditions on the site; network hardware and software; and third-party devices.

Wireless LAN Implementation Plan Development

Develop a detailed, site-specific plan for implementing your voice over wireless LAN solution. Define the activities, configurations, and commissioning test plans required to deploy and commission the technology.

Why: Reduce delays, rework, and other problems during implementation by creating a detailed implementation plan and by accurately estimating the time and resources required to implement the new system or solution.

Wireless LAN Operations Implementation Plan Development

Develop an operations implementation plan detailing the tasks needed to deploy and commission the operations and network management system for your voice over wireless LAN solution to be deployed. Include scheduling of priorities, resources, and responsibilities.

Why: Reduce delays, disruption, and other problems by accurately estimating the time and resources required to implement new operations and network management systems.

Wireless LAN Acceptance Test Plan Development

Develop a test plan that can be used to demonstrate that the voice over wireless LAN solution to be deployed meets operational, functional, and interface requirements at implementation.

Wireless LAN Migration Plan Development

Develop a step-by-step plan for migrating your existing wireless network and associated mobility services to the proposed secure wireless LAN solution.

Why: Improve the speed and efficiency of the migration by developing a plan that covers the steps necessary to migrate from the existing state to a future state while continuing to minimize the risk and disruption to critical production systems and applications.

Wireless LAN Site Readiness Assessment (RF Site Survey)

Gauge the ability of your environment to allow secure wireless LAN access in the desired coverage area. Assess your current state and future needs so you can make informed decisions about how to build your wireless network architecture.

Why: Obtain the best performance out of your voice over wireless LAN solution by placing access points in optimal locations and reduce the interference caused by other radio emitters to a minimum.

Security Implementation Plan Development

Develop a step-by-step staging plan detailing the Cisco Security Agent installation and service-commission requirement tasks to be staged in a controlled implementation environment that emulates your network.

Why: Reduce delays and other problems during staging with a detailed plan that addresses staging requirements including physical, electrical, and environmental conditions on the site; network hardware and software; and third-party devices.

Lifecycle Services Methodology—Implement Phase

A network is essential to any successful organization, and it must deliver vital services without disruption. In the *implement* phase, a company works to integrate devices and new capabilities in accordance with the design-without compromising network availability or performance. After identifying and resolving potential problems, the company can speed return on investment with an efficient migration and successful implementation.

Cisco recommends the following activities to support successful deployment:

- Cisco Security Agent Implementation
- Security Implementation Engineering
- Security Network Admission Control Implementation
- Wireless LAN Staging
- Wireless Control System Implementation
- Wireless LAN Controller Implementation
- Wireless LAN Operations Implementation
- Wireless LAN Migration
- Staff Training
- Acceptance Test and Network Deployment Verification Audit

These activities are described briefly in the sections that follow.

Cisco Security Agent Implementation

Install, configure, and integrate Cisco Security Agent solution components in a production environment.

Why: Successfully deploy the new technology solution by following an in-depth, detailed implementation process based on leading practices.

Security Implementation Engineering

Develop security design specifications in accordance with your security policies detailing the security design topology, feature configuration, and policy implementation contains the detailed security design of the systems, including network diagrams and sample software configurations for protocols, policies, and features taking you through the initial development process, testing processes, deployment phases as well as integration, management, and the optimization processes.

Why: More effectively mitigate network security threats by using a sound implementation methodology to deploy a new security solution that will reduce your operating costs and total cost of ownership by helping to ensure consistent deployment of security policies.

Security Network Admission Control Implementation

Install, configure, and integrate Network Admission Control components as specified in your implementation plan. Complete predefined test cases.

Why: Successfully deploy the Network Admission Control components by following an in-depth, detailed implementation process based on leading practices.

Wireless LAN Staging

Stage and test your voice over wireless LAN solution in a controlled environment that does not affect your live network, as outlined in your predefined staging plan.

Why: Staging can help you to improve efficiency and reduce costly delays and rework during implementation by identifying and resolving issues.

Wireless Control System Implementation

Install/upgrade WCS and then configure the WCS software to support for the customer wireless requirements. Wireless LAN controllers will be configured in WCS along with policy provisioning, network optimization, security monitoring, and customized fault settings

Why: Realize the business and technical goals of your new system in accordance with recommendations made in the earlier phases of the lifecycle to monitor and configure the entire wireless LAN solution from a centralized appliance.

