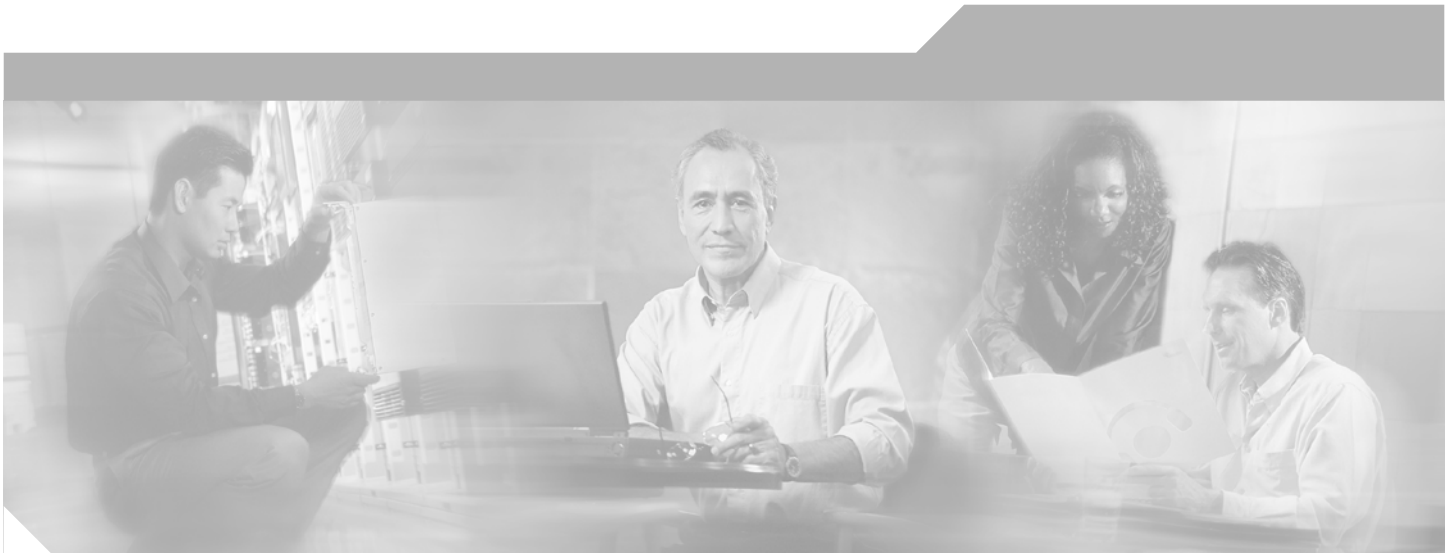


Cisco 7920 Wireless IP Phone Design and Deployment Guide

October 2005

Corporate 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: 408 526-4100

Text Part Number: OL-6383-04

CONTENTS

Preface

This document provides design and deployment considerations and guidelines for implementing wireless Cisco IP Telephony solutions based on the Cisco Architecture for Voice, Video, and Integrated Data (AVVID).

This document builds upon ideas and concepts presented in the *Cisco IP Telephony Solution Reference Network Design (SRND)* and the *Cisco Wireless LAN SRND*, both which are available online at

http://cisco.com/go/srnd

This document assumes that you are already familiar with the terms and concepts presented in the *Cisco IP Telephony SRND* and the *Cisco Wireless LAN SRND*. If you want to review any of those terms and concepts, refer to the documentation at the preceding URL.

New or Changed Information for This Release

Table 1 lists the topics that are new in the current release of this document or that have changed significantly from previous releases.

Table 1 New or Changed Information

Topic	Described in:
Switch port template for connecting APs to the Cisco Catalyst 3550 switch	Interconnecting WLANs to the Cisco Campus Infrastructure, page 4-6

Revision History

The following table lists the revision history for this document.

Revision Date	Comments
October, 2005	Corrected several typographical errors in Example 4-1 in the section on Interconnecting WLANs to the Cisco Campus Infrastructure, page 4-6.
March, 2005	Minor changes made to some of the configuration examples.

Revision Date	Comments
September, 2004	Various typographical errors were corrected. In addition, a configuration example was revised to illustrate a switch port template for connecting APs to the Cisco Catalyst 3550 switch (see Interconnecting WLANs to the Cisco Campus Infrastructure, page 4-6).
August, 2004	This design and deployment guide is a combination of the now obsolete *Wireless IPT Design Guide for the Cisco 7920 IP Phone* and the most recent version of the *Cisco Wireless IP Phone 7920 Deployment Recommendations*.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Overview of Cisco Wireless IP Telephony

Cisco Wireless IP Communications solutions deliver fully integrated communications by enabling data, voice, and video to be transmitted over a single wireless network infrastructure using standards-based 802.11 (a, b, and g) protocol. Leveraging the framework provided by Cisco IP hardware and software products, Cisco Wireless IP Communications solutions deliver unparalleled performance and capabilities to address current and emerging communications needs in the enterprise environment. Cisco Wireless IP Communications solutions are designed to optimize feature functionality, reduce configuration and maintenance requirements, and provide interoperability with a wide variety of other applications. Cisco Wireless IP Communications solutions provide this capability while maintaining a high level of availability, quality of service (QoS), and security for your network.

Cisco Wireless IP Communications encompasses the following solutions:

- IP Telephony
- Wireless LAN
- Device Mobility

The following sections in this chapter present an overview of the Cisco IP Telephony solution and its major components:

- Why Wireless IP Telephony?, page 1-1
- Architecture Overview, page 1-2

For more information on Wireless LAN and IP Telephony, refer to the design guides for those solutions, available online at

http://cisco.com/go/srnd

Why Wireless IP Telephony?

The communications industry, and industry analysts in general, now widely accept and acknowledge that wireless IP networks and applications have become a highly desirable transport medium for enterprise networks. The rapid adoption and migration of vendors to wireless IP as a transport for data and now voice further endorse this medium as a viable network paradigm. The message is clear: the move toward wireless IP is happening now.

Cisco provides a solid wireless IP network solution based on open standards, with an established portfolio of wireless access points (APs) and wireless endpoints to support your transition. The Cisco Wireless IP Telephony solution is the leading wireless network telephony solution for organizations that want to increase productivity and reduce the costs associated with managing and maintaining separate voice endpoints at each physical location. The flexibility and sophisticated

functionality of the Cisco wireless IP network infrastructure provides the framework that permits deployment of wireless phones throughout the enterprise, thus enhancing productivity and increasing enterprise revenues.

Architecture Overview

The Cisco IP Communications solution provides the foundation for next-generation IP networking across a number of network types including LANs, WANs, wireless LANs (WLANs), and Metro-Optical networks. The Cisco IP Communications network architecture not only delivers data, voice, and video over a converged IP network, but it also provides the framework for high availability, quality of service, and security.

The underlying network architecture for the Cisco Wireless IP Telephony solution consists of the following primary components:

Cisco Wireless LAN Infrastructure

The wireless network infrastructure includes access points (APs), antennas, and wireless endpoint devices, including wireless network interface cards (NICs) and wireless phones such as the Cisco 7920 Wireless IP Phone. The infrastructure can support various client types such as hardware phones and software phones.

Like wired LAN networks, 802.11 WLAN networks enable devices to transmit data, voice, and video at data rates up to 54 Mbps. Wireless networks have certain characteristics that make them different from wired networks:

- A WLAN operates as a shared medium, which means that communication on the WLAN is half-duplex and that all devices within a single WLAN share the same wireless connection. Speeds vary as follows, depending on the type of radio you are using:
  - 802.11a = 54 Mbps
  - 802.11b = 11 Mbps
  - 802.11g = 54 Mbps.
- WLAN bandwidth depends on the distance between the WLAN client and a WLAN AP. The farther the distance, the lower the supported data rates.
- Because all WLAN traffic is seen by all other WLAN devices within range, additional security measures must be taken to ensure that traffic is not captured or manipulated by intruders.

Cisco 7920 Wireless IP Phone

The Cisco 7920 Wireless IP Phone extends the Cisco family of IP phones from 10/100 Ethernet to 802.11 WLANs. The Cisco 7920 Wireless IP Phone provides multiple line appearances with functionality similar to existing Cisco 7900 Series IP Phones. In addition, the Cisco 7920 phone provides enhanced WLAN security and Quality of Service (QoS) for operation in 802.11b networks. The Cisco 7920 phone also provides support for XML-based data access and services.

Call Processing Agent

Cisco CallManager is the core call processing software for the Cisco IP Telephony solution. It builds call processing capabilities on top of the Cisco IP network infrastructure. Cisco CallManager software extends enterprise telephony features and capabilities to packet telephony network devices such as IP phones, media processing devices, Voice over IP (VoIP) gateways, and multimedia applications.

You can deploy the call processing capabilities of Cisco CallManager according to one of the following models, depending on the size, geographical distribution, and functional requirements of your enterprise:

- Single-site call processing model
- Multi-site WAN model with centralized call processing
- Multi-site WAN model with distributed call processing
- Clustering over the IP WAN

For more details on these call processing deployment models, refer to the *Cisco IP Telephony Solution Reference Network Design (SRND)* at

http://cisco.com/go/srnd

Security

The Cisco Wireless IP Telephony solution addresses security in the following main areas, among others:

- Physical security for restricting physical access to important application servers and network components, including Cisco CallManager servers and APs.
- Network access security to prevent hostile logins or attacks, including encryption and authentication using WEP and Cisco LEAP, and the elimination of rogue APs on the Wireless LAN.
- Security measures for Cisco CallManager, endpoint devices, and various directories and databases, including passwords for the Cisco 7920 Wireless IP Phones and strong password policies for Microsoft Windows and software applications.
- Mechanisms for defining calling privileges for various classes of users through the use of calling search spaces and partitions in Cisco CallManager.
- Careful network design and management to enhance security, including logging of network events (APs, switches, and routers), endpoint events, application software changes, and call detail records.

Quality of Service (QoS)

While Voice over IP (VoIP) technology does convert voice signals into IP data packets and converges them with data traffic, the IP network requirements for voice and data are very different. Data traffic typically has the following characteristics:

- Bursty — Traffic can be sent in large or small bursts, depending on the application.
- Maximum bandwidth consumption — TCP applications attempt to use as much bandwidth as the network will allow.
- Insensitive to packet loss — The retransmission capabilities of TCP enable data applications to continue to work correctly even with a certain amount of packet loss on the network.
- Insensitive to packet delays — Most TCP applications can handle some packet delay without affecting overall performance.

In contrast, voice traffic on an IP network has strict requirements concerning packet loss, delay, and delay variation (also known as jitter). To meet these requirements for voice traffic, the Cisco Wireless IP Telephony solution includes Quality of Service (QoS) features such as traffic classification, queuing, and shaping. In general, voice traffic has the following characteristics:

- Smooth — VoIP packets are sent at consistent intervals with uniform packet sizes.
- Minimal bandwidth consumption — VoIP packets attempt to use only the amount of bandwidth necessary to transmit from end to end. VoIP does not use any windowing to determine data rates.
- Sensitive to packet loss — VoIP traffic is extremely sensitive to packet loss. Excessive loss will degrade overall voice quality.
- Sensitive to delay and jitter — While VoIP can tolerate some amount of delay, excessive delay or excessive delay variation (jitter) will degrade overall voice quality.
- UDP Best Effort — VoIP sends RTP packets using UDP, which does not have a mechanism to retransmit lost packets.

Cisco has defined the following network guidelines for proper VoIP operation:

- Delay — not to exceed 150 ms (one-way)
- Delay variation (jitter) — not to exceed 30 ms
- Packet loss — not to exceed 1%

Note While isolated testing might show that VoIP calls could operate in a network outside of these guidelines, deploying a VoIP network under those conditions can lead to unpredictable results and poor voice quality. If problems arise in such cases, support from the Cisco Technical Assistance Center (TAC) will be limited.

The QoS components of the Cisco Wireless IP Telephony solution are provided through the rich IP traffic management, queueing, and shaping capabilities of the Cisco IP network infrastructure. Key elements of this infrastructure that enable QoS for IP Telephony include:

- Traffic marking
- Multiple queues
- Priority queuing
- Traffic shaping
- Call admission control

Network Management

The Cisco Wireless IP Telephony network infrastructure offers a number of network management, QoS, and security management tools that support the IP Communications solution. Cisco CallManager offers enhanced software and configuration management tools that leverage the strength and flexibility of IP networks. The Cisco CallManager user interface simplifies the most common subscriber and telephony configuration tasks by building upon legacy telephony administration systems and adding software and web-based applications.

In addition, CiscoWorks2000 includes a number of network management tools to manage the operations, administration, and maintenance of IP Telephony networks. In particular, CiscoWorks IP Telephony Environment Monitor (ITEM) provides a suite of applications and tools that facilitate effective management of both small and large IP Telephony installations based on the Cisco IP Communications network architecture as well as Cisco IOS software. CiscoWorks ITEM provides the following major features:

- Problem-focused fault analysis — Provides timely information about the health of IP Telephony environments.
- Confidence testing and monitoring — Uses synthetic testing to emulate normal day-to-day operations and to validate operational readiness of the IP infrastructure and the Cisco IP Telephony deployment.
- Intelligent integration with existing management infrastructures — Generates intelligent traps that can be forwarded to other event-management systems installed in the network, be sent to email or pager gateways, or be displayed on the Alerts and Activities Display (AAD).
- Evaluation and correlation capabilities — Evaluates the general health of the IP Telephony environment in the monitored network environment.
- Alerts and Activities Display (AAD) — Provides a proactive, web-based operations screen for real-time status and alerting of actual and suspected problems in the underlying IP network as well as in the Cisco IP Telephony implementation.
- ITEM Multi-View — Enables large enterprise customers and managed service providers to partition specific user communities and manage all of them from a single ITEM implementation.

The CiscoWorks Wireless LAN Solution Engine (WLSE) is another network management tool used specifically for monitoring and configuring wireless infrastructure devices. WLSE provides a simplified interface for managing large numbers of wireless APs and bridges, and it provides the following functionality:

- Configuring and upgrading firmware on APs and bridges within the infrastructure
- Reporting on device, client, and security information
- Monitoring of devices for faults, performance conditions, and misconfigurations as well as authentication server responses
- Managing the wireless radio environment to make deployment and expansion easier

For more information on CiscoWorks WLSE, refer to the Cisco AVVID Wireless LAN Design SRND, available at

http://cisco.com/go/srnd

In addition to the tools outlined above, both Cisco CallManager and Cisco APs provide detailed logging functionality that enables network administrators to monitor behavior and identify network problems or errors.

Radio Frequency and Site Survey

This chapter defines and explains radio frequency (RF) and RF requirements within the wireless network infrastructure needed to build a wireless IP Telephony system in an enterprise environment. In addition, this chapter examines in detail the site survey requirements and provides recommendations for performing an adequate site survey, including tools, parameters, and parameter values.

Wireless IP Telephony networks require careful RF planning, which begins with the successful completion of a thorough voice site survey to determine the proper level of wireless coverage and to identify sources of interference. Once the site survey has been performed, you can then determine AP placement and antenna selection and configure the wireless network infrastructure.

The following sections describe the nature of RF, site surveys, and the proper settings and environments for wireless telephony:

RF Overview

Before beginning any WLAN deployment, the network administrator should first complete a site survey of the environment where the WLAN devices will be deployed. The site survey should help to determine the number of APs required to provide RF coverage and the correct AP configurations. It should also take into consideration which types of antennas will provide the best coverage, as well as identifying sources of RF interference.

It is important to keep in mind that two physical environments rarely have the same RF characteristics. For this reason, any discussions of RF in this document are generalized, and network administrators might have to adjust the information to their specific RF environment and requirements.

Although many network administrators have already performed RF site surveys for their initial data WLAN deployments, the Cisco 7920 Wireless IP Phone has somewhat different roaming characteristics and different coverage requirements than Cisco Aironet NIC cards. Therefore, network administrators must perform a second site survey for voice to prepare for the performance requirements of the Cisco 7920 Wireless IP Phone. This second survey gives network administrators the opportunity to tune the APs to ensure that the Cisco 7920 Wireless IP Phones have enough RF coverage and bandwidth to provide proper voice quality.

Site Survey Verification

This section describes some of the tools, methods, and recommendations for performing the site survey.

Note Before you begin a site survey, Cisco recommends that you read this entire document to become familiar with all the differences between data and voice RF network requirements.

Site Survey Tools

Cisco produces some tools to perform the site survey for the Cisco Wireless IP Phone 7920 and the Cisco Aironet Client Utility for Cisco 340, 350, and CB20A wireless cards. The CiscoWorks Wireless LAN Solution Engine (WLSE) has an assisted site survey utility that can aid in the deployment of wireless networks for enterprises. Although CiscoWorks WLSE is highly effective, Cisco recommends that you use a third-party tool for very dense deployments or environments that have a high amount of interference. Third-party tools such as AirMagnet also provide additional detailed information that can aid in performing site surveys. After using a third-party site survey tool, Cisco recommends that you perform an additional site survey verification with end-use devices (in this case, Cisco 7920 Wireless IP Phones) because each client card can behave differently, depending on factors such as antenna gain and application limitations. This document describes certain important site survey data that you can obtain using both the Cisco 7920 Wireless IP Phone and the Cisco Aironet Client Utility for laptops.

RF Recommendations

You should perform a site survey to determine the number of APs required to provide RF coverage. The survey should take into consideration which types of antennas provide the best coverage, as well as where sources of RF interference exist. However, prior to beginning a site survey or deployment, perform an RF walkthrough to identify and mitigate sources of non-802.11 RF interference and rogue APs. Repeat the RF walkthrough periodically throughout the site survey and throughout the life of the deployment. Cisco has automated tools to assist with the site survey. (For information on those tools, see Conducting a Site Survey, page 2-6.)

For additional information on RF design considerations, refer to the chapter on WLAN Radio Frequency (RF) Design Considerations in the *Cisco Wireless LAN Design Guide*, available at

http://cisco.com/go/srnd

Channels

To improve roaming characteristics and to ensure proper functionality of the Cisco 7920 Wireless IP Phone, Cisco recommends that you use only non-overlapping channels to program the APs. For information on non-overlapping channels, see Cisco 7920 Wireless IP Phone Site Survey Tool, page 2-6.

When you configure the AP, Cisco recommends that you *disable* the option to search for the least-congested channel. Cisco recommends that administrators manually set all RF channels according to the data gathered during the site survey and site survey verification steps. For details on configuring the AP settings, see AP Configuration (for Installation), page 7-2.

If you use the option to select the least-congested channel, the AP will change to a different channel every time its power is reset, thus leaving no predictability and negating the time and effort spent on the site survey. Random selection of channels causes roaming times to increase because the phone has to scan all channels rather than a smaller subgroup of active channels.

Every regulatory domain specifies different allowable radio channels. Observe the following guidelines when selecting which channels to use:

- Always use channels that are a minimum of five radio channels apart so that they do not overlap. (For example, use channels 1, 6, and 11 or use 2, 7, and 12.) This practice reduces the ambient noise on each channel.

Note In this document, channel sets are groups of channels that overlap (such as 1, 2, 3, 4, and 5).

- Use the same non-overlapping channels throughout your deployment. This practice decreases roaming times.
- Always use diversity antennas for both indoor and outdoor environments. This practice tremendously reduces the effects of multipath interference.
- Refer to Site Survey RF Recommendations, page B-1, for best practices in RF deployments and for information on how to avoid common problems.

Recommended Environment for the Cisco 7920 Wireless IP Phone

This section describes the environment needed for a successful voice deployment. The environment will change when used for both data and voice.

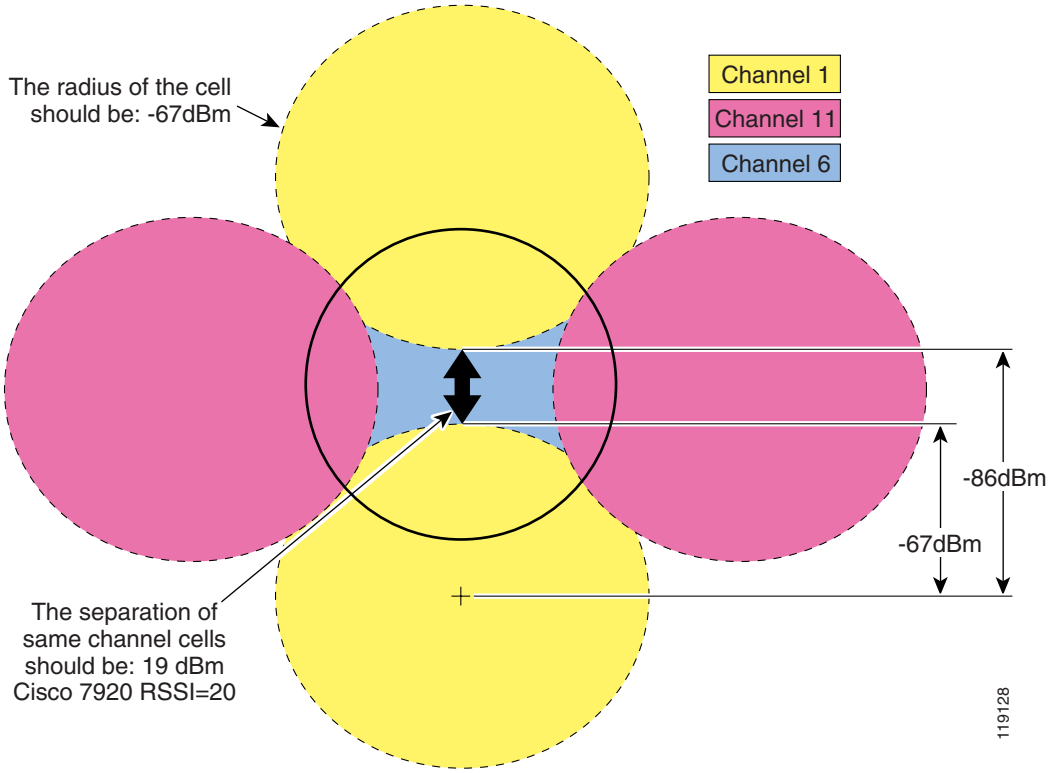
Note You must test the values listed here, both during the site survey and when the network is enabled for all users.

