CHAPTER 2

An Overview of the Voice Over IP Wireless Network

With the introduction of wireless communication, wireless IP phones can provide voice communication within the corporate wireless local area network (WLAN). The Cisco Unified Wireless IP Phone 7921G depends upon and interacts with wireless access points and key Cisco IP telephony components, including Cisco Unified CallManager, to provide wireless voice communication.

This chapter provides you with an overview of the interaction between the Cisco Unified Wireless IP Phone 7921G and other key components of the Voice-over-IP (VoIP) network in the WLAN environment.

Understanding the Wireless LAN

This section includes the following topics about the wireless LAN:

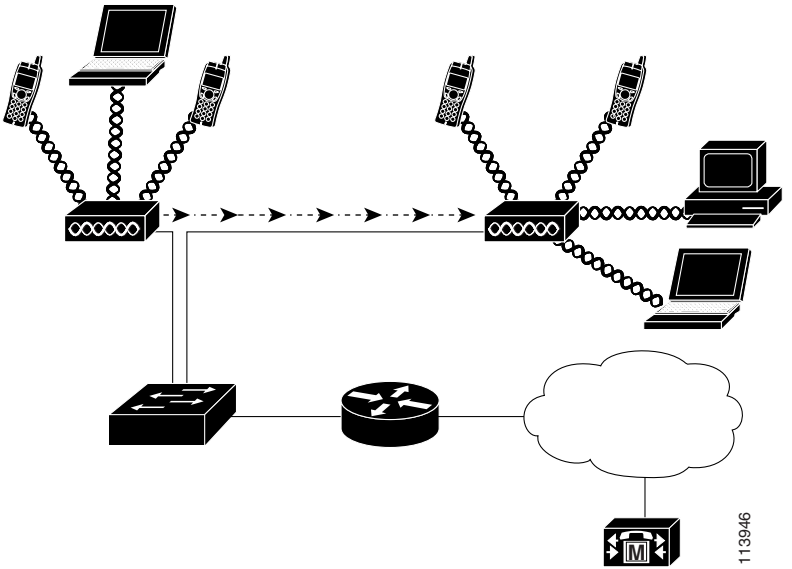
In a traditional LAN, phones and computers use cables to transmit messages and data packets over a wire conductor. Wireless LANs use radio waves to carry the messages and data packets.

WLANs require access point devices that receive and transmit radio signals. Cisco Aironet Access Points, such as the 1200, 1100, and 350 series models, support voice on a WLAN. Figure 2-1 shows a typical WLAN topology that incorporates wireless data for laptop computers and wireless IP telephony (WIPT) for wireless IP phones.

When a wireless device powers on, it immediately searches for and becomes associated with an access point. As users move from one location to another within the corporate WLAN environment, the wireless device roams out of range of one access point and into the range of another. The access point uses the wired network to transmit data and voice packets to the switches and routers. Voice signaling packets are sent to the Cisco Unified CallManager server for call processing and routing.

For more information about the Cisco wireless products, refer to http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_package.html

Figure 2-1 Wireless LAN with Wireless IP Phones



The 802.11 Standards for Wireless LAN Communications

Wireless LANs must follow the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards that define the protocols that govern all Ethernet-based wireless traffic. The Cisco Unified Wireless IP Phone 7921G supports these standards:

- The 802.11b standard was the first standard in wireless LAN communications, which is commonly called Wi-Fi.The 802.11b standard specifies the radio frequency (RF) of 2.4 GHz for both transmitting and receiving data.
- The 802.11g standard uses the same unlicensed 2.4 GHz band as 802.11b, but extends the data rates to provide greater performance by using Orthogonal Frequency Division Multiplexing (OFDM) technology.
- The 802.11a standard uses the 5 GHz band that provides more channels and improved data rates by using OFDM technology.