Wireless LAN Controller Implementation

Install and configure the wireless LAN controller and access points to be assigned to the required Controller according to the wireless LAN detailed design. Configure the security policy including IEEE 802.1X (or VPN) authentication to the RADIUS server and backend database will be configured along with mobility management including L2/L3 roaming (if required), RF network optimization, including RF interference detection, TX power and channel optimization, security monitoring, including rogue AP detection/containment, and intrusion detection, QOS settings, load balancing, policy provisioning, and customize fault settings.

Why: Successfully deploy the new voice over wireless LAN solution by following an in-depth, detailed implementation process based on leading practices.

Wireless LAN Operations Implementation

Install, configure, test, and commission the wireless LAN operations and network management system you are deploying in accordance with your operations implementation plan.

Why: Reduce network operating expenses by improving the efficiency of operations processes and tools.

Wireless LAN Migration

Migrate your existing network services for the solution you are deploying as specified in your migration plan. Include equipment, interfaces, applications, services, and hardware platforms.

Why: Reduce risks such as downtime, delays, and the need for rework by following a thorough, detailed implementation process based on leading practices.

Staff Training

Manage and implement the staff development plan for your deployment or operations teams. Includes scheduling classes, creating the enrollment process, providing course materials, and managing training vendors. Can include delivery of workshops or instructor-led training classes with hands-on lab exercises, e-learning, mentoring, materials for self-paced study, and leading-practice documentation.

Why: Increase overall productivity and reduce ongoing wireless LAN solution operating costs through training designed to close the skill gaps that were identified in developing your staff plan.

Wireless LAN Acceptance Test and Network Deployment Verification Audit

Perform systems-level acceptance testing by performing a survey of the RF environment for coverage, interference, and general performance of your wireless LAN solution to objectively measure operability and functionality of the system you are deploying to verify that it meets your business and technical requirements and is ready for production.

Why: Systems acceptance testing help you speed the migration process; accelerate return on investment; and reduce unnecessary risk, including disruption, delays, rework, and other problems.

Lifecycle Services Methodology—Operate Phase

Network operations represent a significant portion of IT budgets, so it's important to be able to reduce operating expenses while continually enhancing performance. Throughout the *operate* phase, a company proactively monitors the health and vital signs of the network to improve service quality; reduce disruptions; mitigate outages; and maintain high availability, reliability, and security. By providing an efficient framework and operational tools to respond to problems, a company can avoid costly downtime and business interruption. Expert operations also allow an organization to accommodate upgrades, moves, additions, and changes while effectively reducing operating costs.

Cisco recommends implementing the following processes to support successful operations:

- Wireless LAN Systems Monitoring
- Wireless LAN Incident Management
- Wireless LAN Problem Management
- Wireless LAN Change Management
- Wireless LAN Configuration Management
- Wireless LAN Supplier Management
- Wireless LAN Security Administration

These activities are described briefly in the sections that follow.

Wireless LAN Systems Monitoring

Monitor, manage, and report on service-level metrics and abnormal events or trends that might adversely affect the availability, capacity, performance, and security of your wireless LAN solution.

Why: Improve service quality and reduce disruptions and outages by proactively monitoring system health.

Wireless LAN Incident Management

Manage and resolve real-time incidents with wireless LAN solution components using an incident management process that creates and maintains a report of the status of an incident from isolation to closure.

Why: Restore normal service operation quickly by providing an in-depth incident management process that includes case management, investigation, and diagnosis; hardware and software replacement or updates; and service restoration, testing, and verification.

Wireless LAN Problem Management

Manage and resolve recurring incidents using an in-depth problem management process that analyzes incident trends to identify patterns and systemic conditions.

Why: Reduce the risk of downtime and increase network and/or application availability, reliability, and stability by analyzing the root cause of recurring wireless LAN incidents and rectifying underlying problems through hardware and software support.

Wireless LAN Change Management

Standardize methods and procedures for authorizing, documenting, and performing wireless LAN solution changes.

Why: Reduce operating costs and limit change-related incidents by providing a consistent and efficient change management process.

Wireless LAN Configuration Management

Obtain an accurate, real-time logical model of your wireless LAN solution hardware, software, and applications by using an efficient, reliable process for tracking components and component interrelationships. Identify, control, monitor, maintain, change, and verify versions of individual and interrelated solution components.