Observe the following guidelines when setting up the environment for the Cisco 7920 Wireless IP Phone:

- Deploy a minimum of two APs on non-overlapping channels, with a Received Signal Strength Indicator (RSSI) that is greater than 35 at all times in the phone's site survey utility.
- Deploy no more than one AP per overlapping channel set, with a received signal strength indicator (RSSI) that is greater than 35.
  - Although APs might appear to have an RSSI that is less than 35 (on overlapping APs), this situation can still cause interference and should be minimized as much as possible. (This interference or noise will degrade voice quality.)
  - Noise is additive. Having three extra APs on the same channel, all with low RSSI, can be as harmful as a single extra AP with a higher RSSI.

Figure 2-1 shows a typical deployment, with a 15% to 20% overlap of a given AP's cell from each of the adjoining cells. This configuration provides almost complete redundancy throughout the cell, thus complying with the above requirements.

Figure 2-1 Cell Overlap Guidelines



- Two of the APs (including the one with which the wireless phone is associated) must have an RSSI that is greater than 35 (which is equivalent to a receiver threshold of -67 decibels per milliwatt) and a channel utilization QoS Basis Service Set (QBSS) load that is less than 45. This requirement provides for smoother roaming and a backup AP if one of the APs suddenly becomes unavailable or busy.

  The QBSS load represents the percentage of time that the channel is in use by the AP. The overall channel load might be much higher than the QBSS load because several APs could be sharing the same RF channel and background or environmental noise could add to the load too. The Cisco 7920 Wireless IP Phone uses the QBSS load in its roaming algorithm. The measured QBSS load will vary, depending on the time of day when you perform the site survey. For example, at night (when the network is largely idle), the QBSS load will usually be very low. Therefore, you should perform the site survey during peak hours. You can reduce the QBSS load by adding APs as needed.

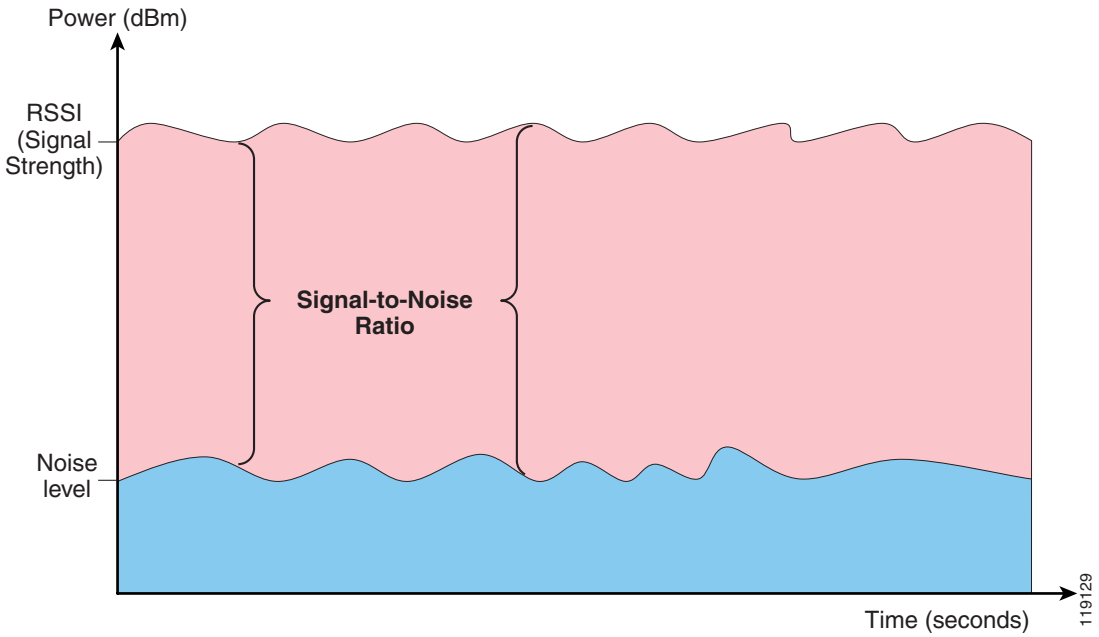
  Note The RSSI and channel utilization values can be read directly from the Cisco 7920 Wireless IP Phone site survey tool (identified in the section below). Table 2-2 shows the relationship between decibels per milliwatt (dBm, the industry standard values) and RSSI (relative values for the Cisco 7920 Wireless IP Phone). You can use these values to identify signal strength through the use of other site survey tools.

- Maintain at least 11 Mbps of available link speed at all times for data clients as well as voice clients.
- Maintain an AP coverage overlap of at least 15% to 20%.

Note In certain situations, data rates below 11 Mbps must be enabled for legacy devices. This lower speed will affect voice quality and the RF environment, and it is not the recommended setting. If you have to enable both 11 Mbps and 2 Mbps, these low speeds will reduce the number of simultaneous calls that each AP can handle and will also increase the overlap because they will extend the range of the APs.

- Maintain a packet error rate (PER) no higher than 1% (or a success rate of 99%).
- Maintain a minimum signal-to-noise ratio (SNR) of 25 dB (see Figure 2-2).

Figure 2-2 Signal-to-Noise Ratio



- Try to use the same transmit power on the AP and on the phones. If the transmit power of the APs varies, set the transmit power of the phones to the highest transmit power of the APs.

Note If enabled on the AP, Dynamic Transmit Power Control (DTPC) allows the AP to broadcast its transmit power, and clients can automatically configure themselves to that power while associated with that AP. The Cisco IOS command for enabling DTPC is **power client** and was first introduced in Cisco IOS version 12.2(4)JA. Beginning with firmware version 1.0(8), DTPC is enabled on the Cisco 7920 Wireless IP Phone, and the phone will automatically adjust its transmit power to the client power level configured on the AP to which it is associated.

- All AP antennas must use diversity. For more information, refer to Site Survey RF Recommendations, page B-1.
- APs in an optimal setting can handle seven G.711 or eight G.729 concurrent phone calls. If more concurrent phone calls are needed in a single location (a high usage area, for example), plan to have load-balancing APs available during the site survey. Overlapped basic service sets (BSSs, or APs sharing the same RF channel) reduce the number of concurrent phone calls per AP.

Conducting a Site Survey

The site survey process includes the following steps.

Step 1 Identify areas in the physical environment where there is non-802.11 RF interference. Interference sources include, but are not limited to, microwave ovens, Bluetooth transmitters, Frequency Hopping Access Points (FHAPs), and cordless phones. Interference from these devices can lead to choppy voice.

Step 2 Identify and eliminate rogue APs by using sniffers or the Cisco Structured Wireless-Aware Network (SWAN) architecture, which can automatically (and on an ongoing basis) detect rogue APs and non-802.11 interference. For more information on Cisco SWAN, visit

http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_package.html

Step 3 Determine the proper AP location and transmitter power levels so that the RF footprint of APs provides sufficient coverage for operation of the Cisco 7920 Wireless IP Phones. Make sure there is sufficient signal strength overlap so that the phones can roam between APs without dropping calls. Also make sure there is a sufficient signal-to-noise ratio (SNR) so that voice packets can be received despite any interference.

Step 4 Survey multiple floors together to ensure that coverage from one floor does not negatively impact other floors.

Step 5 Check roaming behavior to ensure that common roaming locations are not over a Layer-3 network.

Step 6 Install and configure the APs, verify coverage and SNR, and validate the network by making phone calls.

Cisco 7920 Wireless IP Phone Site Survey Tool

The site survey on the Cisco 7920 Wireless IP Phone is a display of information about the APs currently within range of the phone. It can be accessed by selecting **Menu > Network Config > Site Survey**. The survey displays a list of APs within range with the same Service Set Identifier (SSID) and security settings as the phone. The last two numbers (37 and 5 in Example 2-1) are RSSI and channel utilization values that are needed for a successful deployment. RSSI is the strength of the signal being heard by the phone. The QBSS value, or channel utilization, is the associated AP's use of the channel, which affects the phone's roaming decision. The section on Recommended Environment for the Cisco 7920 Wireless IP Phone, page 2-3, listed recommended values for both RSSI and channel utilization, and those values should be used for the site survey verification.Example 2-1 shows the type of information displayed on the phone.

Example 2-1 Site Survey Reading

1(C), SSID…, 37, 5

1 = The AP channel number (channel 1)

C = The channel state (see Table 2-1)

SSID = The SSID of the AP

37 = The RSSI value

5 = The AP channel utilization value (also known as the QBSS load value)

For each AP, you can display more information by pressing the Detail soft key. The display will give all the above information plus the full SSID and the MAC address of the AP. If more than one AP is current (C), you can determine which is the connected AP by looking at the AP detail, where a (C) will be listed after the MAC address. If this condition occurs (meaning that there are two or more APs detected on the same channel), all but one AP should have a signal strength below 35, although ideally all will have RSSIs as low as possible.

Table 2-1 lists the AP channel state codes.

Table 2-1 Channel States Reported by the Cisco 7920 Wireless IP Phone Site Survey Utility

Channel State	Relationship of AP to Cisco 7920 Wireless IP Phone
C	Current: The channel to which the Cisco 7920 Wireless IP Phone is currently associated.
A	Available: Active channel is available and is a possible candidate for roaming.
N	Non-overlapping: If the Cisco 7920 Wireless IP Phone is currently associated with CH6, then the non-overlapping channels are: 1 and 11 for North America; 1 and 11 or 12 or 13 for Europe; 1 and 11 or 12 or 13 or 14 for Japan.
O	Overlapping: If the Cisco 7920 Wireless IP Phone is currently associated with CH6, then the overlapping channels are 2,3,4,5,7,8,9, and 10.
I	Incompatible

As a standard, RF values are measured in decibels per milliwatt (dBm). Table 2-2 shows the correlation between the dBm rating and the corresponding RSSI value for the Cisco 7920 Wireless IP Phone.

Table 2-2 Comparison of dBm and RSSI Values for Cisco 7920 Wireless IP Phones

RSSI	5	10	15	20	25	30	35	40	45	50	55	60	65	70
dBm	-98	-97	-89	-83	-79	-75	-67	-61	-57	-49	-44	-41	-38	-34

Table 2-3 shows the dBm ratings and the corresponding RSSI values for the Cisco Aironet 350 Series Access Points. The RSSI is labeled with a % sign in the Cisco Aironet Client Utility (ACU).

Table 2-3 Comparison of dBm and RSSI Values for Cisco ACU Client Adapters

RSSI	0	5	10	15	20	25	30	35	45	50	55	60	65	70	75
dBm	-113	-108	-103	-97	-92	-87	-82	-77	-62	-58	-50	-47	-43	-39	-33

Using the Cisco 7920 Wireless IP Phone Site Survey Tool

Observe the following guidelines when using the Cisco 7920 Wireless IP Phone Site Survey Tool:

- Configure the Cisco 7920 Wireless IP Phone with the same SSID, encryption, and authentication settings as the APs.
- Once the phone is associated with the WLAN, navigate to the Site Survey menu on the Cisco 7920 Wireless IP Phone by selecting **Menu > Network Config > Site Survey**.

- Walk through all areas where phones will be in use, and take readings in each area. During this stage of the verification, Cisco recommends that you approach important areas from different directions to check the roaming possibilities from different perspectives.
- Adjust the AP and antenna placement, as well as the AP power settings, to comply with the Recommended Environment for the Cisco 7920 Wireless IP Phone, page 2-3.

Using the Cisco Aironet Client Utility Site Survey Utility

You can use the Cisco Aironet Client Utility (ACU) in conjunction with the Cisco 7920 Wireless IP Phone to adjust the WLAN for voice applications. For instructions on how to use the Cisco Aironet Client Utility, refer to the *Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows*, available at

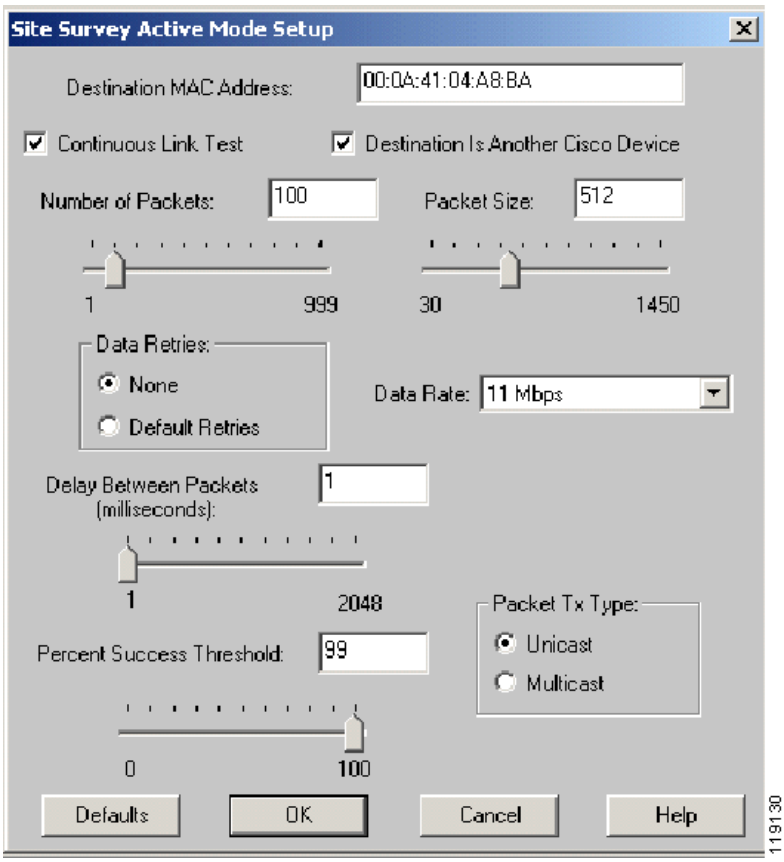
http://www.cisco.com

Use the following steps to set up a site survey in Active Mode.

Step 1 Use the following settings, shown in Figure 2-3:

- Data Rate: 11 Mbps
- Percent Success Threshold: 99

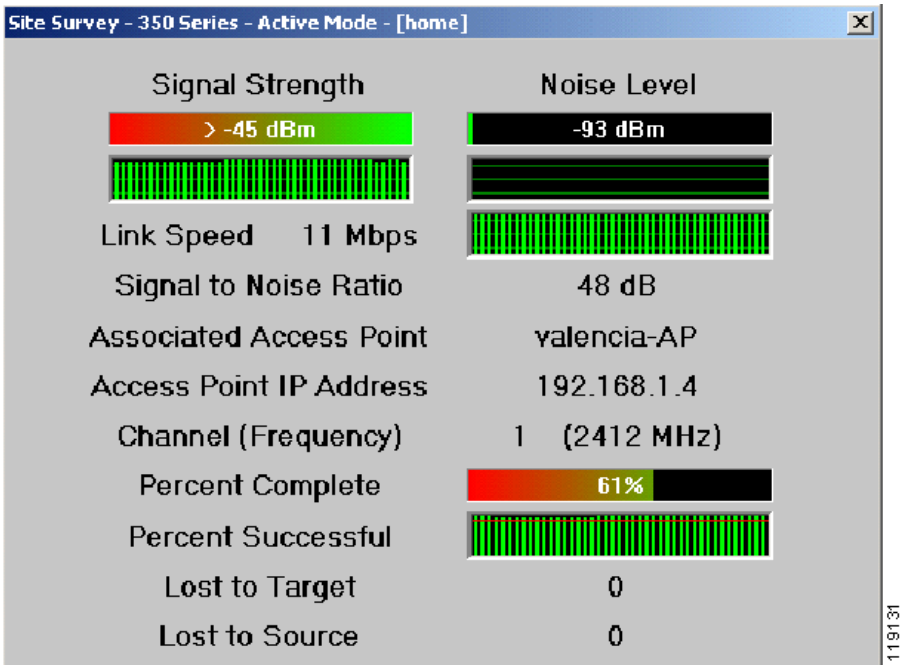
Figure 2-3 Cisco ACU Site Survey Screen



Step 2 Click **Start** and walk through the coverage area. Verify the following values to ensure acceptable coverage for the Cisco 7920 Wireless IP Phone (see Figure 2-4):

- Signal-to-noise ratio (SNR) should not drop below 25 dB. Anything less might not provide a robust 11 Mbps data rate.
- The Percent Successful bar should not drop below the 99% threshold set up in Step 1.

Figure 2-4 Output from Cisco ACU Site Survey Utility



Step 3 To check for the percentage overlap, walk through the full coverage area for each AP to find the locations where the SNR is no longer in the acceptable range, and mark those locations on a site plan.

Step 4 Conduct this test for each AP sequentially, and check the coverage overlap of each cell. If the overlaps are too great, begin by lowering the transmit power on the AP. If necessary, adjust the location of the AP or the type of antenna used on that AP.

CHAPTER 3

Security

Wireless IP Telephony networks require a carefully planned security implementation to ensure that the telephony network operates properly and that voice traffic is secure. This chapter defines and explains security for the Cisco 7920 Wireless IP Phone and the wireless network infrastructure needed for a highly secure Wireless IP Telephony system in an enterprise environment. This chapter also discusses deployment methods and some of the configuration steps.

The Cisco 7920 Wireless IP Phone is supported in the architecture of the Cisco Wireless Security Suite. This architecture fits into the overall Cisco SAFE security architecture. For a description of the Cisco Wireless Security Suite and design guidelines for Cisco SAFE, refer to the documentation for these topics available at

http://www.cisco.com

The following sections describe network security, deployment options, and configuration settings for the Cisco 7920 Wireless IP Phone and WLAN:

Security Mechanisms

The Cisco 7920 Wireless IP Phone supports both Static Wired Equivalent Privacy (WEP) and Cisco LEAP for authentication and data encryption. If either encryption model is used, both the signaling (Skinny Client Control Protocol, or SCCP) and media (RTP) are encrypted between the Cisco 7920 phone and the AP.

Static WEP

Static WEP requires that a 40-bit or 128-bit key be entered manually on all of the Cisco 7920 phones as well as the APs. It performs AP-based authentication by verifying that the accessing device (in this case, the Cisco 7920 phone) has a matching key.

LEAP

LEAP allows devices (such as the Cisco 7920 phone and AP) to be authenticated mutually (phone-to-AP and AP-to-phone) based on a user name and password. Upon authentication, a dynamic key is used between the Cisco 7920 phone and the AP to encrypt traffic.

If LEAP is used, a LEAP-compliant RADIUS server, such as the Cisco Access Control Server (ACS), is required to provide access to the user database. The Cisco ACS can either store the user name and password database locally, or it can access that information from an external Microsoft Windows NT directory.

When using LEAP, ensure that strong passwords are used on all wireless devices. Strong passwords are defined as being between 10 and 12 characters long and can include both uppercase and lowercase characters as well as the special characters * & % $ # @.

Because most users save their passwords on the phone, Cisco recommends that you use different user names and passwords on data clients and wireless voice clients. This practice helps with tracking and troubleshooting as well as security.

Note Although it is a valid configuration option to use an external (off-ACS) database to store the user names and passwords for the Cisco 7920 phones, Cisco does *not* recommend this practice. Because the ACS must be queried whenever the Cisco 7920 phone roams between APs, the unpredictable delay to access an off-ACS database could cause excessive delay and poor voice quality.

ACS Deployment Options

When deploying LEAP, give careful consideration to the placement of the Cisco ACS. LEAP authentication is required every time a Cisco 7920 phone roams between APs, and RTP traffic (voice) will not flow until the LEAP authentication is completed. Therefore, reducing the amount of delay between the AP and the ACS is a critical component of engineering proper voice quality into the WLAN network.

You can deploy the Cisco Access Control Servers in one of the following ways:

- Centralized ACS

  All users access the ACS in a central location within the network.

- Remote ACS

  For remote offices that have slow-speed WAN links or congested WAN links that might delay LEAP processing, an ACS could be deployed locally at each remote office.

- Local and/or fallback RADIUS server functionality in the Cisco AP

  Cisco IOS Release 12.2(11)JA introduced support for the Cisco AP to authenticate LEAP users without having to access an external ACS. This functionality supports up to 50 user names and is supported for LEAP only. This functionality does not interact with a centralized or remote ACS for database synchronization. This functionality is designed to be used as the primary RADIUS functionality in a small office, but it could also be used as a backup to a Cisco ACS in case of a WAN link failure. (See Example Configurations for AP and RADIUS Server, page C-1, for a configuration example.)

Note With Cisco Centralized Key Management (Cisco CKM), the phone can perform fast Layer-2 or Layer-3 roaming with a Wireless LAN Services Module (WLSM) in the network because the APs cache credentials and thus do not have to re-authenticate the device with the ACS each time.

Wireless Network Infrastructure

The Wireless IP Telephony network, just like a wired IP Telephony network, requires careful planning for VLAN configuration, network sizing, multicast transport, and equipment choices. For both wired and wireless IP Telephony networks, you should configure separate voice and data VLANs, provision sufficient network bandwidth, select the appropriate protocols and transport mechanisms, properly plan and configure connectivity to other networks, and select servers and switches for the network based on expected loads, numbers of users, and required features.

The following sections discuss various components and configurations that you should consider when designing a Wireless IP Telephony network:

VLANs

Virtual LANs (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.

Purpose of VLANs

Wireless LANs (WLANs) use VLANs to provide the following functions:

- Segment traffic into distinct broadcast domains or IP subnets
- Create separate security domains for various security models (Open, WEP, LEAP, PEAP, and EAP-TLS).

Voice and Data VLANs

Cisco recommends that you configure separate VLANs for voice and data traffic: a native VLAN for data traffic and a voice or auxiliary VLAN for voice traffic. 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, thus ensuring that appropriate QoS is provided for various classes of traffic and helping to resolve addressing issues such IP addressing, security, and network dimensioning.

Number of VLANs and SSIDs

Cisco Aironet 350, 1100, and 1200 Series Access Points support up to 16 VLANs. Cisco APs can be connected to Cisco Catalyst Switches via 802.1Q trunks. (In hybrid mode, the native VLAN's Port VLAN ID (PVID) is not tagged.) Each VLAN is then mapped to a unique Service Set Identifier (SSID) on the AP. Users (or IP Phones) can then be assigned to VLANs either statically based on SSID or dynamically though use of RADIUS authentication. Each VLAN can use a different security mechanism, although only one can be unencrypted (open).

For more details on deploying VLANs in wireless networks, refer to the Cisco Aironet 350, 1100, or 1200 Series *Wireless Virtual LAN Deployment Guide*, available at

http://www.cisco.com

Network Sizing

IP Telephony network sizing is essential to ensure that adequate bandwidth and resources are available to carry mission-critical voice traffic. In addition to the usual IP Telephony design guidelines for sizing components such as PSTN gateway ports, transcoders, WAN bandwidth, and so forth, also consider the following 802.11b issues when sizing your Wireless IP Telephony network:

Number of 802.11b Devices per AP

Cisco recommends that you have no more than 15 to 25 802.11b devices per AP.