Radio Frequency Ranges

Wireless LAN communications uses these two radio frequency ranges:

- 2.4 GHz radio frequency range—This open RF range does not require licensing. To reduce interference within this band, WLANs transmit on non-overlapping channels, which are typically limited to three channels, although Japan uses four channels. Many devices operate in this bandwidth including cordless phones and microwave ovens; consequently, wireless communication is susceptible to interference or noise. Interference does not destroy the signal, but can impede the transmission speed and reduce an 11 Mbps signal all the way down to a 1Mbps signal. In addition, RF interference can reduce the voice quality over the wireless network.
- 5 GHz radio frequency range—This band has been divided into several sections called Unlicensed National Information Infrastructure (UNII) bands which have four channels each. The channels were spaced at 20 MHz thereby providing non-overlapping channels. As a result, 802.11a provides more channels.

Wireless Modulation Technologies

Wireless communications uses these two methods for carrying data and signals:

- Direct-Sequence Spread Spectrum (DSSS) technology—To help prevent interference, DSSS technology was developed to spread the signal out over the frequency range or bandwidth. DSSS technology multiplexes chunks of data over several frequencies so that multiple devices can communicate without interference. Each device has a special code that it uses to identify its data packets and to ignore all others. The Cisco wireless 802.11b/g products use DSSS technology to support multiple devices on the WLAN.
- Orthogonal Frequency Division Multiplexing (OFDM) technology—OFDM is a physical layer encoding technology for transmitting signals through the RF. This method breaks one high-speed data carrier into several lower-speed carriers that transmit in parallel across the particular RF spectrum. OFDM, when used with various modulation types such as 802.11g and 802.11a, is capable of supporting data rates as high as 54 Mbps.

Table 2-1 provides a comparison of the Wi-Fi standards and their features.

Table 2-1 Comparing Wi-Fi Standards Features

Item	802.11b	802.11g	802.11a
Data Rates	1, 2, 5.5, 11 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps
Non-overlapping Channels	3 (Japan uses 4)	3 (Japan uses 4)	Up to 23
Wireless Modulation	DSSS	DSSS, ODFM	ODFM

Connecting to the Wireless Network

The critical components in the wireless network are the access points that provide the wireless links or “hot spots” to the network. Cisco requires that the access points supporting voice communications must run Cisco IOS Version 12.3(8)JA or later. Cisco IOS provides features for managing voice traffic. For more information about access points, see the “Voice Over IP Wireless Network Configuration” section on page 2-27.

Each access point has a hard-wired connection to an Ethernet switch, such as a Cisco Catalyst 3750, that is configured on the LAN. The switch provides access to gateways and the Cisco Unified CallManager server to support wireless IP telephony (WIPT).

Access points transmit and receive RF signals over channels within the 2.4 GHz or 5.1 to 5.8 GHz frequency band. Regulatory domains determine the number of channels that wireless communications can use within the frequency band. Table 2-2 lists the frequency ranges and operating channels for three regulatory domains. The Cisco Unified Wireless IP Phone 7921G has a fourth domain type (product number is CP-7921G-W) for all other regions in the world. Wireless LANs in the rest of the world will use 802.11d to inform the phone which channels and data rates to use.

An access point broadcasts on a specific channel within the available channel range. To provide a stable wireless environment and reduce channel interference, you must specify non-overlapping channels for each access point. The recommended channels for 802.11b/g in North America are channels 1, 6, and 11.

Note In a non controller-based wireless network, it is recommended that you statically configure channels for each access point. If your wireless network uses a controller, you can use the Auto-RF feature with minimal voice disruption.