Why: Improve operational efficiency by maintaining an accurate, reliable solution configuration database and managing configuration changes through an orderly, effective process.

Wireless LAN Supplier Management

Facilitate the efficient delivery of networking products and services by hardware and software vendors through management of fulfillment, assurance, and financial processes.

Why: Increase operational productivity by aligning supplier processes and tools with your organizational requirements.

Wireless LAN Security Administration

Protect the confidentiality, integrity, and availability of information on the wireless LAN network using a thorough security administration process. Manage security incidents, identify and address vulnerabilities, and secure the delivery of content.

Why: Reduce the risk of wireless LAN network disruptions by proactively identifying security breaches and defining a remediation plan.

Lifecycle Services Methodology—Optimize Phase

A good business never stops looking for a competitive advantage. That is why continuous improvement is a mainstay of the wireless LAN solution lifecycle. In the *optimize* phase, a company is continually looking for ways to achieve operational excellence through improved performance, expanded services, and periodic reassessments of network value. Have business goals or technical requirements changed? Is a new capability or enhanced performance recommended? As an organization looks to optimize its wireless network and prepares to adapt to changing needs, the lifecycle begins anew-continually evolving the network and improving results.

Cisco recommends the following activities:

- Wireless LAN Business Requirements Alignment
- Wireless LAN Technology Assessment
- Wireless LAN Operations Assessment
- Wireless Security Assessment

These activities are described briefly in the sections that follow.

Wireless LAN Business Requirements Alignment

Evaluate how successfully your voice over wireless LAN solution is meeting the requirements established in your business requirements assessment. Analyze data on operational and capital costs, return on investment, and other related factors.

Why: Help realize your voice over wireless LAN investment goals by making recommendations to remediate gaps in solution performance relative to your objectives and requirements.

Wireless LAN Technology Assessment

Improve the performance, availability, capacity, and security of your voice over wireless LAN solution by assessing system performance and software configurations and recommending changes.

Why: Improve network performance, availability, capacity, and security by assessing a particular system and recommending improvements.

Wireless LAN Operations Assessment

Improve the performance and functionality of the operations and network management environment supporting your voice over wireless LAN solution by assessing it and recommending changes.

Why: Help reduce solution operating expenses and improve solution operational productivity, performance, and functionality by assessing your operations and network management environment and recommending changes.

Wireless Security Assessment

Assess network security system performance. Measure your security systems for trends and exceptions related to security policy and procedures and user access. Audit intrusion-detection data. Make recommendations for improvement.

Why: Improve the security of your company's information assets and your company's ability to mitigate intrusion attempts.

Cisco and our Wireless LAN Specialized Partners offer a broad portfolio of end-to-end services based on proven methodologies for deploying and operating a variety of secure voice and data wireless network solutions and technologies. For more information, please see http://www.cisco.com/en/US/products/ps8306/serv_home.html.

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.
CSM	Content Switching Module.
CSSC	Cisco Secure Services Client. Cisco Key Integrity Protocol (CKIP) and Cisco Message Integrity Check (CMIC).

D

DoS	Denial of service.
DTIM	Delivery Traffic Indication Map.

E

EAP	Extensible Authentication Protocol.
EAP-FAST	EAP-Flexible Authentication via Secured Tunnel.
EAP-TLS	EAP-Transport Layer Security.
EDCF	Enhanced distributed coordination function.
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

LAN	Local Area Network.
LAP	LWAPP Access Point.
LBS	Location-based service
LWAPP	Lightweight Access Point Protocol.

M

MAP	Mesh AP
MFP	Management frame protection.
MCS	Media Convergence Server.
MIC	Message integrity check.

N

NAC	Network Admission Control.
NAM	Network Analysis Module.

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.
PTK	Pairwise Transient Key.

R

RADIUS	Remote Authentication Dial-In User Service.
RF	Radio frequency.
RFID	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.
SSLSM	Secure Sockets Layer Services Modules.
SSO	Single sign-on.
SVI	Switched virtual interfaces.

T

TKIP	Temporal Key Integrity Protocol.
TLS	Transport Layer Security.

U

UCM	Unified Communications Manager
UDLD	UniDirectional Link Detection (UDLD)

V

VoWLAN	Voice over Wireless LAN.

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.