Number of 802.11b Phones per AP

Before any discussion about network planning can take place, it helps to understand the basics of the overall network capacity.

The following network capacity guidelines apply to sizing the Wireless IP Telephony network:

- No more than 7 concurrent G.711 calls per AP.
- No more than 8 concurrent G.729 calls per AP.

Note These design recommendations assume that Voice Activity Detection (VAD) has been disabled on the Cisco 7920 Wireless IP Phones. Use of VAD on the Cisco 7920 phones can conserve bandwidth, but Cisco recommends that you disable VAD on all Cisco CallManager servers to provide better overall voice quality.

In addition to determining how much bandwidth is needed for an 802.11b VoIP call, you must also consider overall radio contention for a particular RF channel. The general rule is that you should not deploy any more than 20 to 25 802.11b endpoints per AP. The more endpoints you add to an AP, the more you reduce the amount of overall bandwidth and potentially increase transmission delays.

The maximum number of phones per AP depends on the calling patterns of individual users (based on Erlang ratios). Cisco recommends no more than 7 concurrent calls using G.711 or 8 concurrent calls using G.729. Beyond that number of calls, when excessive background data is present, the voice quality of all calls becomes unacceptable.

Packetization rates for these recommendations are based on 20-ms sample rates with VAD disabled. This rate generates 50 packets per second (pps) in each direction. Using a larger sample size (such as 40 ms) could result in a larger number of simultaneous calls, but it will also increase the end-to-end delay of the VoIP calls.

Number of 802.11b Phones per Layer-2 Subnet or VLAN

The number of 802.11b phones you can deploy per Layer-2 subnet or VLAN depends on the following factors.

- No more than seven G.711 or eight G.729 active calls per AP
- The calling ratio used to determine the number of active and non-active calls. This ratio is often determined using Erlang calculators.

Based on these factors and normal business-class Erlang ratios (between 3:1 and 5:1), Cisco recommends that you deploy no more than 450 to 600 Cisco 7920 phones per Layer-2 subnet or VLAN.

Multicast and Wireless Voice

Multicast network traffic can be problematic on a wireless network, especially for wireless voice networks. Although 802.11b WLANs are capable of sending multicast IP packets, there are technical limitations that make multicast unsuitable for voice networks and real-time applications such as multicast music on hold (MoH).

Multicast network traffic can be an issue on wireless networks due to the following factors:

- Multicast transport on the WLAN is unacknowledged. While this factor might seem irrelevant for UDP packets such as voice traffic, the difference is that an Ethernet connection has a bit-error rate (BER) of about 10^{10} while a WLAN has a BER of about 10^{5}. WLANs resolve this issue by using acknowledgements on the link layer to ensure reliable delivery. This reliable delivery does not occur for multicast traffic.
- Multicast packets are transmitted at the lowest rate of any device associated with the AP, whether that client wants the multicast packets or not. Thus, an AP supporting multiple bit rates will send multicast traffic at the lowest bit rate. This behavior degrades the overall performance of the WLAN.
- When devices operate in power-save mode (such as when a Cisco 7920 phone enters power-save mode to extend its battery life), the AP buffers the multicast packets and does not send them until the devices are no longer in power-save mode. This practice ensures that all clients receive the multicast traffic.

For these reasons, the Cisco 7920 Wireless IP Phone does not support multicast traffic, and Cisco recommends unicast-only traffic in wireless telephony environments. Although it is usually desirable to send traffic such as music-on-hold to phones via multicast for all voice endpoint devices, multicast is not possible for the Cisco 7920 phone because only unicast MoH is supported. Currently Cisco CallManager software has no ability to differentiate automatically between those endpoint devices that are enabled for multicast and endpoint devices that are capable of unicast only. Thus, even if a Cisco CallManager is configured with both multicast and unicast MoH resources, it has no way to determine dynamically which devices are capable of receiving multicast streams. To handle a mixture of multicast and non-multicast endpoint devices, Cisco CallManager must be told which devices can

receive multicast MoH streams and which devices can receive only unicast MoH streams. You can provide Cisco CallManager with this information by configuring separate media resource groups (MRG) and media resource group lists (MRGL) for multicast and unicast resources.

Server and Switch Recommendations

The following sections recommend server and switch types to use in building the wireless network infrastructure for the Cisco 7920 Wireless IP Phones.

Server Recommendations

A voice network requires at least one Cisco CallManager server. This server can be located either on-site or remotely over a WAN link; however, servers located over a WAN link can cause delays in phone registration, roaming, and call set-up. If problems arise, test the scenario with wired phones going to the same Cisco CallManager to test the WAN speeds. The wired phone must be on the same VLAN and switch port as the AP in order to check the entire path of the packet, just as if it came from the AP to the Cisco CallManager server. It might become necessary to either decrease the delay times on the WAN link or move the Cisco CallManager server on-site.

Note Cisco recommends that you use Cisco CallManager Release 3.3 (3) SR1 or later for wireless voice deployments.

A central authentication, authorization, and accounting (AAA) server can be used to perform LEAP and/or MAC authentication. This server can also be placed on-site or over a WAN link. A WAN link can add considerable delays in authentication, so Cisco generally recommends that you deploy a local AAA server to expedite the authentication process. AAA functions can also be performed by a dedicated Cisco IOS AP that is running local authentication. However, this AP can only support 50 users and should be considered only in small offices or specialty locations (for example, retail stores).

Note Cisco recommends that you use Cisco Authentication and Control Server (ACS) version 3.1 or later for wireless voice deployments.

If two APs terminate on the same network appliance, Cisco highly recommend that you do *not* use a hub because the hub will add delays on the Ethernet interface as well as on the RF interface. Rather, use a switch, which has multiple collision domains. In addition, Cisco recommends that you do not use hubs anywhere that devices connect to an AP because the hub will send unnecessary data to the AP.

Switch Recommendations

Note If you are using a Cisco Catalyst 4000 Series Switch as the main router in the network, ensure that it contains, at a minimum, either a Supervisor Engine 2+ (SUP2+) or Supervisor Engine 3 (SUP3) module. The SUP1 or SUP2 module can cause roaming delays, as can the Cisco Catalyst 2948G, 2980G, 2980G-A, 4912, and 2948G-GE-TX switches.

You can create a switch port template for use when configuring any switch port for connection to an AP. This template should add all the baseline security and resiliency features of the Standard Desktop template. In addition, when attaching the AP to a Cisco Catalyst 3550 switch, you can optimize the performance of the AP by using Multilayer Switching (MLS) QoS commands to limit the port rate and to map Class of Service (CoS) to Differentiated Services Code Point (DSCP) settings. For an example of an AP switch port template for the Catalyst 3550 switch, see Interconnecting WLANs to the Cisco Campus Infrastructure, page 4-6.

While Ethernet switch ports can typically transmit and receive at 100 Mbps, APs (depending on the type of radio) have a lower throughput rate because individual 802.11 standards allow for a maximum data rate of 54 Mbps. Furthermore, wireless LANs are a shared medium and, due to contention for this medium, the actual throughput is substantially lower. This throughput mismatch means that, with a burst of traffic, the AP will drop packets, thus adding excessive processor burden to the unit and affecting performance.

By taking advantage of the Catalyst 3550 policing and rate limiting capabilities, you can eliminate the need for the AP to drop excessive packets. The proposed AP switch port template will rate-limit the port to the practical throughput of 7 Mbps for 802.11b and guarantee 1 Mbps for high-priority voice and control traffic. With this prioritization, the template can be used with the Cisco 7920 Wireless IP Phones. Table 4-1 shows the allowed throughput for various types of AP radios.

Table 4-1 Switch Port Throughput for Various Radio Types

Type of Radio	Throughput Allowed by Switch Port
802.11a	42 Mbps
802.11b	7 Mbps
802.11g	36 Mbps
802.11a + 802.11b	49 Mbps
802.11a + 802.11g	78 Mbps

This template helps create a secure and resilient network connection with the following features:

- Return Port Configurations to "default" — Prevents configuration conflicts by clearing any pre-existing port configurations.
- Disable Dynamic Trunking Protocol (DTP) — Disables dynamic trunking, which is not needed for connection to an AP.
- Disable Port Aggregation Protocol (PagP) — PagP is enabled by default but is not needed for user-facing ports.
- Enable Port Fast — Allows a switch to quickly resume forwarding traffic if a Spanning Tree link goes down.
- Configure Wireless VLAN — Creates a unique wireless VLAN that isolates wireless traffic from other data, voice, and management VLANs, thereby isolating traffic and ensuring greater control of traffic.
- Enable Quality of Service (QoS); Don't trust port (mark down to 0) — Ensures appropriate treatment of high-priority traffic, including softphones, and prevents users from consuming excessive bandwidth by reconfiguring their PCs.

Cisco 3550-24-PWR Inline Power Switches can be used to provide power to APs that are capable of receiving inline power.

Interconnecting WLANs to the Cisco Campus Infrastructure

The following switch configuration shows an example of a switch port template for connecting APs to the Cisco Catalyst 3550 switch.

Example 4-1 Connecting APs to Catalyst 3550 SMI/EMI

```
default interface <xx/yy>
spanning-tree bpduguard enable
spanning-tree bpdufilter enable
no channel-protocol pagp
spanning-tree portfast
!
mls qos
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos map policed-dscp  24 26 46 to 8
mls qos aggregate-policer AGG-POL-1M-VOICE-OUT 1000000 8000 exceed-action
policed-dscp-transmit
mls qos aggregate-policer AGG-POL-6M-DEFAULT-OUT 6000000 8000 exceed-action drop
!
class-map match-all EGRESS-DSCP-0
  match ip dscp 0
class-map match-all EGRESS-DSCP-8
  match ip dscp 8
class-map match-all EGRESS-DSCP-16
  match ip dscp 16
class-map match-all EGRESS-DSCP-32
  match ip dscp 32
class-map match-all EGRESS-DSCP-48
  match ip dscp 48
class-map match-all EGRESS-DSCP-56
  match ip dscp 56
class-map match-any VOICE-SIGNALING
  match ip dscp 24
  match ip dscp 26
class-map match-all VOICE
  match ip dscp 46
class-map match-all INGRESS-DATA
  match any
class-map match-all INGRESS-VVLAN-VOICE
 match vlan 3
 match class-map VOICE
class-map match-all INGRESS-VVLAN-VOICE-SIGNALING
 match vlan 3
 match class-map VOICE-SIGNALING
class-map match-all INGRESS-DVLAN
 match vlan 2
 match class-map INGRESS-DATA
!
policy-map EGRESS-RATE-LIMITER
 class EGRESS-DSCP-0
  police aggregate AGG-POL-6M-DEFAULT-OUT
 class EGRESS-DSCP-8
  police aggregate AGG-POL-6M-DEFAULT-OUT
 class EGRESS-DSCP-16
  police aggregate AGG-POL-6M-DEFAULT-OUT
 class EGRESS-DSCP-32
  police aggregate AGG-POL-6M-DEFAULT-OUT
 class EGRESS-DSCP-48
  police aggregate AGG-POL-6M-DEFAULT-OUT
 class EGRESS-DSCP-56
  police aggregate AGG-POL-6M-DEFAULT-OUT
```

```
 class VOICE
  police aggregate AGG-POL-1M-VOICE-OUT
 class VOICE-SIGNALING
  police aggregate AGG-POL-1M-VOICE-OUT
!
policy-map INGRESS-QOS
 class INGRESS-VVLAN-VOICE
  set ip dscp 46
 class INGRESS-VVLAN-VOICE-SIGNALING
  set ip dscp 24
 class INGRESS-DVLAN
  set ip dscp 0
!
!
interface [interface id]
 description 11Mb towards Wireless Access Point
 switchport access vlan 2
 switchport voice vlan 3
 no ip address
 mls qos monitor dscp 0 10 18 24 26 34 46 48
 mls qos monitor dscp 56
 service-policy output EGRESS-RATE-LIMITER
 service-policy input INGRESS-QOS
 wrr-queue bandwidth 5 25 70 1
 wrr-queue cos-map 1 1
 wrr-queue cos-map 2 0
 wrr-queue cos-map 3 2 3 4 6 7
 wrr-queue cos-map 4 5
 priority-queue out
```

CHAPTER 5

Layer 2 and Layer 3 Roaming

An integral concept for wireless networks is device roaming. It is important to understand what roaming is, how and when it occurs, what types of roaming there are, and how the types differ. One of the obvious benefits of WLAN IP Phones compared to wired IP Phones is the ability of the user to move from place to place while having a conversation. But unlike cellular phone services, where coverage areas are usually nationwide or international, WLAN IP Phones have smaller coverage areas. In addition, administrators of WLAN IP Phone networks need to understand and consider their IP addressing schemes before deploying WLAN IP Phones. They need to consider how WLAN IP Phone coverage overlays with the Layer 2 and Layer 3 addressing within the IP network. A Layer 2 network is defined as a single IP subnet and broadcast domain, while a Layer 3 network is defined as the combination of multiple IP subnets and broadcast domains.

The following sections explain roaming concepts and how roaming works:

Roaming Terminology

In voice systems, roaming usually refers to physical movement and the locations from which a call can originate. For 802.11 data networks, roaming also refers to physical movement, but it is often associated with data connectivity while physically moving.

For purposes of this document, the following terms apply to roaming:

- Pre-call roaming

  This type of roaming occurs when a user with a Cisco 7920 Wireless IP Phone moves from place to place (within a campus or between sites) before making a voice call. This roaming may occur within a Layer 2 VLAN or across Layer 3 subnet boundaries. If it is within a Layer 2 VLAN, the IP address on the Cisco 7920 phone will remain the same. If it is across a Layer 3 boundary and DHCP is enabled on the Cisco 7920 phone, then the phone will recognize that it is no longer in the previous subnet and will use DHCP to obtain a new IP address.

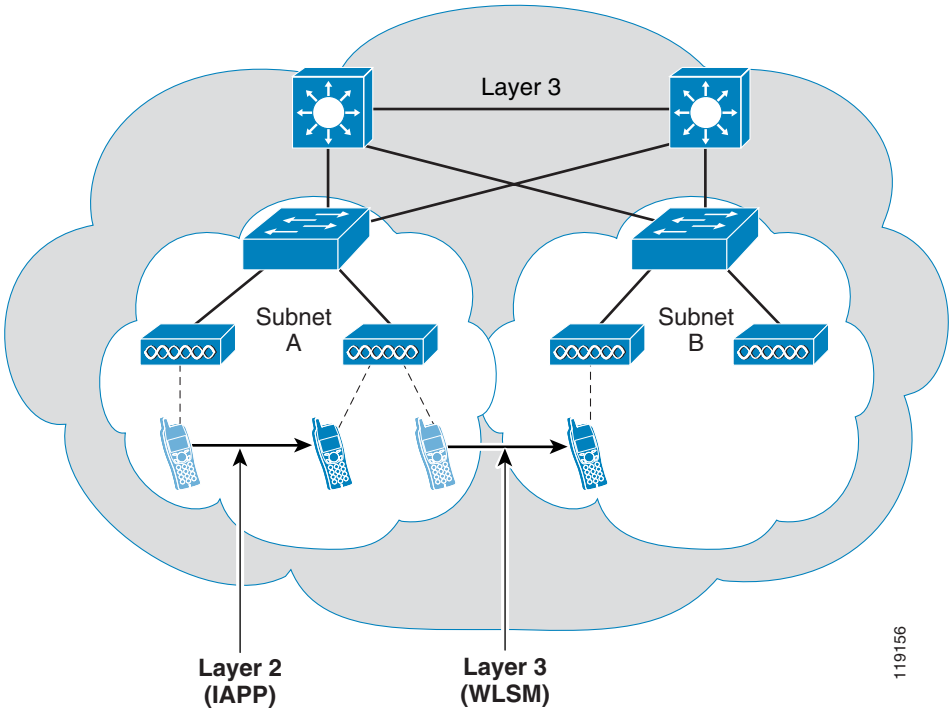
- Mid-call roaming

  This type of roaming occurs when a user with a Cisco 7920 Wireless IP Phone moves from place to place (within a campus or between sites) while a voice call is active on the phone.

Note Throughout the remainder of this document, the terms "roam" and "roaming" refer to mid-call roaming.

The Cisco 7920 Wireless IP Phone currently supports both Layer 2 and Layer 3 roaming. The Cisco 7920 phone itself supports Layer 2 roaming, but Layer 3 roaming requires the use of a Cisco Wireless LAN Services Module (WLSM) in the network. Figure 5-1 illustrates Layer 2 and Layer 3 roaming behavior.

Figure 5-1 Layer 2 and Layer 3 Roaming



Layer 2 Roaming

Layer 2 roaming occurs when a WLAN device (for example, a Cisco 7920 phone) moves far enough that its radio associates with a different AP. With Layer 2 roaming, the original and the new AP offer coverage for the same IP subnet, so the device's IP address is still be valid after the roam.

Cisco 7920 phones perform a Layer 2 roam for any of the following reasons:

- Initial boot-up of the Cisco 7920 phone is considered a roaming event because the phone is associating with a new AP.
- If the Cisco 7920 phone does not receive beacons from the associated AP, it believes that the AP is no longer available. If the Cisco 7920 phone does not receive three consecutive beacons and its unicast packet to the AP is not acknowledged, the phone will begin the roaming process to another AP.
- The Cisco 7920 phone periodically scans for a better AP. Because initial startup is considered to be a roaming event, all client stations have roamed at least once. After the roaming process is completed, the client station maintains the list of eligible roam targets. When all AP information is received (channel update and current AP update), the phone evaluates its current AP against the list of eligible roam targets. If conditions change on the current AP (low RSSI or high QBSS) so that one of the APs in the client's stored list now appears to be a better choice than the current AP, the phone will start a handoff procedure to associate with the better AP.

- A change in SSID or encryption type on the Cisco 7920 phone will also cause Layer 2 roaming.

Once one of these events occurs, the Layer 2 roaming process proceeds as follows:

1. The Cisco 7920 phone looks at its list of eligible roam targets (APs with a matching SSID and encryption type) and chooses the best candidate. The phone then attempts to associate and authenticate with this AP. If either the association or authentication fails, the phone tries the next best candidate AP.

   Note As a Cisco 7920 phone roams between APs, it re-authenticates with each new AP.

2. The candidate AP (AP B) sends a null-MAC multicast message using the source address of the Cisco 7920 phone. This message updates the CAM tables in upstream switches and directs further LAN traffic for the phone to AP B and not AP A.
3. AP B sends a MAC multicast message using its own source address to tell the old AP (AP A) that AP B now has the client associated to it. AP A receives this multicast message and removes the client MAC address from its association table. This message uses the Inter-Access Point Protocol (IAPP).

The Cisco 7920 phone uses the following variables to determine the best AP for Layer 2 roaming:

- RSSI

  The Cisco 7920 phone uses the Received Signal Strength Indicator (RSSI) to determine the signal strength of available APs within an RF coverage area. Initially, the phone attempts to associate with the AP that has the highest RSSI value as well as matching authentication and encryption type.

- QBSS

  The QoS Basis Service Set (QBSS) is a beacon information element (IE) that enables the AP to communicate its channel utilization to the Cisco 7920 phone. Because APs with high channel utilization might not be able to handle voice traffic effectively, the phone uses the QBSS value to determine if it should attempt to roam to another AP.

When roaming, the Cisco 7920 phone uses the following process to determine which AP should be the next candidate:

1. Determine which APs have an RSSI that is above the threshold of the currently associated AP.
2. Determine which APs are advertising QBSS in their beacons. These APs are considered handoff candidates before APs that are not advertising QBSS. If any of these APs meet the threshold criteria, begin the roaming process.
3. If no APs advertise QBSS, then RSSI is the only value used to determine roaming. Cisco recommends, however, that you enable QBSS on all APs used for voice deployments.
4. RSSI always takes precedence over QBSS if both thresholds have been met.

The amount of time it takes for the Cisco 7920 phone to roam between APs depends on which of the following security models is used (average times are listed):

- Layer 2 roaming with Static WEP: less than 100 ms
- Layer 2 roaming with LEAP and local ACS authentication: 200 to 400 ms

Note Delay times with LEAP could be longer than 200 to 400 ms if the Cisco ACS is heavily used by other applications such as remote-access dial-up, VPN, TACACS authentication, and so forth.

Layer 2 roaming time represents the time between the last RTP packet seen on AP-1 and the first RTP packet seen on AP-2. It also includes the time it takes to re-authenticate and re-associate with AP-2.

Figure 5-2 shows a sample trace of a Cisco 7920 phone roaming to a new AP, as well as the LEAP messaging between the phone and the AP.

Figure 5-2 Wireless Packet Trace of Cisco 7920 Phone Roaming

Packet	Source	Destination	BSSID	Protocol	Data Rate	Channel	Signal	Size	Delta Time	Relative Time
32	AP1200 - 2	7920	AP1200 - 2	EAP Request	11.0	1	100%	82		00.000000
33	7920	AP1200 - 2	AP1200 - 2	EAP Response	11.0	1	100%	53	00.002129	00.002129
34	AP1200 - 2	7920	AP1200 - 2	EAP Request	11.0	1	100%	82	00.015799	00.017928
35	7920	AP1200 - 2	AP1200 - 2	EAP Response	11.0	1	100%	80	00.007655	00.025583
37	AP1200 - 2	7920	AP1200 - 2	EAP Success	11.0	1	100%	82	00.024313	00.049896
38	7920	AP1200 - 2	AP1200 - 2	EAP Request	11.0	1	100%	64	00.008010	00.057906
40	AP1200 - 2	7920	AP1200 - 2	EAP Response	11.0	1	100%	82	00.017285	00.075191
41	AP1200 - 2	7920	AP1200 - 2	EAPOL-Key	11.0	1	100%	97	00.001223	00.076414

119157

Layer 2 roaming with either Static WEP or LEAP provides acceptable QoS using either G.711 or G.729. If LEAP is used, Cisco recommends that you define users locally on the Cisco ACS because using off-ACS databases can result in unpredictable response times, which could adversely affect overall QoS during Layer 2 roaming.