Table 2-2 Regulatory Domain Frequency Band and Channel Usage

Regulatory Domain	Frequency Band Range	Operating Channels
Federal Communications Commission (FCC) Product number is CP-7921G-A	2.412-2.462 GHz	11 channels
	5.15-5.25 GHz (UNII-1) 5.25-5.35 GHz (UNII-2) 5.725-5.825 (UNII-3) 5.470 - 5.725 (DFS)	12 channels
	5.47-5.725 GHz (pending approval	11 channels
ETSI (Europe) Product number is CP-7921G-E	2.412-2.472 GHz	13 channels (1-13)
	5.15-5.725 GHz	19 channels

Table 2-2 Regulatory Domain Frequency Band and Channel Usage

Regulatory Domain	Frequency Band Range	Operating Channels
Japan Product number is CP-7921G-P	2.412-2.472 GHz	13 channels (ODFM)
	2.412-2.484 GHz	14 channels (CCK)
	5.15-5.35 GHz	8 channels
World Product number is CP-7921G-W	Uses 802.11d to identify band ranges	Uses 802.11d to identify channels

The access point has a transmission range or coverage area that depends on its type of antenna and transmission power. The access point coverage range is from 500 to 1000 feet with effective isotropic radiated power (EIRP) output that scales at 1, 5, 20, and 50 mW. To provide effective coverage, access points need a range overlap of approximately 20 percent to allow uninterrupted connections as phone users roam from one access point to another.

Wireless networks use a service set identifier (SSID). The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. The SSID provides a way to group a set of user devices that can associate with a set of access points.

For more information about wireless network components and design, refer to *Cisco Enterprise Distributed Wireless Solution Reference Network Design* at http://www.cisco.com/application/pdf/en/us/guest/netsol/ns178/c649/ccmigration_09186a00800d67eb.pdf.

Security for Voice Communications

Because all WLAN devices that are within range can receive all other wireless LAN traffic, securing voice communications is critical. To ensure that voice traffic is not manipulated or intercepted by intruders, the Cisco Unified Wireless IP Phone 7921G and Cisco Aironet Access Points are supported in the overall Cisco SAFE Security architecture.

To secure voice communications, wireless networks use authentication and encryption methods. Wired Equivalent Privacy (WEP) is the method that was first introduced for wireless security, but this method is easily compromised. To address the security problems and weaknesses of WEP, the Wi-Fi Alliance defined Wireless Protected Access (WPA.)

Wi-Fi Protected Access is a standards-based, interoperable security enhancement that increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages Temporal Key Integrity Protocol (TKIP) for data protection and 802.1x for authenticated key management.

Through stronger encryption algorithms, stronger authentication, and rapid key updates, WPA has significantly improved security compared to WEP. Wireless clients, such as wireless IP phones, can authenticate at either the access point or with the network by using a centralized remote authentication dial-in user service (RADIUS) server.

The Cisco Wireless IP telephony solution provides wireless network security that prevents unauthorized logins and compromised communications by using these features:

- Encryption and authentication with Wired Equivalent Privacy (WEP)
- Wireless Protected Access (WPA and WPA2)
- Extensible Authentication Protocol (EAP)
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)

For additional information about Cisco Wireless LAN Security, refer to http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.html

Related Topics

- Networking Protocols Used with Cisco Unified Wireless IP Phones, page 2-8
- Authentication Mechanisms in the Wireless Network, page 2-19

Components of the VoIP Wireless Network

The wireless IP phone must interact with several network components in the wireless local area network (WLAN) to successfully place and receive calls.

The following topics provide an overview of the network components:

Networking Protocols Used with Cisco Unified Wireless IP Phones

Cisco Unified IP Phones support several industry-standard and Cisco networking protocols for voice communication. Table 2-3 provides an overview of the networking protocols that the Cisco Unified Wireless IP Phone 7921G supports.

Table 2-3 Supported Networking Protocols on the Cisco Unified Wireless IP Phone 7921G

Networking Protocol	Purpose	Usage Notes
Advanced Encryption Standard (AES)	Encryption standard that uses Cipher Blocking Chain (CBC) mode to IP security (IPSec).	Cisco Unified Wireless IP Phone 7921G can use AES to secure and preserve the integrity of wireless voice communications.
Cisco Centralized Key Management (CCKM)	Key generation protocol used for fast authentication in wireless networks.	Cisco Unified Wireless IP Phone 7921G can use CCKM for fast, secure roaming between access points.