Layer 3 Roaming

Layer 3 roaming occurs when a client moves from an AP that covers one IP subnet to an AP that covers another IP subnet. At that point, the client would no longer have an IP address and default gateway that are valid within the new IP subnet. Because the client's IP address and default gateway are no longer valid, its existing data sessions or voice calls will fail because the remote client can no longer reach the local client.

With the release of the new Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM), the Cisco 7920 phone now supports Layer 3 mobility while using Static WEP. Cisco Centralized Key Management (Cisco CKM) enables the Cisco 7920 phone to achieve full Layer 3 mobility while using LEAP. For details about the Cisco WLSM, refer to the product documentation available at

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/wlsm/index.htm

Note For WLAN deployments in multi-story buildings, where the WLANs on each floor have different subnets, take extra care in the RF site survey to ensure that stations on one floor do not roam to WLANs on floors above or below.

Quality of Service

Quality of Service (QoS) is essential to ensure that voice traffic receives timely and reliable treatment with low delay, low jitter, and little or no packet loss on the network. QoS ensures that voice traffic receives priority treatment when traveling across the network. It is required for both wired and wireless VoIP networks.

The following sections discuss QoS for wireless voice traffic:

QoS for Voice Traffic

Because WLANs operate as a shared medium, QoS is more difficult to achieve on wireless networks than on wired networks because the endpoints on a wireless network do not have dedicated bandwidth for sending and receiving traffic. The following characteristics apply to QoS for voice traffic on a wired network:

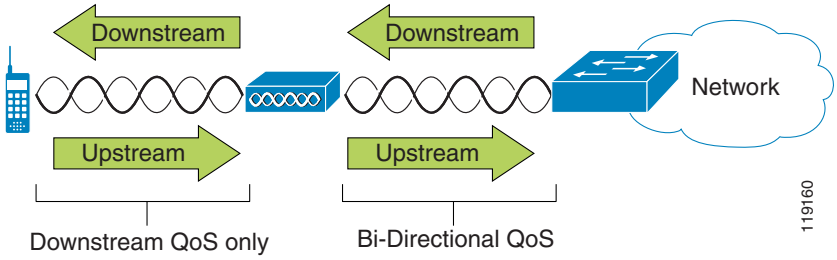
- Dedicated access per user or device (switched ethernet, point-to-point WAN)
- Packets marked with 802.1p and IP Type of Service (ToS) or Differentiated Services Code Point (DSCP)
- QoS can be applied to upstream or downstream traffic
- Can provide complete call admission control

The following characteristics apply to QoS for voice traffic on a wireless network:

- Shared access to bandwidth
- Packets marked with 802.1p and IP ToS or DSCP
- QoS is currently available to downstream traffic from the AP, but few devices other than the Cisco 7920 phone can provide upstream QoS toward the AP.
- Can provide only limited admission control

Unlike wired networks with dedicated bandwidth, WLAN networks have to consider traffic direction when implementing QoS. Traffic is considered as either upstream or downstream from the point of view of the AP, as shown in Figure 6-1.

Figure 6-1 Upstream and Downstream Traffic



WLAN Traffic Transmission

This section describes the following topics pertaining to traffic transmission over a WLAN:

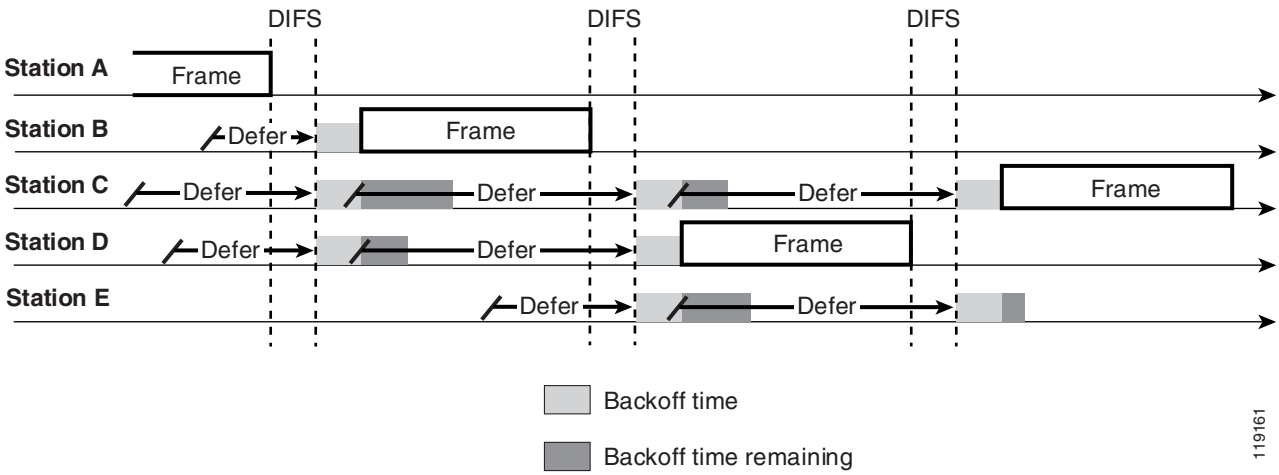
Collision Avoidance

Similar to wired Ethernet networks, 802.11b WLANs employ Carrier Sense Multiple Access (CSMA). However, instead of using collision detection (CD), WLANs use collision avoidance (CA). Instead of each station trying to transmit as soon as the medium is free, WLAN devices use a CA mechanism to prevent multiple stations from transmitting at the same time.

Distributed Coordination Function (DCF)

The model used for WLAN data transmission is called Distributed Coordination Function (DCF), illustrated in Figure 6-2.

Figure 6-2 802.11b DCF Model

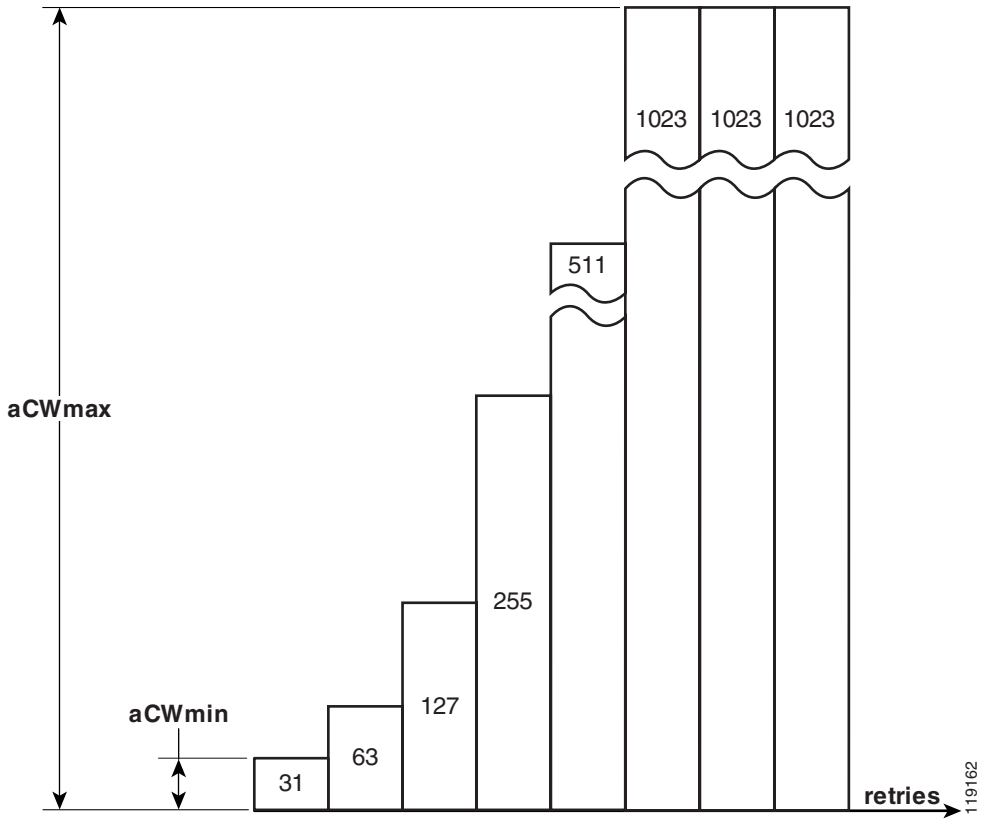


DCF ensures that the following events occur when the endpoints try to transmit data:

1. After the previous frame has been transmitted and detected by the other endpoints, each endpoint waits for a period of time called the inter-frame space (IFS). There are three potential values for the IFS:
   - Short IFS (SIFS) — The shortest interval, used by APs to send acknowledgements and management traffic
   - Point-coordination IFS (PIFS) — Not used by commercial products
   - Distributed IFS (DIFS) — The interval used by most other endpoints
2. After the IFS interval has expired, the endpoints begin their collision avoidance (CA) procedure. This procedure uses two contention window (CW) values, called CWmin and CWmax. The CW determines the additional amount of time an endpoint should wait, after the IFS, before attempting to transmit a packet. The value of the CW is determined by the following procedure:
   a. Each endpoint has the values for CWmin and CWmax defined.
   b. After the IFS expires, the endpoint selects a value between 0 and CWmin. The endpoint then waits the length of this value and determines if the medium is available for transmission.
   c. If the medium is available, the endpoint transmits its packets.
   d. If the medium is unavailable (that is, if another device sent a packet), the endpoint waits until the end-of-packet transmission (from another device) plus the IFS period. In addition, it doubles the value chosen in step "b" and then attempts to transmit.
   e. The endpoint continues to double the value from step "b" until it either reaches CWmax or the packet is transmitted.

Figure 6-3 shows the growth in the random backoff range with retries, as outlined in the preceding steps.

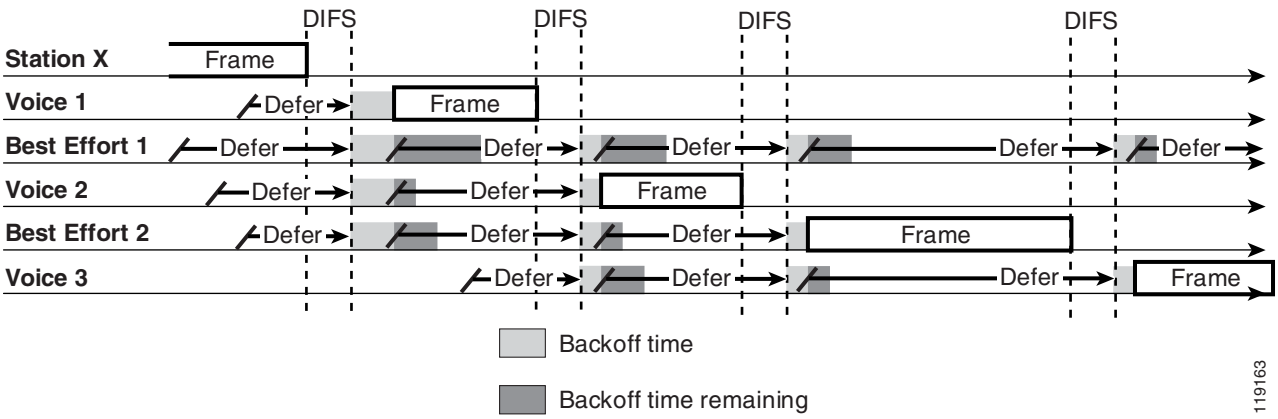
Figure 6-3 Growth in Random Backoff Range with Retries



Enhanced DCF (EDCF)

For WLAN QoS, Cisco APs and 7920 Wireless IP Phones use a technique similar to IEEE 802.11e, called enhanced DCF (EDCF). EDCF enables endpoint devices that have delay-sensitive multimedia traffic to modify their CWmin and CWmax values to allow for statically greater (and more frequent) access to the medium. In practice, EDCF on Cisco WLAN devices works as illustrated in Figure 6-4.

Figure 6-4 802.11b EDCF Model



The default values in Cisco IOS for CWmin and CWmax have been determined as the best possible values for a voice deployment. (Figure 7-7 shows an example of these default values.)

Queues

Beginning with Cisco IOS Release 12.2(11)JA, Cisco Aironet APs support EDCF-type QoS, with up to eight queues for downstream (toward the 802.11b clients) QoS. These queues can be allocated in any of the following ways:

- Based on ToS or DSCP settings of the packets
- Based on Layer 2 or Layer 3 access lists
- Based on VLAN
- Based on dynamic registration of devices such as the Cisco 7920 Wireless IP Phone

Although eight queues are supported on the AP, Cisco recommend that you have only two queues for traffic on the AP to ensure the best possible voice QoS. Voice (RTP) and signaling (SCCP) traffic should be placed into the highest priority queue, and all data traffic should be placed into a best-effort queue. While 802.11b EDCF does not guarantee that voice traffic will be protected from data traffic, using this queuing model should provide the best statistical results for voice QoS.

The Cisco 7920 phones support EDCF-type QoS for upstream (toward the AP) traffic. In addition, the Cisco 7920 phone dynamically announces its presence to the Cisco Aironet AP to ensure that its downstream traffic is placed into the high-priority queue on the AP. This dynamic announcement is done via Cisco Discovery Protocol (CDP). The CDP packets are sent from the Cisco 7920 phone to the AP, and they identify the phone so that the AP can place all traffic to the phone in the high-priority queue.

DSCP Marking

The SCCP signaling messages are marked with DSCP 26 or Per-Hop Behavior (PHB) AF31, and RTP packets are marked with DSCP 46 (PHB EF). These markings match the DSCP markings of Cisco wired Ethernet IP phones and make the QoS settings consistent for both LAN and WLAN environments.

Note The recommended DSCP or PHB marking for voice control signaling traffic has been changed from DSCP 26 (PHB AF31) to DSCP 24 (PHB CS3). A marking migration is planned within Cisco to reflect this change; however, many products (including the Cisco 7920 phone) still mark signaling traffic as DSCP 26 (PHB AF31). Therefore, in the interim, Cisco recommends that both PHB AF31 and PHB CS3 markings be used for access to call signaling queues.

QoS Basis Service Set (QBSS)

In addition to setting the DSCP or PHB markings correctly and supporting EDCF-type QoS, the Cisco 7920 phone also supports an intelligent mechanism to determine the QoS that can be provides by a given AP. This mechanism uses an algorithm that takes into consideration the Received Signal Strength Indicator (RSSI) and the RF channel utilization (CU) based on updates received by the Cisco AP in beacon messages using the QBSS element. Based on this information, the Cisco 7920 phone can determine if the load on a given AP is excessive and if it should attempt to associate with a less congested AP in order to preserve QoS for an IP Telephony call.

Additional Considerations

Beyond providing proper queuing and DSCP (or PHB) markings for the voice packets, you must consider delay and jitter. These factors are especially important for upstream traffic because there is no queuing among clients on the 802.11b side of the AP. The simplest way to reduce delay and jitter is to stay within the guidelines for the number of WLAN clients per AP. Exceeding these guidelines creates additional opportunities to introduce packet delay and jitter.

For more details about deploying QoS in WLAN networks, refer to the Cisco Aironet *Wireless Quality-of-Service Deployment Guide*, available at

http://www.cisco.com

Deployments and Configuration

The following sections describe deployment and configuration steps for the Cisco 7920 Wireless IP Phones and the Cisco Aironet Access Points:

Cisco 7920 Phone Configuration (for Installation)

This section describes how to verify the main configuring settings for the Cisco 7920 Wireless IP Phone.

Gathering Information

Before configuring the Cisco 7920 Wireless IP Phone, it is important to check the phone hardware revision number and firmware version.

Hardware Revision Number

The phone hardware should be Rev 1 or later. You can determine the hardware revision number in one of the following ways:

- By removing the battery and reading the sticker in the phone
- By navigating through the phone menus as follows: **Menu > Phone Settings > Phone Status > Hardware Info**

Any version earlier than Rev 1 indicates a non-production phone and can cause unpredictable problems. Such phones are not supported by Cisco TAC and should be used only for demonstration purposes in the field.

Phone Firmware

The firmware version can be found by navigating through the phone menus as follows: **Menu > Phone Settings > Phone Status > Firmware Info > Firmware Version**. The phone should be running the most current load, which can be found under IP Phones on the Cisco.com Software Download center at

http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser-crypto

Note To be fully compatible with the guidelines in this document, Cisco recommends using the most current version of the firmware for the Cisco 7920 Wireless IP Phone. Cisco also recommends that you frequently check the Cisco.com Software Download site for the latest phone firmware.

Phone Configuration

You can configure Cisco 7920 Wireless IP Phones in either of the following ways:

- By using the keypad on the phone (Refer to the *Cisco Wireless IP Phone 7920 User Guide*.)
- With a PC, by using the Cisco 7920 Configuration Utility and the USB cable (Refer to the *Cisco Wireless IP Phone 7920 Administrator Guide*.)

The documentation for both of these processes is available at

http://www.cisco.com

Configuration Verification

Verify the following settings to ensure that the Cisco 7920 phone works properly:

- Network configuration settings

  The network configuration settings can be verified by navigating to **Menu > Network Config > Current Config**. Check that the DHCP server or static settings (IP Address, Subnet Mask, Primary Gateway, Primary TFTP, and Primary/Secondary DNS) are correct for the associated network.

- Wireless settings

  The wireless settings can be verified by navigating to **Menu > Network Config > 802.11b Configuration**. Check to ensure that the SSID(s) and authentication/encryption type are correct and are for the voice VLAN. If using WEP, verify that the WEP key has been entered correctly (and identically) on both the phone and the AP. If using LEAP, ensure that the username and password are entered identically on both the phone and the ACS (or local LEAP server on a Cisco AP). If authentication fails, Cisco recommends simply re-entering this information on the phone because it is quite easy to enter these values incorrectly.

AP Configuration (for Installation)

This section identifies only the key AP configuration options that are required for optimal voice performance, and it should not to be considered a comprehensive list of configuration options for a production AP. For detailed information and full AP configurations, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*, available at

http://www.cisco.com

The section on Example Configurations for AP and RADIUS Server, page C-1, lists the Cisco IOS text output from the recommended configuration outlined in this chapter.

Note Cisco requires that all APs used with voice calls be either AIR-AP350 Series, AIR-AP1100 Series, or AIR-AP1200 Series. Cisco also recommends that APs used for production run a minimum Cisco IOS release of 12.2.(15)JA.

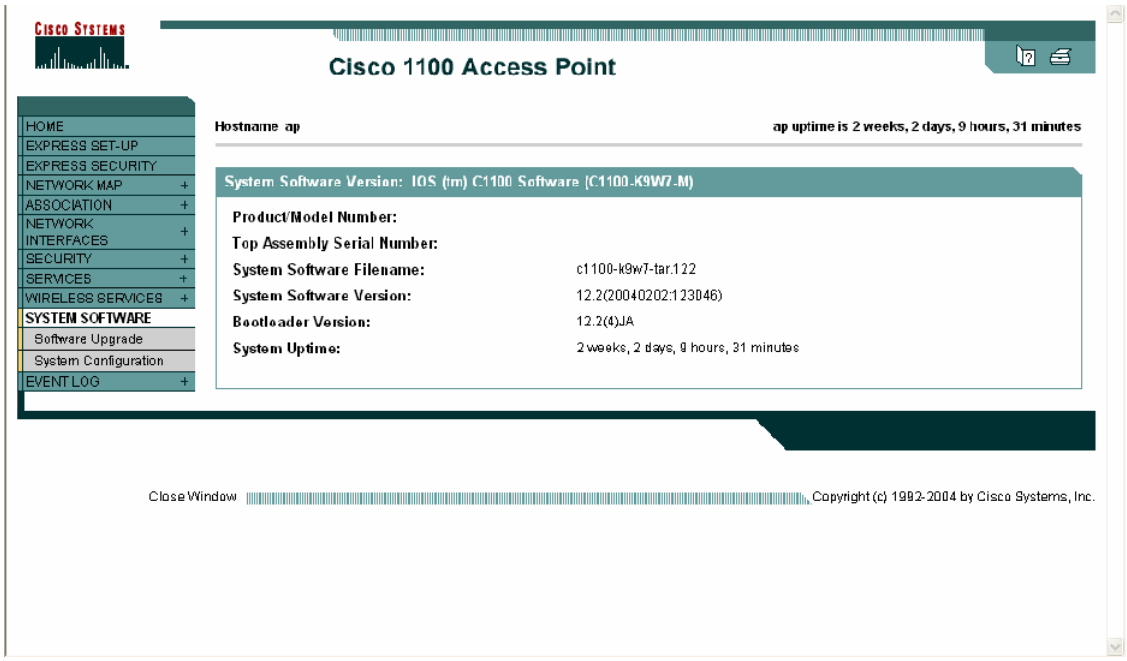
Cisco IOS is required on voice APs because VxWorks will no longer add new features that are required for successful voice deployments, such as Address Resolution Protocol (ARP) caching.

Execute the following configuration steps on the APs. (Figure 7-1 through Figure 7-10 illustrate the web interface of a Cisco IOS AP.)

Step 1 Assign a unique name and unique IP address to each AP. When doing this, note the radio MAC address of the AP in relation to the AP name and IP address. This information will allow for easier identification of APs because almost all site survey tools use radio MAC addresses to identify the APs.

Step 2 Click **System Software** and check the Cisco IOS version of the AP (see Figure 7-1). If it is not the recommended version, update it to the recommended version.

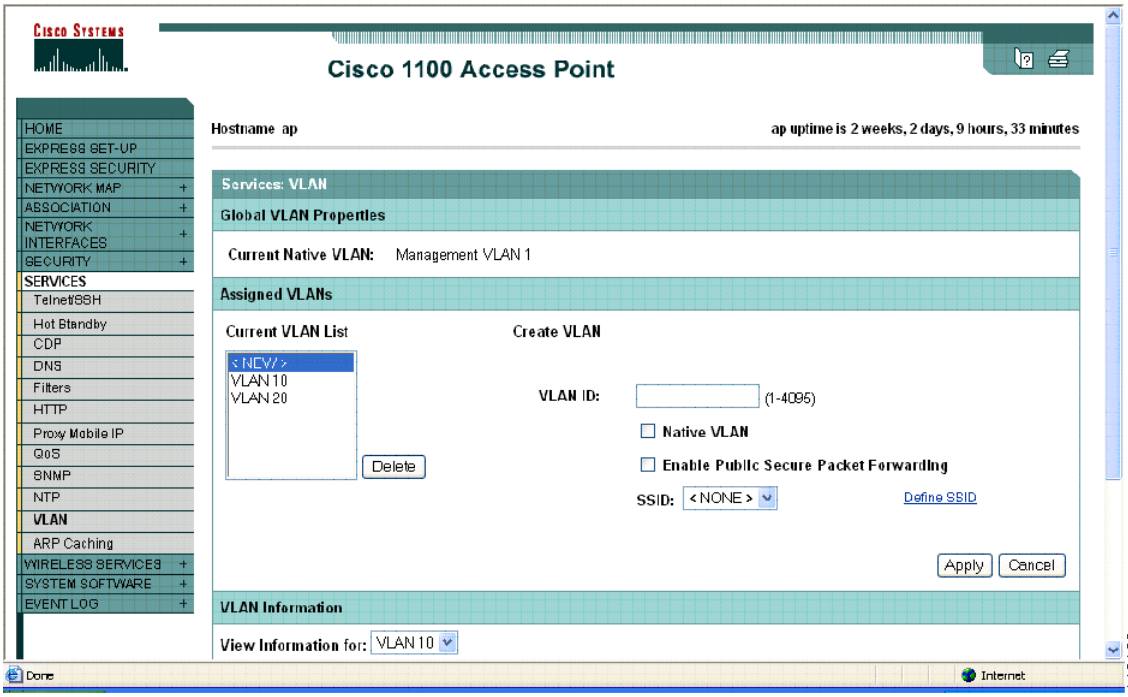
Figure 7-1 AP System Software Version: IOS



Step 3 Cisco recommends separating voice traffic from data traffic through the use of VLANs. Create a minimum of two VLANs. (The VLAN number assigned to the AP must coincide with the wired VLAN number.) One VLAN must be designated as the Native VLAN, which will carry all administrative traffic. This VLAN can also be used to carry data traffic. It must also be identified as the Native VLAN on the switch and can be configured under **Services > VLAN** (see Figure 7-2).

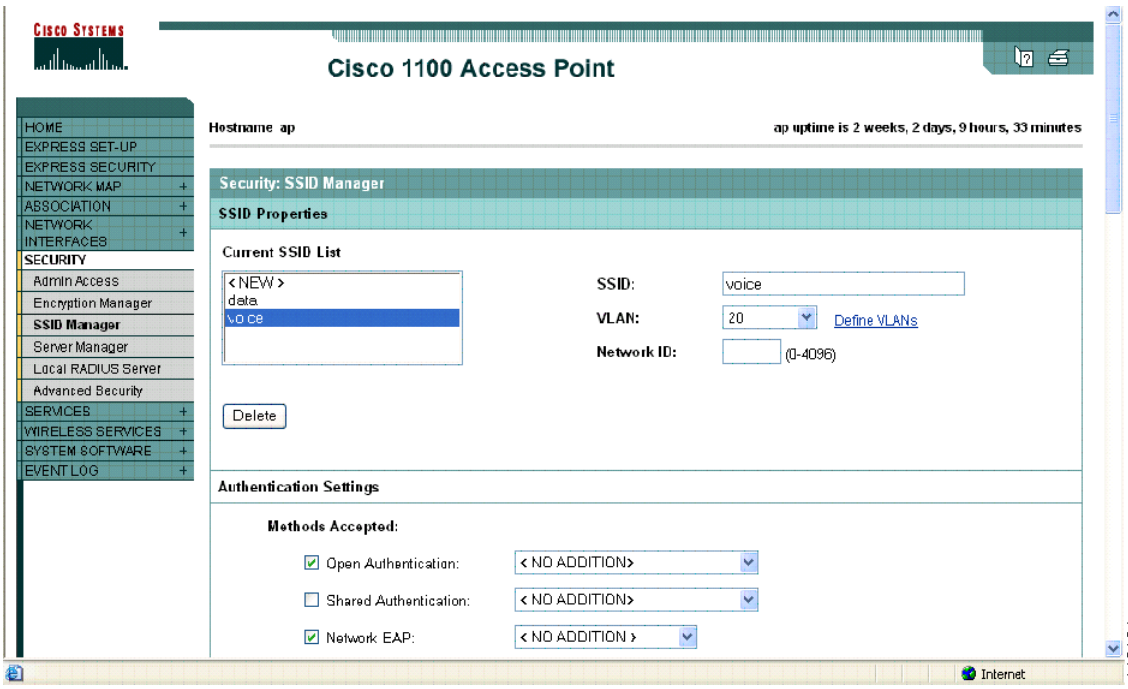
Note Ensure the switch port is properly configured prior to applying AP VLAN configurations. Otherwise, when enabling VLANs, connectivity to the AP via the wired port will be lost until the switch port is properly configured.

Figure 7-2 AP VLAN Configuration



Step 4 Click **Security > SSID Manager** and assign an SSID to each VLAN (see Figure 7-3).

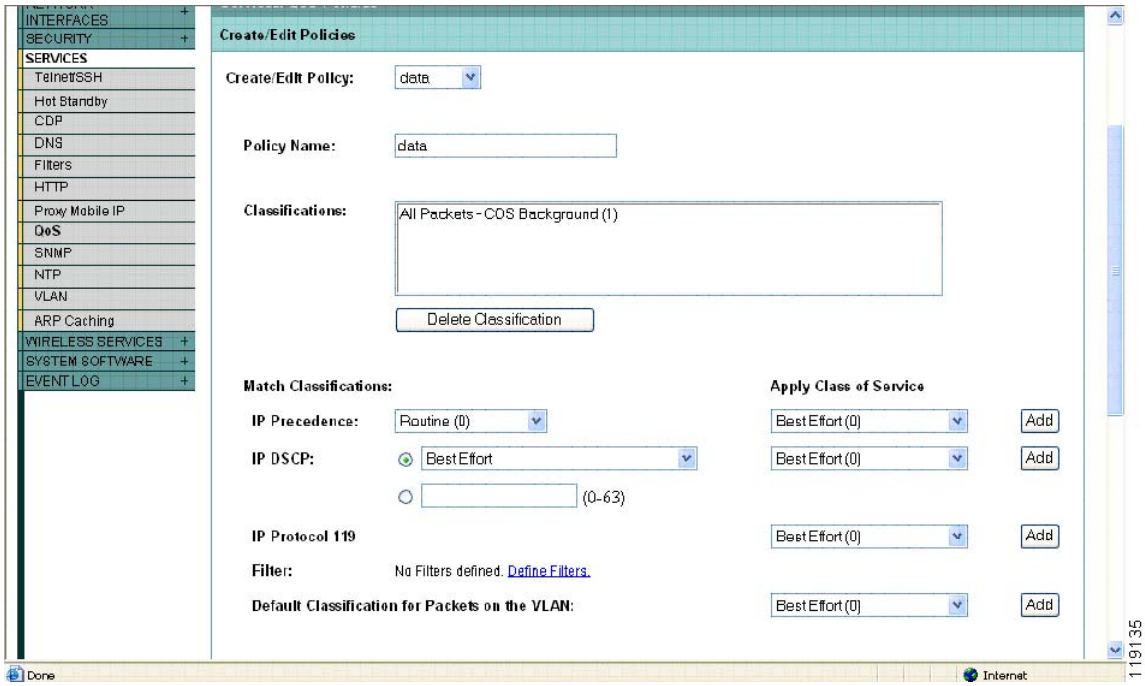
Figure 7-3 AP SSID Configuration



Step 5 The purpose of using data and voice VLANs is to enable specific QoS settings on all traffic on the VLAN. Separating traffic by VLAN and using the "Default QoS for all traffic on a VLAN" frees the AP from having to examine each packet to identify the type of traffic it contains. To apply these settings, click **Services > QoS** (see Figure 7-4).

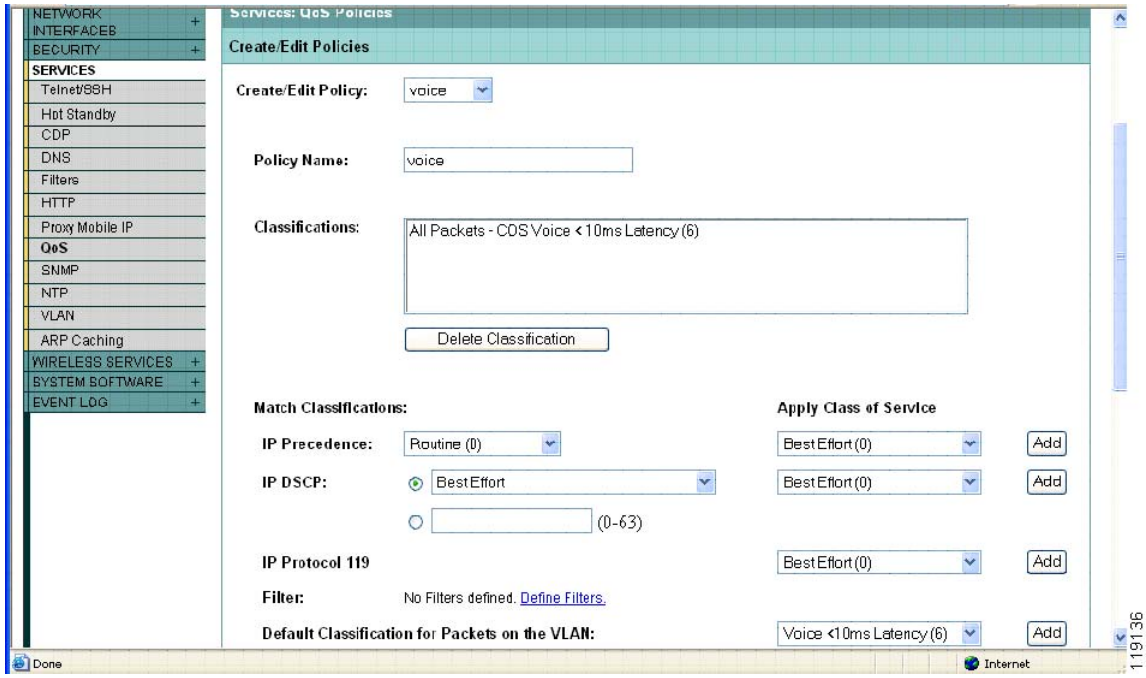
a. Create a policy for data and give it a default CoS value of 0, or Background data.

Figure 7-4 AP QoS Policy Settings Configuration: Data



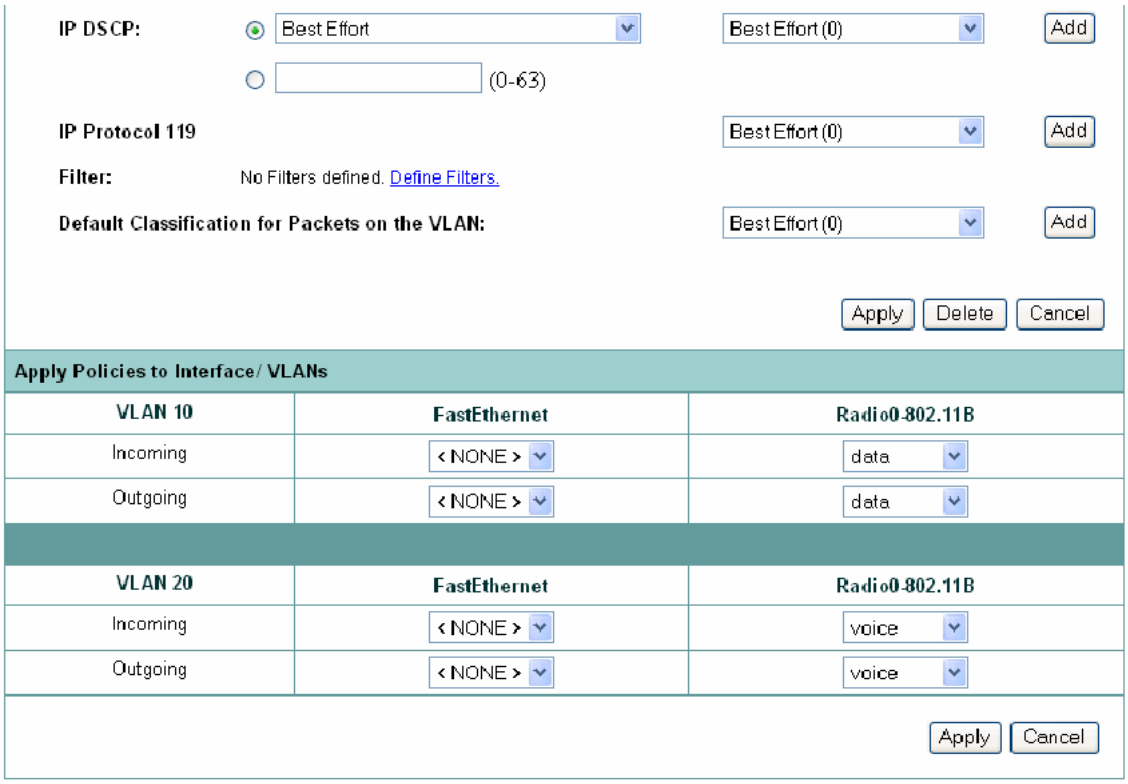
b. Perform the same procedure for a voice VLAN but set the default CoS to level 6, or voice traffic (see Figure 7-5).

Figure 7-5 AP QoS Policy Settings Configuration: Voice



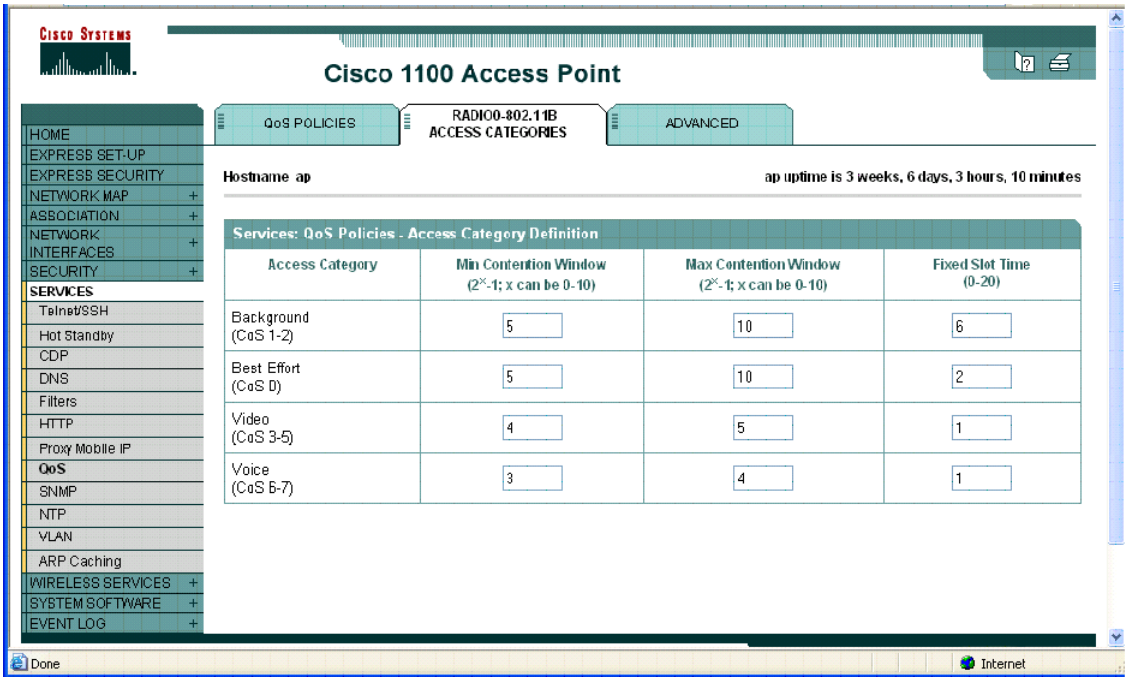
Step 6 After creating the policies in the previous steps, use the same configuration page to apply those policies to the proper VLANs on the radio interface, both incoming and outgoing only (see Figure 7-6). These QoS profiles are not added to the wired interface because that 100-Mbps connection is rarely the bottleneck, and applying the QoS profiles to this interface would put an unnecessary load on the processor.

Figure 7-6 AP QoS Policy Setting Configuration: Assigning Policies to VLANs



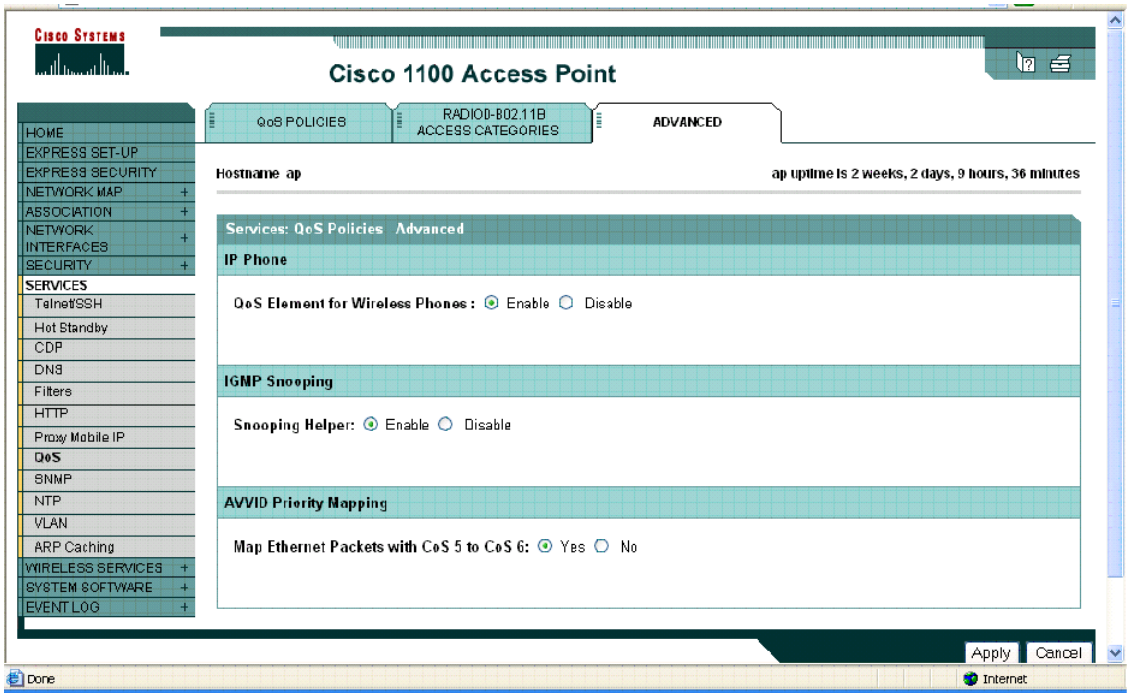
Step 7 Clicking on the tab **Radio-802.11b** (or in some cases 802.11g) **Access Categories** opens a page where you can change the values of these classifications. Cisco recommends that you do *not* change any of these settings. Figure 7-7 shows the defaults values for reference.

Figure 7-7 AP Access Categories Configuration: Contention Window Size (cwMin, cwMax)



Step 8 Under the **Advanced** tab for QoS, ensure that the **QoS Element for Wireless Phones** is enabled (see Figure 7-8).

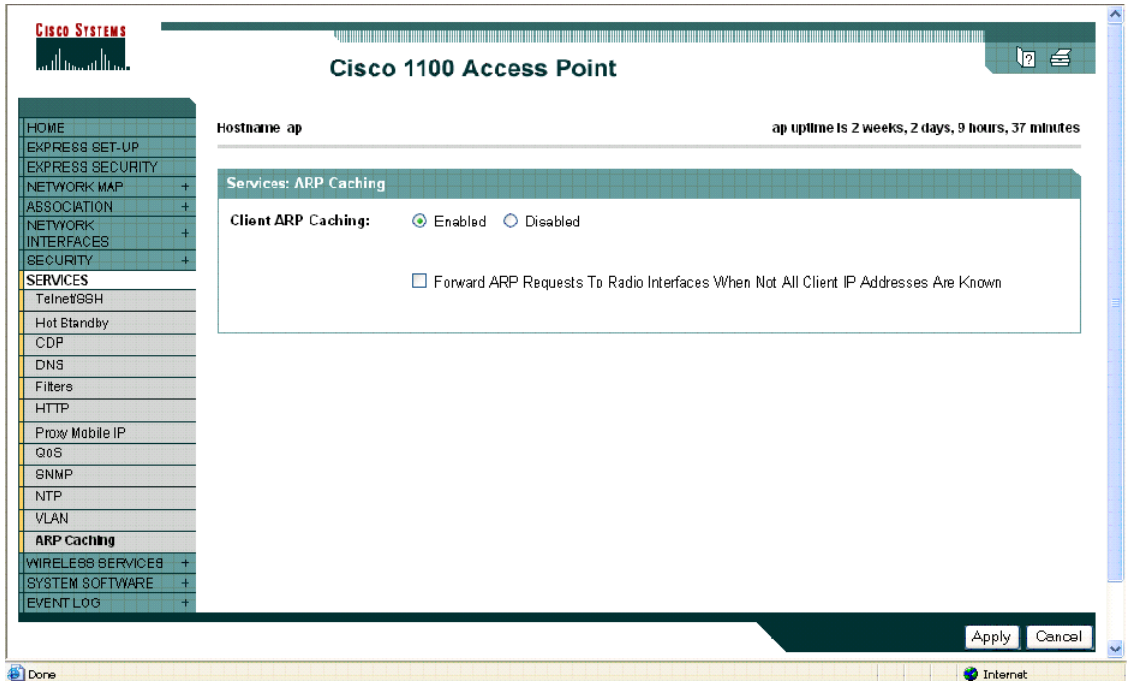
Figure 7-8 AP QoS Element Configuration



Step 9 A common AP configuration error concerns ARP caching. The phones expect this option to be enabled on the AP, but it is disabled be default on the AP. For optimal performance, Cisco recommends enabling ARP caching on the AP, especially when using Wi-Fi devices capable of power management. If you are using Cisco Aironet cards, ARP caching is enabled by default, but you should ensure that this setting has not be changed by any central client management groups. To configure ARP caching on the AP, select **Services** > **ARP Caching** (see Figure 7-9).

Note Cisco highly recommends that you enable ARP caching on all APs.

Figure 7-9 AP ARP Caching Configuration

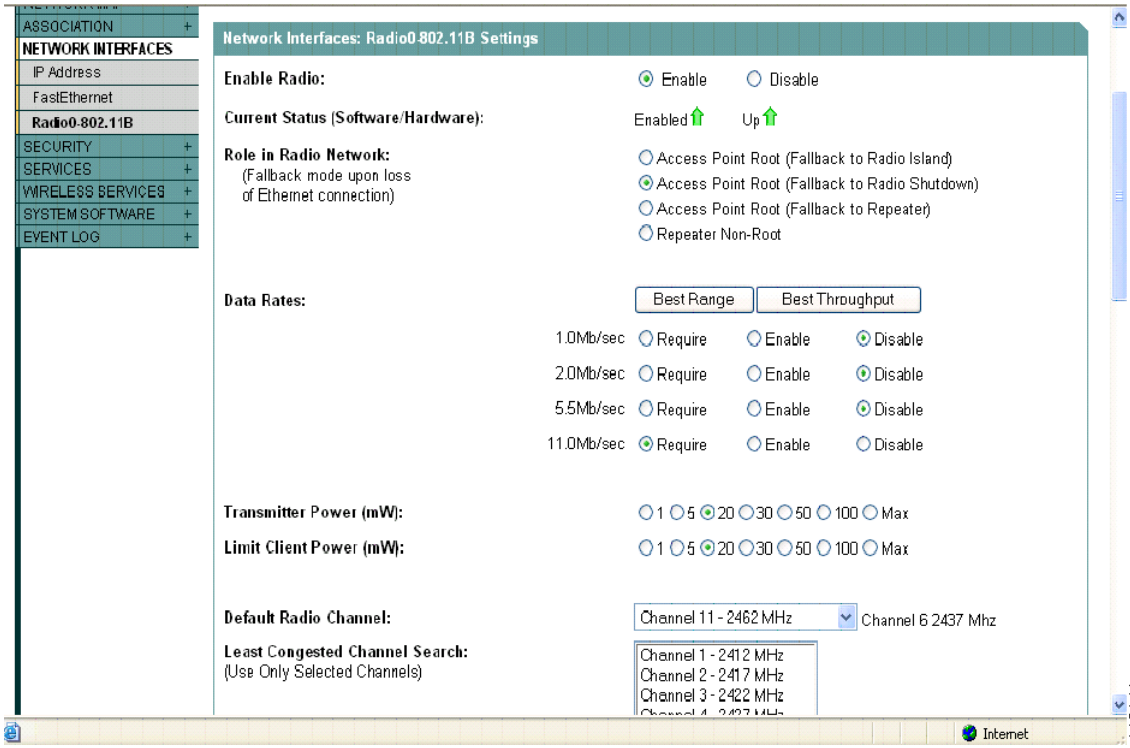


Step 10 When conducting a site survey, it is imperative to adjust the AP channel transmit power and data rates based on the guidelines listed in the chapter on Radio Frequency and Site Survey, page 2-1. These settings can be modified by selecting **Network Interfaces > Radio0-802.11B > Settings** (see Figure 7-10).

Note Cisco highly recommends enabling Dynamic Transmit Power Control (DTPC) on the AP by using the Limit Client Power field in the user interface (or the **power client** command in Cisco IOS) to ensure that the APs and Cisco 7920 phones use the same transmit power to avoid one-way audio. If you are not using a version of the firmware that supports DTPC (such as version 1.0(8) or later), configure the Cisco 7920 phones to use the same transmit power as configured on the APs. If the power of the APs varies, set the transmit power of the Cisco 7920 phones to the same level as configured on the AP with the highest transmit power.

Note Cisco highly recommends that you do *not* use the option to Search for Least Congested Channel but set the channel manually instead.

Figure 7-10 AP Channel Transmit Power Configuration



Step 11 Cisco highly recommends that all deployments use high levels of security on both their data and voice VLANs. For the data VLAN, Cisco highly recommends that you use some type of 802.1x authentication and encryption system. For voice, LEAP and WEP are both currently available. To enhance security on the voice VLAN, you can use wired-side access control lists (ACLs) to limit the traffic to Cisco CallManager and the APs on the voice VLAN.

Step 12 Cisco highly recommends filtering to eliminate any unnecessary traffic that might cause delays in the essential wireless traffic. Although a Cisco AP is capable of performing this task, Cisco recommends that the filtering be performed on a Layer 3 switch connected to the AP because the switch performs the filtering in hardware and significantly reduces the processing time required to perform this task. If no Layer 3 switch is available, the APs can perform Layer 3 filtering, but this task might affect AP performance.

a. Cisco highly recommends that all traffic not required for the AP and RF devices be blocked or filtered at the closest switch. At the AP or switch port, filter all protocols that are not required by the data clients and the voice clients.

For example, unless your wireless data clients are running IBM 3278 terminal emulation, block all Systems Network Architecture (SNA) traffic from the data and voice VLAN. If you are using IBM 3278 data on the data VLAN, then block SNA traffic on the voice VLAN. In many network environments, protocols such as NetBUI, NetWare, and SNA create a large amount of unnecessary wireless traffic that can easily be filtered.

b. The filters for traffic not needed to support WLAN clients should be on all VLANs on the AP.

For example, the radio would send an SNA broadcast packet for each VLAN on the AP. If there are four VLANs on the AP, there is the potential for that packet to be sent four times. If the client is in an area of overlapping AP coverage for the same channel, then the Cisco 7920 phone will see that unusable SNA packet eight times. This type of unnecessary traffic adversely affects voice quality because it consumes bandwidth needed for voice traffic.

Note The section on Example Port Configurations for Voice Operations, page D-1, identifies many of the key packet types needed for the Cisco 7920 Wireless IP Phone.

c. While Ethernet switch ports can transmit and receive at 100 Mbps, 802.11b APs have a throughput of only 11 Mbps (about 7 Mbps of actual throughput) or less through the RF port. Because of the bursty nature of some network traffic, this throughput mismatch means that the AP will have to drop packets, thus adding excessive processor load to the AP. An alternative is to configure the first-hop switch to drop these packets using policing and rate limiting features. Thus, the switch port to which the AP is connected can be rate-limited to a throughput of 11 Mbps or less.

If you are using a Cisco Aironet AP equipped for 802.11g or 802.11a, increase the rate limit to the total throughput of the RF ports, as follows:

- 802.11g = 54 Mbps (about 22 Mbps of actual throughput)
- 802.11a + 802.11g = 100 Mbps (no rate limiting necessary)
- 802.11a + 802.11b = 64 Mbps (about 42 Mbps of actual throughput)

Step 13 Optionally, you can filter all video prioritized traffic at the switch so that it cannot be sent to the APs. The number of calls per AP has been characterized without video prioritized traffic on the network. Prioritized video traffic (those packets marked with CoS in the range of 3 to 5, inclusive) significantly diminishes the call capacity of an AP because it is granted access to the wireless media at a higher priority than best-effort data.

Step 14 If there are 802.11g APs in the network, then the 802.11g protection mechanism must be enabled to make sure that 802.11b clients (such as the Cisco 7920 phone) do not have packet collisions with 802.11g packets. This protection mechanism is enabled automatically on the AP if the 802.11b data rates are enabled.

Wireless IP Telephony Verification

After conducting an RF site survey and configuring the APs and the phones, it is crucial to conduct verification tests to ensure that everything works as desired. These tests should be performed at all of the following locations:

- The primary area of each AP cell (where the phones will most likely connect to that particular AP)
- Any location where there might be high call volume
- Locations where usage might be infrequent but coverage still has to be certified (for example, stairwells, restrooms, and so forth)
- At the fringes of the AP's coverage area

These tests can be performed in parallel or series. If performed in parallel, ensure that phones are powered off between testing points to test full association, authentication, and registration at each location. Roaming and load tests must, of course, be the final tests.

The following sections discuss various wireless network techniques:

Association, Authentication, and Registration

The following sections explain how to verify that the Cisco 7920 Wireless IP Phone is associating, authenticating, and registering properly.

Association

At multiple points throughout the environment, power-up the phone and verify association with the AP. If the client does not associate with the AP, perform the following checks:

- Check the phone configuration to ensure proper SSID, authentication type, and so forth.
- Check the AP configuration to ensure proper SSID, authentication type, radio channels, and so forth.
- Check your site survey to ensure the location has adequate RF coverage.

Authentication

At multiple points throughout the environment, ensure that the phone authenticates through the AP successfully. If the client does not authenticate, perform the following checks:

- Check either the WEP key or the LEAP username and password on the phone.
  - If these entries are incorrect, retype them on the phone.
  - If using domains, enter the username as *domain\username*.
- Check either the WEP key or the security configurations on the AP.
- Check the username and password on the AAA server by using a wireless laptop with identical credentials.

Registration

At multiple points throughout the environment, ensure that the phone registers with Cisco CallManager and receives the proper phone number. If the client does not register, perform the following checks:

- Check the Cisco CallManager settings. (Is the phone configured in Cisco CallManager?) You can use a wired IP phone to test the Cisco CallManager configurations.
- Verify that the phone has the correct IP Address, Subnet Mask, Primary Gateway, Primary TFTP, Primary/Secondary DNS, and Cisco CallManager information.
- Use the Trace Route function (see Advanced Cisco 7920 Commands, page A-1) to check connectivity between the phone and Cisco CallManager, gateway, and so forth.

Phone Calls and Load Testing

The following sections explain how to verify that calls can be placed successfully from the Cisco 7920 Wireless IP Phone with acceptable voice quality.

Stationary Phone Calls

At multiple points throughout the environment, while standing still, make a phone call to a wired phone and conduct 60 to 120-second voice tests to check voice quality. If the voice quality is unacceptable, perform the following checks:

- If you make a call using the wired phone, is the voice quality acceptable? If not, verify the wired network design against the guidelines listed in the *Cisco IP Telephony Solution Reference Network Design (SRND)*, available at

  http://www.cisco.com/go/srnd
- Use the site survey tools to verify that there is no more than one AP per RF channel from that location with a signal strength (RSSI) greater than 35. If there are two APs present on the same channel, ensure that the signal-to-noise ratio (SNR) is as high as possible to minimize interference. For instance, if the stronger AP has an RSSI of 35, ideally the weaker AP should have an RSSI of less than 20. To achieve this goal, you might have to reduce one AP's transmit power or move the AP.
- Check the QoS settings on the AP to confirm proper recommended settings.

Roaming Phone Calls

Place a call to a wired IP phone and continually check voice quality while traversing the total wireless coverage area. Cisco recommends using an earpiece so that you can test the voice quality while still looking at the site survey information on the phone. If the voice quality is insufficient, perform the following checks:

- Listen for all unacceptable changes in voice quality and take note of the values in the phone's site survey.
- Watch and listen for the phone to roam to the next AP.
- Note the other available APs in the site survey to check coverage and interference.

Make adjustments to AP placement and settings to fine-tune the WLAN, and perform the following checks to ensure voice quality:

- Using the site survey tools, verify that there is no more than one AP per channel with an RSSI value greater than 35 in any given location. Ideally, all other APs on the same channel should have RSSI values as low as possible (preferably less than 20). At the border of the coverage area where the RSSI is 35, the RSSI for all other APs on the same channel should ideally be less than 20.
- Use the site survey tools to verify that there are at least two APs (total, on separate channels) visible in all location with sufficient signal strength.
- Check that the APs in a given roaming area are all on a Layer 2 network.

Load Testing

Gather a sampling of all the planned wireless phone users, and equip them with Cisco 7920 Wireless IP Phones. Have seven users begin by making phone calls in a given area. Then have users start to move apart while placing new calls. Continue to check voice quality during this process.

Ongoing Verification

The RF environment will constantly be changing as the number of users increases, types of applications being used changes, and physical changes are made to the environment.

- Periodically check for acceptable environmental conditions (see Overview of Cisco Wireless IP Telephony, page 1-1), especially in the beginning as you ramp up for full deployment. Pay particular attention to QBSS or AP channel utilization, which will typically be low during a site survey but will increase as more users are added to the wireless network.
- Also continually checking for rogue APs and other sources of RF noise that can interfere with production operations. These issues can occur at any time and must be monitored continually and mitigated quickly. Through the use of the Cisco Structured Wireless-Aware Network (SWAN) architecture, Cisco provides automated tools for detecting rogue APs and 2.4 GHz (non-802.11) noise. For more information about Cisco SWAN, refer to the documentation available at

  http://www.cisco.com

Troubleshooting the Cisco 7920 Phone

The following sections describe many of the issues and problems that can arise in a Cisco Wireless IP Telephony network, along with recommended solutions for each issue:

Heat Issues

The Cisco 7920 Wireless IP Phone can get warm at times, but it is well within acceptable temperature levels and meets all compliance regulations. Heat is produced when a call is in progress or if the phone is constantly scanning for new APs in the case of a poor RF signal or at the border of RF coverage. To reduce the amount of heat generated, you can perform the following optimizations:

- Calls in progress

  Lowering the RF output power on the phone will reduce heat but can also affect voice quality. The correct RF setting must be determined on a site-by-site basis.

- Constant scanning for a new APs

  If the phone is constantly going on and off the network or scanning for channels while not associated with an AP, heat will be generated as if the phone is on an active call. In this case, adjust the RF coverage to provide a more stable environment.

Switch Issues

If a Cisco Catalyst 4000 Series Switch is used as the main Layer 3 switch in the network, ensure that it contains, at a minimum, either a Supervisor Engine 2+ (SUP2+) or Supervisor Engine 3 (SUP3) module. The SUP1 or SUP2 module can cause roaming delays.

The Cisco Catalyst 2948G, 2980G, 2980G-A, 4912, and 2948G-GE-TX switches are also known to introduce roaming delays. Cisco does *not* recommend using these switches in a wireless voice network.

DHCP Errors

You can power-cycle the phone to release and renew the phone's Dynamic Host Configuration Protocol (DHCP) settings. The following notes also apply to DHCP:

- Loss of RF will not release the DHCP settings unless a time-out state has been reached.
- Phone firmware version 1.0(5) and later gives precedence to Option 150.
- The phone might associate with the AP but be unable to obtain an IP address from the network. In this case, check the WEP key settings. The phone uses the following process:
  1. Authenticate (WEP or LEAP)
  2. Associate with the AP
  3. Obtain an IP address.
- Ensure that Temporal Key Integrity Protocol (TKIP) and Message Integrity Check (MIC), or Cisco KIP and Cisco MIC, are not enabled for the voice VLAN Service Set Identifier (SSID) on the AP. These features are not supported on the Cisco 7920 Wireless IP Phone.

Phone Firmware Upgrade Failure

All firmware versions after 1.0(6) have mechanisms in place to prevent the firmware from getting corrupted and the phone from being unable to boot successfully. Firmware can be upgraded via TFTP from Cisco CallManager or via USB through the Cisco 7920 Configuration Utility.

If there is a failure or power is lost during an upgrade, you will have to use the Configuration Utility to recover the phone. Perform the following steps in this scenario

1. Boot the phone while holding down the power key, **END(!)**, and **#** at the same time. You will be prompted for a USB connection.
2. The Configuration Utility will prompt you to browse to the phone firmware on the PC. The latest firmware can be downloaded from the Software Center on Cisco.com.

Phone Firmware Downgrades after Cisco CallManager Upgrade or Patch

If a Cisco CallManager patch is applied that is older than the current running firmware, the phones might automatically downgrade to the load contained in the patch. Check 7920 device default image in Cisco CallManager and the OS7920.txt file in the TFTP folder to fix this issue.

Active and Standby

The Cisco 7920 Wireless IP Phone can be in either active and standby mode. Active mode occurs when there is an active call or a scheduled event to send Cisco Discovery Protocol (CDP) or keep-alive packets. To maximize battery life and talk time, the Cisco 7920 Wireless IP Phone goes into standby mode after a minute or so of idle time in a stable RF environment. The phone enters standby mode every 2 seconds after an active scan is completed. The phone will not enter standby mode with an active RTP stream. The following events also cause the phone to awake from standby mode:

- Key activity
- Roaming
- Power cycling
- Loss of network connectivity
- Loss of RF connectivity
- Scheduled CDP or keep-alive packets

If a phone is in an unstable RF environment, it will remain in active mode and scan constantly.

Battery Life

The following types of batteries are available for the Cisco 7920 Wireless IP Phone:

- Standard 1560 mA lithium ion, with an average battery life of 3.5 hours talk-time or 21 hours standby
- Extended 1960 mA lithium ion, with an average battery life of 4.25 hours talk-time or 30 hours standby

Active call time will reduce the standby time.

Consider the following points with regard to battery life:

- An unstable RF environment affects battery life. If the phone is never able to enter standby mode because of continuous roaming or scanning, battery life will be greatly reduced. When leaving an area of coverage, shut down the phone to preserve battery life.
- Vibrate mode can reduce battery life.
- The background light should not affect battery life.
- Lithium ion batteries do not exhibit memory effects. Partial charges decrease the talk time for that charge but do not damage the battery.
- Batteries stop charging once they are fully charged. It is acceptable to leave batteries in the charger for extended periods of time.
- Batteries should be able to handle over 4000 recharges.
- Higher phone transmit power also affects battery life.

Configuration Utility Issues

Consider the following points when using the Cisco 7920 Configuration Utility:

- USB must be enabled on the Cisco 7920 Wireless IP Phone for it to be recognized by Microsoft Windows. You can enable USB through the keypad by selecting **Menu > Phone Settings > USB Enable/Disable**.
- Do not assign a static address to the network interface called Cisco 7920 USB. It will receive an IP address automatically from the Cisco 7920 Configuration Utility. Static addressing can cause the utility to fail.
- You must select a ring tone when configuring the phone via the Configuration Utility, otherwise the phone will have no ring tone until one is configured manually.
- If using the 192.168.1.x network for the PC where you are running the Configuration Utility, disable the Ethernet interface when using the Configuration Utility because it could cause a conflict with the USB interface for configuring the phones.

Note Ensure that USB is disabled on the phone after using the Configuration Utility; leaving it enabled could cause IP network connectivity issues.

Common Roaming Issues

The following roaming issues can occur with the Cisco 7920 phone:

- Phone does not roam when placed directly under AP
  - Phone is most likely not reaching the roaming differential thresholds for the received signal strength indicator (RSSI) and channel utilization (CU). Adjust the power settings on the APs.
  - Phone is not receiving beacons or probe responses from AP.
- Phone roams too slowly
  - Make sure the Cisco 7920 Wireless IP Phone has another acceptable AP as a roaming option in the phone's site survey. The next AP ideally should have an RSSI value of 35 or higher for roaming.
  - Check the Cisco Catalyst 4000 Series Switch. Supervisor Engine 2 (SUP2) modules can cause significant delays; upgrade to SUP2+ or SUP3 instead.
- Phone loses connection to Cisco CallManager when roaming
  - Check authentication for a possible WEP mismatch.
  - The phone is capable of seamless Layer 2 roaming only (unless WLSM is configured), so ensure that the new AP is not serving a different IP subnet.
  - If using LEAP, check that TCP ports are not blocked by filters on the AP. Port 1645 is used for the Access Control Server (ACS), and port 1812 is used for other RADIUS servers.
  - Verify that the associated AP has IP connectivity to Cisco CallManager.
  - Check RF signal strength.

- Phone looses voice quality while roaming
  - Check for low RSSI on the destination AP.
  - Channel overlap might be insufficient. The phone must have time to hand off the call smoothly before it loses its signal with the original AP.
  - The signal from the original AP might be lost.

Audio Problems

There are a few common configuration errors that can cause some easily resolved audio issues. If possible, check audio problems against a wired phone to help narrow the problem to a wireless issue. Common audio problems include:

- No audio
  - A common reason for no audio is that TKIP and/or MIC are configured on the AP. These features are not yet available for the Cisco 7920 Wireless IP Phone and can cause audio issues if enabled.
- One-sided audio
  - This problem can occur in the fringe areas of an AP, where a signal might be too weak on either the phone side or the AP side. Matching the power settings on the phone and the AP, when possible, can fix this problem. This problem is most common when the variation between the AP setting and the phone setting is large (for example, 100 mW on the AP and 20 mW on the phone).
  - Check the gateway and IP routing for voice quality.
  - Check to see if a firewall or NAT is in the path of the RTP packets. By default, firewalls and NATs cause one-way audio or no audio. Cisco IOS and PIX NATs and firewalls have the ability to modify those connections so that two-way audio can flow.
  - One-way audio can occur if ARP caching is not configured on the AP. Refer to the section on AP Configuration (for Installation), page 7-2, for information on how to set this feature.
- Data rate settings
  - If there is a specific data rate set on the phone or AP, then they must match or the phone must be set to its default of automatic.
- Hardware issues
  - To make sure the speaker is functioning properly, first check the volume settings under the selected profile, then enable keypad tones to check the speaker.
  - For additional speaker issues, refer to Field Notice 29257, available at

    http://www-tac.cisco.com/Support_Library/field_alerts/fn29257.html
- Ring volume too low
  - Louder ring tones (such as loudlaser.raw) are available on Cisco.com. Loud ring tone must be downloaded via TFTP with Cisco CallManager and not with the Configuration Utility.

Registration and Authentication Problems

When encountering problems with authentication, perform the following checks:

- Check SSIDs to make sure they match on the phone and the AP (or network). Also be sure the network has a route to Cisco CallManager.
- Check the WEP keys to make sure they match. It is a good idea to re-enter them on the Cisco 7920 Wireless IP Phone because it is quite easy to make a typing error when entering a WEP key or password.

The following messages or symptoms can occur:

- Registration Rejected

  This error is most likely a Cisco CallManager issue. You will either have to manually configure the phone in Cisco CallManager or enable auto-registration.

- Cisco Wireless IP Phone 7920 shows up as Cisco IP Phone 7960 in Cisco CallManager

  Prior to Cisco CallManager Release 3.3(3) SR1, the phone device ID is shown as 7960. To correct this issue, upgrade the Cisco CallManager software and delete and reconfigure the phones as 7920s.

- Cannot support all Requested Capabilities

  The most likely cause of this error is that TKIP and/or MIC is configured on the associated AP on the voice VLAN. Remove these settings because this functionality is not yet supported on the Cisco 7920 Wireless IP Phone.

- Authentication Failed, No AP found
  - Cisco Centralized Key Management (Cisco CKM) and Cipher suites might be enabled. These features are not supported.
  - Check WEP keys or LEAP username and passwords.

- No service, IPconfig Failed

  This is usually a problem with the connection to the DHCP server. Make sure the phone is able to receive an IP address. Also check encryption.

- Cisco CallManager shows up as TFTP_AS_CM in the current phone configuration

  This error indicates the phone is attempting to connect to the TFTP server but is not getting the correct TFTP responses.

- LEAP Password Prompt

  The setup configuration for some AAA servers might require a fully qualified username if integrated with a Microsoft Windows server. If so, you might have to enter the LEAP username in the format

  domain/username

Non-Cisco Access Points

Cisco 7920 Wireless IP Phones are supported only with Cisco APs, but they will work with any Wi-Fi compliant AP. The following functions are still available with non-Cisco APs:

- Roaming
- Static WEP
- Upstream wireless QoS (7920-to-AP) via lower CWmin and CWmax

The following functions are *not* available with non-Cisco APs that are not Wi-Fi compliant:

- LEAP
- Downstream QoS (two queues)
- QoS Basis Service Set (QBSS) load
- Cisco Discovery Protocol (CDP)
- Dynamic Transmit Power Control (DTPC)

Clock Issues

Occasionally the time or date is incorrect on the phone even though it is correct on Cisco CallManager. Because the Cisco 7920 Wireless IP Phone updates its time and date when it uses TFTP to download its configuration, resetting or power-cycling the phone will correct this problem

VxWorks-to-IOS Conversion

The QoS contention window values might not be set to the standard default settings after a migration from VxWorks to Cisco IOS. Make sure Cisco IOS defaults are configured on the newly migrated AP. (Figure 7-7 shows these default values.) In addition, a number of settings have been known to get corrupted during use of the automated conversion migration tool. Cisco highly recommends that you reset the AP to factory defaults after the conversion and begin all configurations from the factory defaults.

Advanced Cisco 7920 Commands

This section describes special functions that can be used to troubleshoot the Cisco 7920 Wireless IP Phone.

Hidden Phone Menu

There are several settings on the phone that are hidden and can be used only for troubleshooting the phone. Keep in mind that most of these settings can be changed only temporarily and will return to their default values once the phone is power-cycled.

Note If the deployment has moved past the design and testing stages and is into actual production use, do not use these hidden or special options; instead, perform all configurations using the standard menu options.

To access the hidden features, enter **Menu** > * > # > # > **Send**.

The following options are available on the hidden phone menu:

Phone Settings Menu

Menu Option	Description
Power Save[1]	Disabling Power Save temporarily takes the phone out of power-save mode.
WDOG Enable/Disable[1]	This option toggles the Watchdog on or off. (It is enabled by default.) The Watchdog is an error recovery mechanism that sends a reboot message when an error is encountered.

1. These settings can be changed only temporarily.

Network Config Menu

Menu Option	Description
CDP TX Enable/Disable	This option turns Cisco Discovery Protocol (CDP) on or off.
CDP TTL	This option is the CDP Time To Live (TTL) setting. The default is 180 seconds.

Menu Option	Description
CDP TX Interval	This option changes the interval for the transmission of CDP packets.
Trace Route	This option can be used to trace the path of a packet from the phone. Enter the IP address of Cisco CallManager as the destination address, and the trace will show the number of hops required to reach Cisco CallManager, the IP address of each hop, and the final success of the trace.

Wireless Settings Menu

Menu Option	Description
Data Rate	The default for this setting is **automatic**. Statically setting this option to a value lower than 11 mbps will reduce the voice quality of the phone and reduce the number of concurrent phones calls that the AP can handle. The setting here must match the settings on the AP.
Transmit Power	This option changes the transmit power of the phone. 20 mW is the default.

Roaming Menu

Menu Option	Description
Scan[1]	This option disables the phone from scanning for APs.
Channel Improvement[1]	This option disables roaming.
RSSI Threshold[1]	This option sets the RSSI threshold. The default is 5.
QBSS Threshold[1]	This option sets the QBSS threshold. The default is 45.
RSSI Diff Thld[1]	This option is the change in relative signal strength needed for a roam to occur. The default is 15.
QBSS Diff Thld[1]	This option is the change in channel utilization needed for a roam to occur. The default is 15.
O-channel RSSI Thld[1]	This option is the RSSI value needed to change an overlapping channel to an active channel. The default is 30.
A-I-channel Scan Freq[1]	This is the amount of time in seconds that the phone will scan the indicated channels. The default varies by channel type, as follows: • A Channel List — 2 seconds for each channel on which the phone sees an AP transmitting • Non-Overlapping Channel List — 6 seconds per channel • Overlapping Channel List — 60 seconds per channel • Incompatible Channel List — 300 seconds per channel
Active Scan Time[1]	The default is 10 ms.
Passive Scan Time[1]	The default is 110 ms.
Handoff[1]	This option disables the phones ability to roam. The default is yes.
A-I_channel list[1]	This option displays the channels in each category.

1. These settings can be changed only temporarily.

Lost Phone Password

If a phone is locked and the password is lost, please contact Cisco TAC for help.

Site Survey RF Recommendations

This section provides additional details about voice site surveys that are crucial for a successful deployment, and it includes additional information on RF and antenna patterns and behavior.

AP and Antenna Placement

This section gives examples of both proper and improper placement of access points (APs) and antennas.

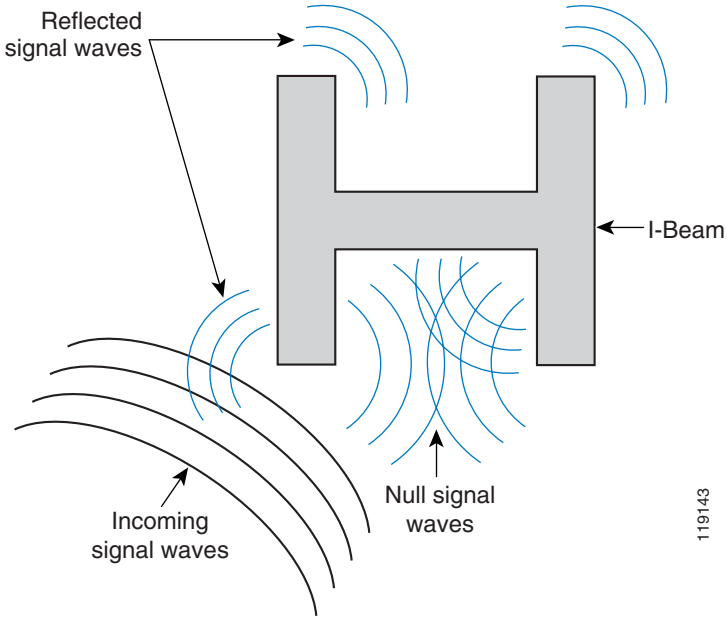
Improper AP and Antenna Placement

Figure B-1 shows improper placement of an AP and antennas close to an I-beam, which creates distorted signal patterns. An RF null point is created by the crossing of signal waves, and multipath distortion is created when signal waves are reflected. This placement results in very little coverage behind the AP and reduced signal quality in front of the AP.

Figure B-1 Improper Placement of Antennas Near an I-Beam

Figure B-2 shows the signal propagation changes or distortions caused by an I-beam. The I-beam creates many reflections from both received packets and transmitted packets. The reflected signals result in very poor signal quality because of null points and multipath interference. However, the signal strength is high because the AP antennas are so close to the I-beam.

Figure B-2 Signal Distortions Caused by Placing the Antennas Too Close to an I-Beam

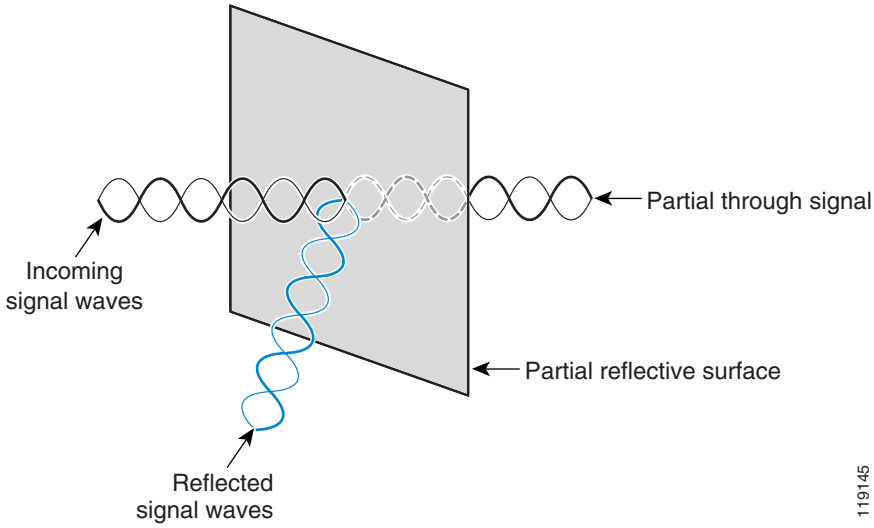


The AP and antenna placement in Figure B-3 is better because it is away from the I-beams and there are fewer reflected signals, fewer null points, and less multipath interference. This placement is still not perfect because the Ethernet cable should not be coiled up so close to the antenna.

Figure B-3 AP and Antennas Mounted on a Wall, Away from I-Beams

Figure B-4 shows the signal propagation caused by the wall on which the AP is mounted.

Figure B-4 Signal Reflection Caused by a Wall



The preceding examples also apply when placing APs and antennas in or near the ceiling in a standard enterprise environment. If there are metal air ducts, elevator shafts, or other physical barriers that can cause signal reflection or multipath interference, Cisco highly recommends that you move the antennas away from those barriers. In the case of the elevator, moving the antenna a few feet away will help eliminate the signal reflection and distortion. The same is true with air ducts in the ceiling.

Conclusion

A survey conducted without sending and receiving packets is not sufficient. The I-beam example shows the creation of null points that can result from packets that have CRC errors. Voice packets with CRC errors will be missed packets that adversely affect voice quality. In this example, those packets could be above the noise floor measured by a survey tool. Therefore, it is very important that the site survey not only measures signal levels but also generates packets and then reports packet errors.

Proper AP and Antenna Placement

Figure B-5 shows a Cisco AP1200 properly mounted to a ceiling T-bar, with the antennas in an omni-directional position.

Figure B-5 Cisco AP1200 Mounted to a Ceiling

Figure B-6 shows a Cisco Aironet 5959 omni-directional diversity antenna properly mounted to a ceiling T-bar. In this case, the Cisco AP1200 would be mounted above the ceiling tile.

Figure B-6 Cisco Aironet 5959 Antenna Mounted to a Ceiling

Figure B-7 shows a Cisco AP1200 properly mounted to a wall.

Figure B-7 Cisco AP1200 Mounted to a Wall

Figure B-8 shows the Cisco Aironet 2012 diversity patch antenna mounted to a wall. In this case, the Cisco AP1200 would be mounted above the ceiling tile.

Figure B-8 Cisco Aironet 2012 Antenna Mounted to a Wall

For areas where user traffic is high (such as office spaces, schools, retail stores, and hospitals), Cisco recommends placing the AP out of sight and placing unobtrusive antennas below the ceiling.

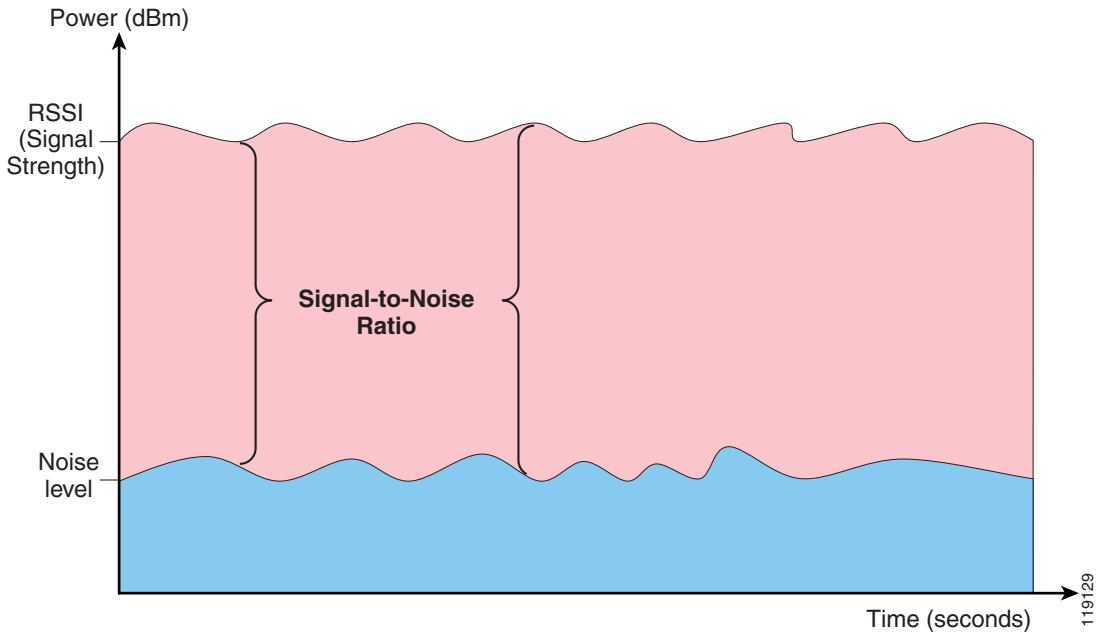
Interference and Multipath Distortion

The throughput performance of the WLAN network is affected by unusable signals.

WLAN interference can be generated by microwave ovens, 2.4 GHz cordless phones, Bluetooth devices, or other electronic equipment operating in the 2.4 GHz band. Interference also typically comes from other APs and client devices that belong in the WLAN but that are far enough away so that their signal is weakened or has become corrupted. APs that are not part of the network infrastructure can also cause WLAN interference and are identified as rogue APs.

Interference and multipath distortion cause the transmitted signal to fluctuate. Interference decreases the signal-to-noise ratio (SNR) for a particular data rate. Packet retry counts go up in an area where interference and/or multipath distortion are high. Interference is also referred to as *noise level* or *noise floor*. The strength of the received signal from its associated AP must be high enough above the receiver's noise level to be decoded correctly. This level of strength is referred to as the signal-to-noise ratio, or SNR. The ideal SNR for the Cisco 7920 Wireless IP Phone is 25 dB. For example, if the noise floor is 98 decibels per milliwatt (dBm) and the received signal at the Cisco 7920 phone is 73 dBm, then the signal-to-noise ratio is 25 dB. (See Figure B-9.)

Figure B-9 Signal-to-Noise Ratio (SNR)



Changing the type and location of the antenna can reduce multipath distortion and interference. Antenna gain adds to the system gain and can reduce interference if the interfering transmitter is not directly in the boresight of the directional antenna.

Conclusion

While directional antennas can be of great value for certain indoor applications, the vast majority of indoor installations use omni-directional antennas. Directionality should be strictly determined by a correct and proper site survey. Whether you use an omni-directional or patch antenna, indoor environments require diversity antennas to mitigate multipath distortion. The Cisco Aironet 350, 1100, and 1200 Series Access Point radios include diversity support; however, the AP radio cannot provide diversity support with a single non-diversity antenna.

Signal Attenuation

Signal attenuation or signal loss occurs even as the signal passes through air. The loss of signal strength is more pronounced as the signal passes through different objects. A transmit power of 20 mW is equivalent to 13 dBm. Therefore, if the transmitted power at the entry point of a plasterboard wall is at 13 dBm, the signal strength will be reduced to 10 dBm when exiting that wall. Table B-1 shows the likely loss in signal strength caused by various types of objects.

Table B-1 Signal Attenuation Caused By Various Types of Objects

Object in Signal Path	Signal Attenuation through Object
Plasterboard wall	3 dB
Glass wall with metal frame	6 dB
Cinder block wall	4 dB
Office window	3 dB
Metal door	6 dB
Metal door in brick wall	12 dB
Human body	3 dB

Each site surveyed will have different levels of multipath distortion, signal loses, and signal noise. Hospitals are typically the most challenging environment to survey due to high multipath distortion, signal losses and signal noise. Hospitals take longer to survey, require a denser population of APs, and require higher performance standards. Manufacturing and shop floors are the next hardest to survey. These sites generally have metal siding and many metal objects on the floor, resulting in reflected signals that recreate multipath distortion. Office buildings and hospitality sites generally have high signal attenuation but a lesser degree of multipath distortion.

Antenna Types Recommended for Indoor Applications

Cisco highly recommends the use of diversity antennas for optimal throughput and performance in indoor deployments.

Figure B-10 and Figure B-12 show two types of antennas recommend for indoor applications, and Figure B-11 and Figure B-13 show the respective radiation patterns for those antennas.

Note The antenna power level ratings are listed as decibels isotropic (dBi).

Figure B-10 Cisco Aironet 2 dBi Diversity Omni-Directional Ceiling Mount Antenna (AIR-ANT5959)

Figure B-11 Radiation Pattern for AIR-ANT5959 Antenna

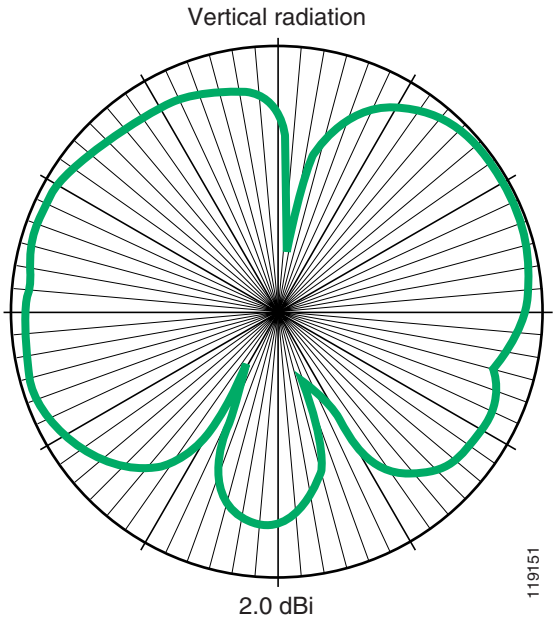
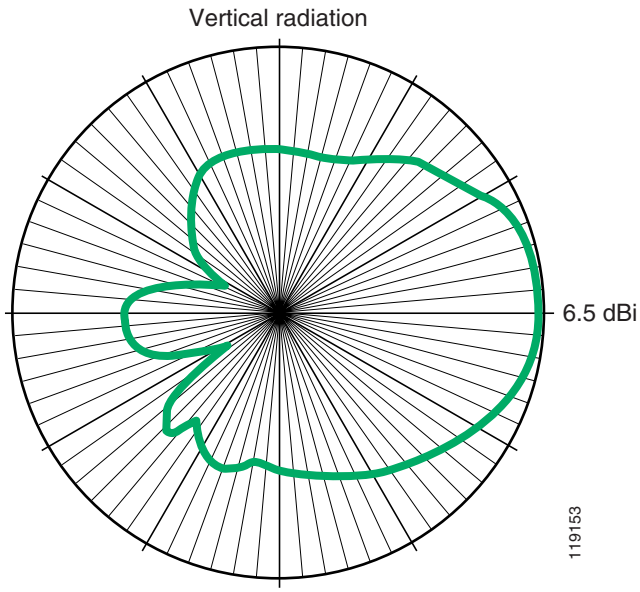


Figure B-12 Cisco Aironet 6.5 dBi Diversity Patch Wall Mount Antenna (AIR-ANT2012)

Figure B-13 Radiation Pattern for AIR-ANT2012 Antenna



Surveying Multi-Floor Buildings, Hospitals, and Warehouses

Consider the factors listed in this section when surveying multi-floor buildings, hospitals, and warehouses.

Note There is no way of determining the distance an RF signal will travel without conducting a survey.

Construction Methods and Materials

Many aspects of the building construction are unknown or hidden from the site survey, so you might have to acquire that information from other sources (such as architectural drawings). Some examples of typical construction methods and materials that affect the range and coverage area of APs include metallic film on window glass, leaded glass, steel-studded walls, cement floors and walls with steel reinforcement, foil-backed insulation, stairwells and elevator shafts, plumbing pipes and fixtures, and many others.

Inventory

Various types of inventory can affect RF range, particularly those with high steel or water content. Some items to watch for include printer paper, cardboard boxes, pet food, paint, petroleum products, engine parts, and so forth.

Levels of Inventory

Make sure you are performing a site survey at peak inventory levels or at times of highest activity. A warehouse at a 50% stocking level has a very different RF footprint than the same warehouse at an inventory level of 100%.

Activity Levels

Similarly, an office area after hours (without people) will have a different RF footprint than the same area full of people during the day. Although many parts of the site survey can be conducted without full occupation, it is essential to conduct the site survey verification and tweak key values during a time when the location is occupied.

The higher the utilization requirements and the higher the density of users, the more important it is to have a well designed diversity solution. When more users are present, more signals are received on each user's device. Additional signals cause more contention, more null points, and more multipath distortion. Diversity on the AP helps to minimize these conditions.

Multi-Floor Buildings

Keep in mind the following guidelines when conducting a site survey for a typical office building:

- Elevator shafts block and reflect RF signals.
- Supply rooms with inventory absorb signals.
- Interior offices with hard walls absorb RF signals.
- Break rooms (kitchens) can produce 2.4GHz interference through the use of microwave ovens.
- Test labs can produce 2.4 GHz or 5 GHz interference, creating multipath distortion and RF shadows.
- Cubicles tend to absorb and block signals.
- Conference rooms require high AP coverage because they are areas of high utilization.

Take extra care when surveying multi-floor facilities. APs on different floors can interfere with each other as easily as APs located on the same floor. It is possible to use this behavior to your advantage during a survey. Using higher-gain antennas, it might be possible to penetrate floors and ceilings and provide coverage to floors above as well as below the floor where the AP is mounted. Be careful not to overlap channels between APs on different floors or APs on the same floor.

In multi-tenant buildings, there might be security concerns that require the use of lower transmission powers and lower gain antennas to keep signals out of neighboring rooms or offices.

Hospitals

The survey process for a hospital is much the same as that for an enterprise, but the layout of a hospital facility tends to differ in the following ways:

- Hospital buildings tend to go through many reconstruction projects and additions. Each additional construction is likely to have different construction materials with different levels of attenuation.
- Signal penetration through walls and floors in the patient areas is typically minimal, which helps create micro-cells.
- The need for bandwidth increases with the increasing use of WLAN ultrasound equipment and other portable imaging applications. Of course, the need for bandwidth increases with the addition of wireless voice as well.
- Healthcare cells are small, and seamless roaming is essential, especially with voice applications.
- Cell overlap can be high, and so can channel reuse.
- Hospitals may have several types of wireless networks installed, including 2.4 GHz non-802.11 equipment. This equipment could cause contention with other 2.4 GHz or 5 GHz networks.
- Wall-mounted diversity patch antennas and ceiling-mounted diversity omni-directional antennas are popular, but keep in mind that diversity is required.

Warehouses

Warehouses have large open areas, often containing high storage racks. Many times these racks reach almost to the ceiling, where APs are typically placed. Such storage racks can limit the area that the AP can cover. In these cases, consider placing APs on other locations besides the ceiling, such as side walls and cement pillars. Also consider the following factors when surveying a warehouse:

- Inventory levels affect the number of APs needed. Test coverage with two or three APs in estimated placement locations.
- Unexpected cell overlaps are likely because of multipath variations. The quality of the signal will vary more than the strength of that signal. Clients might associate and operate better with APs farther away than with nearby APs.
- During a survey, APs and antennas usually do not have an antenna cable connecting them. But in a production environment, the AP and antenna might require antenna cables. All antenna cables have signal loss. The most accurate survey will include the type of antenna to be installed and the length of cable to be installed. A good tool to use to simulate the cable and its loss is an attenuator in a survey kit.

Surveying a manufacturing facility is similar to surveying a warehousing, except that there might be many more sources of RF interference in a manufacturing facility. In addition, the applications in a manufacturing facility usually require more bandwidth than those of a warehouse. These applications can include video imaging and wireless voice. Multipath distortion is likely to be the greatest performance problem in a manufacturing facility.

Testing Active Cisco 7920 Phones without Cisco CallManager

Perform the following steps to test a Cisco 7920 Wireless IP Phone without using Cisco CallManager:

Step 1 Associate the Cisco 7920 phone with the test AP.

Step 2 Use ping commands from the AP to a statically assigned IP address on the phone. Telnet to the test AP and start a continuous ping with the following commands:

a. At the prompt (>), enter the command **enable** and the password **Cisco**.

b. Enter the command **ping** *nnn.nnn.nnn.nnn* **size 256 repeat 1000 validate**, where *nnn.nnn.nnn.nnn* is the IP address of the Cisco 7920 phone.

c. Review the reported success rate.

d. Move to the next coverage test location.

e. Repeat steps b and c.

f. After determining the performance for the new location, walk back to the previous location while pinging the phone.

g. Verify the ping success rate while walking.

h. Repeat the above steps throughout the survey of the site.

Note When the phone is in standby mode, it will not answer every ping. To prevent this condition, place the phone in a call or temporarily disable power-save mode as described in the section on Advanced Cisco 7920 Commands, page A-1.

For voice, the success rate for pings should be 99%. The size value of 256 in Step 2b is used because it is slightly larger than the size of a voice packet. The repeat value of 1000 is just a suggestion for a value when you are stationary. The value can be up to 2147483647. When walking, use a larger value, but the success rate should remain at 99%.

Example Configurations for AP and RADIUS Server

AP Configuration

The following example shows a Cisco IOS configuration for an AP. The configuration and configuration commands in this example are valid for Cisco IOS version 12.2(15)JA. If you are using a newer version of Cisco IOS, some of the commands might be different or might be invalid. Refer to the latest configuration and command reference documentation for your version of Cisco IOS.

```
ap#sh run
Building configuration...

Current configuration : 4324 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
enable secret 5 $1$ZyA5$VTX31sQLnZ2cZnBnGhX6v/
!
username Cisco password 7 00271A150754
clock timezone U -8
clock summer-time U recurring
ip subnet-zero
!
aaa new-model
!
!
aaa group server radius rad_eap
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
```

```
aaa authentication login mac_methods local
aaa authorization exec default local
aaa authorization ipmobile default group rad_pmip
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
dot11 phone
dot11 arp-cache
!
policy-map data
  class class-default
   set cos 1
policy-map management
  class class-default
   set cos 7
policy-map voice
  class class-default
   set cos 6
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 1 key 1 size 128bit 7 C6BDD88611D089948782B58DA1E4 transmit-key
 encryption vlan 1 mode wep mandatory
 !
 encryption vlan 2 key 1 size 128bit 7 9FD518A21653687A4251AEE12308 transmit-key
 encryption vlan 2 mode wep mandatory
 !
 encryption vlan 3 key 1 size 128bit 7 09E1230C15B678330C1A84143960 transmit-key
 encryption vlan 3 mode wep mandatory
 !
 ssid data
    vlan 2
    authentication open
 !
 ssid voice
    vlan 3
    authentication open
 !
 speed basic-11.0
 rts threshold 2312
 power local 20
 power client 20
 channel 2437
 station-role root
!
interface Dot11Radio0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 service-policy input management
 service-policy output management
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.2
 encapsulation dot1Q 2
```

```
 no ip route-cache
 service-policy input data
 service-policy output data
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
 bridge-group 2 spanning-disabled
!
interface Dot11Radio0.3
 encapsulation dot1Q 3
 no ip route-cache
 service-policy input voice
 service-policy output voice
 bridge-group 3
 bridge-group 3 subscriber-loop-control
 bridge-group 3 block-unknown-source
 no bridge-group 3 source-learning
 no bridge-group 3 unicast-flooding
 bridge-group 3 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 ntp broadcast client
!
interface FastEthernet0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 no bridge-group 2 source-learning
 bridge-group 2 spanning-disabled
!
interface FastEthernet0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 no bridge-group 3 source-learning
 bridge-group 3 spanning-disabled
!
interface BVI1
 ip address 10.0.0.5 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.0.0.1
ip http server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
/ivory/1100
ip http authentication local
ip radius source-interface BVI1
!
radius-server attribute 32 include-in-access-req format %h
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
```

```
bridge 1 route ip
!
!
line con 0
line vty 5 15
!
ntp clock-period 2860645
ntp server 10.0.0.1
end
```

Configuring a Fallback RADIUS Server for LEAP

The following steps illustrate how to configure the fallback RADIUS server on the AP for LEAP authentication.

Step 1 Configure the Network Access Server (NAS):

```
radius-server local
  nas 192.168.10.35 key Cisco
  nas 192.168.10.45 key Cisco
```

Step 2 Configure the user database:

```
radius-server local
  user BM-AP1200-one-SCM password Cisco
  user BM-AP1100-two-SCM password Cisco
  user testuser password Cisco
```

Step 3 Configure the local RADIUS server in the AP's RADIUS server list:

```
aaa group server radius rad_eap
 server 192.168.10.45 auth-port 1812 acct-port 1813
 radius-server host 192.168.10.45 auth-port 1812 acct-port 1813 key Cisco
```

Step 4 Configure the RADIUS server time-outs:

```
radius-server deadtime 10
```

Step 5 Disable client holdoff:

```
no dot11 holdoff-time
```

Example Port Configurations for Voice Operations

The following examples show some of the port configurations required for voice operations.

Voice Bearer

```
rtp 16384 - 32767 udp
```

Voice Signaling

```
sccp 2000 tcp
```

Other Traffic

```
dhcp 67 udp (server) --> same as bootp
dhcp 68 udp (client) --> same as bootp
dns  53 udp
tftp 69 udp
```

Note Some protocols (such as TFTP) use dynamic port allocation, therefore Cisco recommends that you do *not* use an explicit deny-all statement for the filtering rules.

Site Information Help Request Form

When requesting assistance from the Cisco Technical Assistance Center (TAC) or your Cisco account team, please provide the information on these forms to better help them understand your environment and any of its problems.

Account Information

Customer Name:
Customer Location:
Customer Contact:
Cisco Systems Engineer:
Partner:

Site Information

Note Please provide a printout of the AP configuration and copies of the site survey documentation, if possible.

Has a Professional Site Survey been completed?
Name of Site Survey provider:
Number of phones:
Phone Firmware Version:
Power Setting on Phone:
Type of Access Point:
Type of Antenna:
Access Point OS:
Access Point Firmware Version:
Is WEP enabled?:

Is LEAP implemented?:
Type of LEAP Server:
LEAP Server Location:
Are VLANs implemented?:
Is QBSS Enabled?:
What Channels are utilized?:
Cisco CallManager Version:
Cisco CallManager Express Version (please provide configuration):

Issue or Problem

Provide a detailed description of the issue or problem:
Does this problem occur on multiple phone:
Does this problem occur in multiple locations:

Provide all the information from the Cisco 7920 Site Survey Tool before, during, and after the problem occurs, if possible:
For example:
`1(C), typhoon 34, 0`
`6(A), typhoon 18, 2`

User Support Help Request Form

The following example is a help request form for users at an enterprise who are experiencing voice problems. It is important to record certain information from each user each time they encounter a problem. This information helps identify trends in recurring problems that might seem random without the recorded data.

User name:
Type of problem: ___Poor voice quality ___Dropped phone call ___Phone not registering ___PWD not valid ___Other
Describe the problem in more detail. Please be as specific as possible (For example, were you walking, standing still, in a call, placing a call, experiencing one-way audio or choppy voice, etc.?):
Location where problem was seen (Please be as specific as possible — list floor, wing, etc.):
Did rebooting the phone help the problem?
Have you seen this problem at other locations?

Using Cisco Emergency Responder for E911 Calls with the Cisco 7920 Phone

Cisco Emergency Responder actively queries Cisco CallManager for new phone and user login registration events. In response to these events, Cisco Emergency Responder automatically searches known Cisco Catalyst switches in the network and finds the location of the phone and the user based on the switch port to which the phone is attached (via Cisco Discovery Protocol or MAC address). This information is then updated in a Cisco Emergency Responder location database and is used to identify a caller's location when an E911 call is placed. With this solution, users can move within a campus or between sites, wherever and whenever they want, without any intervention from the network administrator. This solution eliminates the administrative costs associated with relocating phones or users, while maintaining accurate and updated location information for E911 state and safety mandates.

Cisco Emergency Responder makes informed inbound and outbound call-routing decisions based on the location of emergency callers, and it provides crucial location information to emergency operators in public safety answering points (PSAPs). Outbound emergency calls are directed to a gateway associated with the PSAP that is nearest to the caller. In the event of an unintentional call disconnect or need for additional information, inbound calls from a PSAP are returned to the original caller.

For more information about Cisco Emergency Responder, refer to the documentation available at

http://www.cisco.com

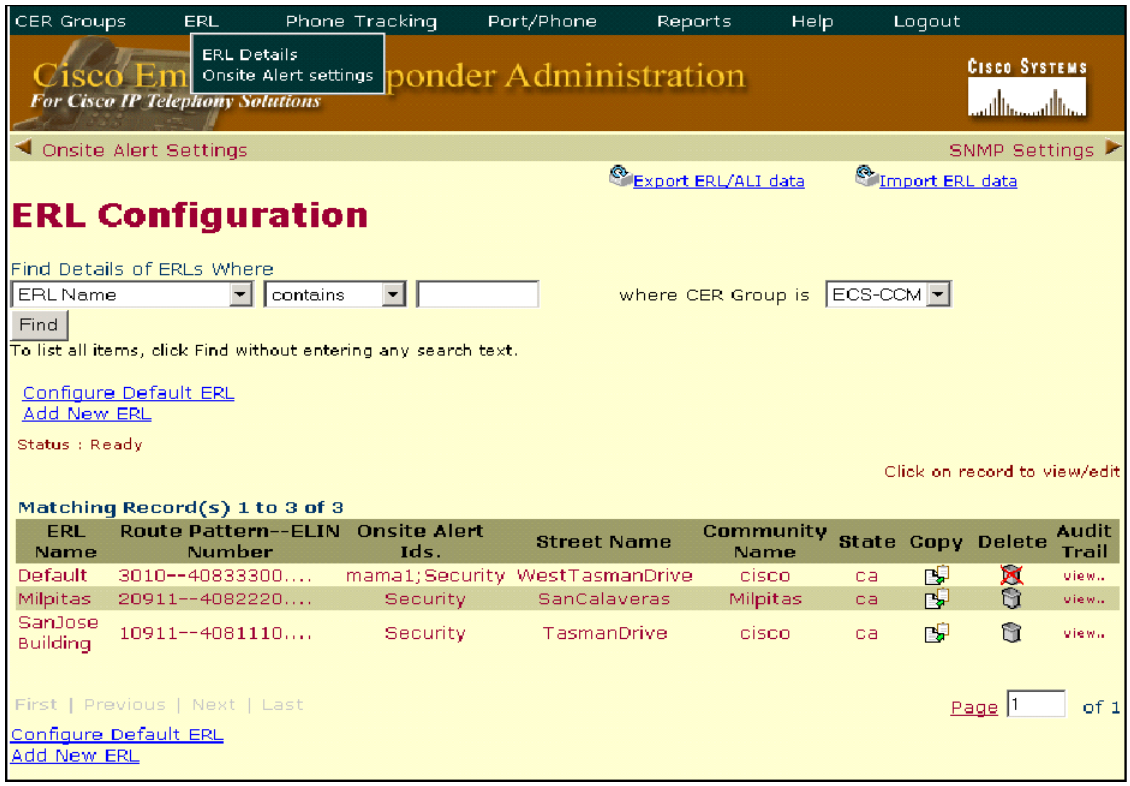
The following guidelines apply to the Cisco 7920 Wireless IP Phone due to the roaming capabilities of this 802.11b phone:

- Cisco Emergency Responder can query for IP Phones via either Cisco Discovery Protocol (CDP) on the Cisco Catalyst switches or MAC address. Because CDP is sent as a link-layer multicast protocol and is used by the Cisco AP to determine the QoS settings for the Cisco 7920 phones, it is not propagated up to the Cisco Catalyst switch. This means that Cisco Emergency Responder should query the Cisco Catalyst switches for the MAC addresses of the Cisco 7920 phones.
- Cisco Emergency Responder groups devices into Emergency Response Locations (ERL) so that they can be identified by a physical location (building, floor, section of floor, and so forth). Depending on how the power levels are configured on the Cisco APs, it is possible for the signal to propagate to floors above or below the AP with which the Cisco 7920 phone is associated. Using antennas that propagate the RF signal in a more horizontal pattern can help mitigate this issue, but emergency personnel within a building should be made aware of this possibility when organizing their searches for the individual or device that initiated the emergency call.

An E911 coverage policy is an individual decision that each company has to make and adapt to all of its various physical locations.

Cisco recommends that you assign each AP to its own ERL (or, minimally, group several adjacent APs into one ERL) using the Cisco Emergency Responder configuration interface, illustrated in Figure G-1. Using a code or abbreviation in the Automatic Location Information (ALI) or switch port location field can help on-site and PSAP personnel to identify that the caller is using a wireless device. This information is important for first-responders because it informs them that adjacent floors, hallways, rooms, and even other buildings might have to be searched to locate the emergency caller.

Figure G-1 Cisco Emergency Responder Configuration Screen



Guidelines and Limitations

This section discusses guidelines and limitations that apply to call admission control, Layer 3 roaming, and device mobility.

Call Admission Control

Call admission control refers to a mechanism for managing bandwidth usage to maintain a certain level of quality for voice calls. In time-division multiplexing (TDM) systems, call admission control is accomplished by limiting the number of DS0 channels. In wired Cisco IP Telephony networks, call admission control is provided by an interaction between the regions and locations configured in Cisco CallManager and the zones configured in Cisco H.323 gatekeepers. These mechanisms address call admission control only for the initial setup of IP Telephony calls, but they do not address call admission control when the underlying network is changing for the IP Phone throughout the call, as is the case when a Cisco 7920 phone roams between two APs.

Although the Cisco APs send out QoS Basis Service Set (QBSS) information about the channel utilization, and although the Cisco 7920 phones can use this information to determine the best AP to associate with, this information does not guarantee that calls will retain proper QoS during a roam between APs. For example, if seven or eight active Cisco 7920 phones all roam into an area served by a single AP, they would exceed the guidelines for calls per AP, thus causing QoS to degrade.

If the channel utilization is above the allowed threshold, the call is not set up and the phone displays a network busy message. If the channel utilization of the candidate handoff AP is above the threshold, the Cisco 7920 phone remains associated to its current AP for as long as possible. If the current AP is lost (no probe response or beacons received), the Cisco 7920 phone switches to the candidate AP regardless of channel utilization. The user hears a beep before the handoff happens so that the user can move back toward the current AP or stop roaming and finish the conversation.

Designing Around the Lack of Layer 3 Roaming

For users that require roaming support for a large area (such as between floors of a buildings), large Layer 2 VLANs (spanning across access-layer switches) can be created to eliminate the need for Cisco 7920 phones to cross a Layer 3 boundary when roaming. Consider the following guidelines before deploying such large Layer 2 VLANs:

- Cisco does *not* recommend letting data VLANs span multiple access-layer switches.
- A Layer 2 VLAN should not cross a building boundary. If this situation is unavoidable, build an additional (overlaid) Layer 2 core to avoid creating instability and excessive traffic in the traditional Layer 3 core.
- Both the voice VLAN and the native VLAN on the AP will have to be trunked across the large Layer 2 VLAN to allow for both voice traffic and Inter-Access Point Protocol (IAPP) traffic between the APs.
- Having Layer 2 VLANs span multiple access-layer switches creates the possibility of spanning-tree loops (if configured incorrectly) and overall network instability. Designs using this model should be reviewed with your Cisco Systems Engineer (SE) before deployment.
- If you plan eventually to extend the Layer 3 network down to the access-layer switches, do *not* use this model for building large Layer 2 VLANs.

Device Mobility with Cisco CallManager

When a wireless IP phone becomes a mobile device and moves from one location to another, the following potential problems could arise:

- Inaccurate bandwidth accounting by Cisco CallManager locations-based call admission control

  When a wireless IP phone roams from one location to another, there is currently no dynamic mechanism in Cisco CallManager to update the phone's location for purposes of call admission control. As a result, bandwidth can be subtracted from locations that are not actually using the bandwidth, and bandwidth can be used in other locations but not be taken into account by locations-based call admission control, thus causing oversubscription of the WAN bandwidth.

- Inappropriate codec selection

  When a wireless IP phone roams from one location to another, there is currently no dynamic mechanism in Cisco CallManager to update its region and/or device pool for purposes of determining codec type. As a result, the wrong codec could be used throughout the telephony network.

- Inappropriate PSTN gateway selection

  When a wireless IP phone roams from one location to another, there is currently no dynamic mechanism in Cisco CallManager to update the dial plan to specify the local PSTN gateway. As a result, the wireless IP phone might use a remote PSTN gateway for PSTN access. If the wireless IP phone places an emergency 911 call through this remote PSTN gateway, the emergency services will be directed to the location of the remote PSTN gateway and not to the location of the wireless IP phone that initiated the call.

Note If Cisco Emergency Responder is deployed, then 911 calls will be routed to the local PSTN gateway and to the appropriate public safety answering point (PSAP). However, call admission control will still be unaware of the bandwidth used by this call, and the wrong codec might be selected.

To prevent these device mobility problems, you must manually reconfigure the following parameters of the wireless IP phone in Cisco CallManager each time the phone is moved from one physical location to another:

- Call admission control location
- Device pool and region
- Calling search space

These parameters must be adjusted appropriately for each location to which the wireless IP phone moves. Other parameters might have to be reconfigured manually if advanced or non-standard features are required. For example, the media resource group list (for conferencing, transcoding, and music-on-hold resources) and the automated alternate routing (AAR) calling search space and group (if AAR is configured) must be reconfigured to ensure that local media resources are used and that automated alternate call routing is appropriate for each location.

These device mobility issues affect both centralized and distributed call processing deployments.

Maximum Throughput Calculations for 802.11b WLAN

Table I-1 lists the packet fields for voice traffic (both G.711 and G.729), and Table I-2 shows the theoretical maximum throughput for voice packets on an 802.11b WLAN network.

Table I-1 Voice Packet Fields

Field	Long Form	Short Form
Preamble (microseconds)	144	72
Header (microseconds)	48	24
Short Inter-Frame Space (SIFS) (microseconds)	10	10
Distributed Inter-Frame Space (DIFS) (microseconds)	50	50
Acknowledgement (ACK) (bytes)	14	14
Backoff (bytes)	32	32
Slot (microseconds)	20	20

Table I-2 Theoretical Maximum Throughput in Bits per Second (bps)

Header Type	Packet Length (bytes)	Transmission Rate			
		11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Long header	128	1,153,625	1,012,585	709,141	482,109
	256	2,088,246	1,710,294	1,047,034	650,571
Short header	128	1,472,033	1,249,889	817,891	Not Applicable
	256	2,596,588	2,036,889	1,160,997	Not Applicable

Note Throughput is based on a single client in disengage-confirmed (DCF) mode using Differentiated Services (DS) 802.11 with zero retries, no WEP, no request to send (RTS) or clear to send (CTS), and no fragmentation.

The throughput values in Table I-2 were calculated as follows:

Theoretical Maximum Throughput =
(Packet Length * 8 * 1000000) / (Preamble + Header + ((Packet Length + 28) * 8 / Rate) + SIFS + Preamble + Header + (ACK * 8 / Rate) + DIFS + ((Backoff / 2) * Slot))

One of the key aspects to remember when calculating network capacity for 802.11b networks is that it is a shared medium, so you must consider radio contention among the various devices. This contention means that the overall throughput is affected by the backoff algorithms in 802.11b that allow multiple devices to access the medium.

For the VoIP calculations in this section, a call has the following characteristics:

- The packets consist of a 20-byte IP header, an 8-byte UDP header, a 12-byte RTP header, and the RTP data.
- The RTP data is a 20-ms voice sample. For G.729 the data is 20 bytes; for G.711 it is 160 bytes.
- The total VoIP packet is 200 bytes of (IP+UDP+RTP) headers plus RTP data. The 802.11 header (Layer 2 MAC address) is 24 bytes long and the packet frame check sequence (FCS) is 4 bytes long, so the total packet size is 228 bytes.
- RTP traffic is transmitted at 50 packets per second (pps) in each direction, or 100 pps for a full-duplex conversation.

Using the 11 Mbps column from Table I-2, we can make the following calculations for G.711:

- Theoretical packet rate for 256-byte packet size = 2,596,588 bps = 324,573 bytes per second
- Bandwidth of G.711 VoIP call = 100 pps * 228 bytes per packet = 22,800 bytes per second
- Theoretical maximum VoIP capacity per 802.11b channel = 324,573 / 22,800 = 14.235 calls
- Theoretical maximum number of VoIP calls at 60% of bandwidth = 14.235 * 0.6 = 8.54 calls

Note Use only 60% of the available bandwidth to calculate the number of VoIP calls because this limit leaves some bandwidth for data traffic as well as for 802.11b management traffic and acknowledgements.

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W