Table 2-3 Supported Networking Protocols on the Cisco Unified Wireless IP Phone 7921G

Networking Protocol	Purpose	Usage Notes
Cisco Discovery Protocol (CDP)	Device-discovery protocol that runs on all Cisco-manufactured equipment. Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.	Cisco Unified IP Phones use CDP to communicate information such as auxiliary VLAN ID, per-port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Extensible Authentication Protocol (EAP)	Password-based mutual authentication scheme between the client (phone) and a RADIUS server.	Cisco Unified Wireless IP Phone 7921G can use EAP for authentication with the wireless network.
Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)	Protected Access Credential (PAC) authentication scheme between the client (phone) and an EAP-FAST RADIUS server.	Cisco Unified Wireless IP Phone 7921G can use EAP-FAST for authentication with the wireless network.
Dynamic Host Configuration Protocol (DHCP)	Dynamically allocates and assigns an IP address to network devices. DHCP enables an IP phone to connect to the network and become operational without the administrator assigning an IP address or configuring additional network parameters.	DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and an TFTP server on each phone locally. Use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, refer to *Cisco Unified CallManager System Guide*.

Table 2-3 Supported Networking Protocols on the Cisco Unified Wireless IP Phone 7921G

Networking Protocol	Purpose	Usage Notes
Internet Protocol (IP)	Messaging protocol that addresses and sends packets across the network.	To communicate using IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnet, and gateway identifications are automatically assigned if you are using the Cisco Unified IP Phone with DHCP. If you are not using DHCP, you must manually assign these properties to each phone locally.
Light Extensible Authentication Protocol (LEAP)	Cisco proprietary password-based mutual authentication scheme between the client (phone) and a RADIUS server.	Cisco Unified Wireless IP Phone 7921G can use LEAP for authentication with the wireless network.
Power Save Poll (PS-Poll)	Allows the phone to be in power save mode yet receive queued packets from AP.	Cisco Unified Wireless IP Phone 7921G can use PS-Poll to preserve battery life.
Real-Time Control Protocol (RTCP)	Used with the RTP protocol to provide control over the transporting of real-time data, such as interactive voice and video, over data networks.	Cisco Unified IP Phones use the RTCP protocol to allow monitoring of the data delivery and minimal control and identification functionality.
Real-Time Transport (RTP)	Standard for transporting real-time data, such as interactive voice and video, over data networks.	Cisco Unified IP Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.
Skinny Client Control Protocol (SCCP)	Uses Cisco-proprietary messages to communicate between IP devices and Cisco Unified CallManager.	Cisco Unified IP Phones use SCCP protocol for VoIP call signaling and enhanced features such as Message Waiting Indication (MWI).
Temporal Key Integrity Protocol (TKIP) with message integrity check (MIC)	Encryption and data integrity protocol that encrypts data sent over the wireless LAN.	Cisco Unified Wireless IP Phone 7921G can use TKIP/MIC algorithms to secure and preserve the integrity of voice communications.

Table 2-3 Supported Networking Protocols on the Cisco Unified Wireless IP Phone 7921G

Networking Protocol	Purpose	Usage Notes
Transmission Control Protocol (TCP)	Connection-oriented transport protocol.	Cisco Unified IP Phones use TCP to connect to Cisco Unified CallManager and to access XML services.
Trivial File Transfer Protocol (TFTP)	Method for transferring files over the network. On the Cisco Unified IP Phone, TFTP enables you to obtain a configuration file specific to the phone type.	You must have a TFTP server in your network that the DHCP server automatically identifies. If more than one TFTP server is running in your network, you must manually assign a TFTP server to each phone.
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	When security is implemented, Cisco Unified IP Phones use the TLS protocol when securely registering with Cisco Unified CallManager.
Unscheduled Asynchronous Power Save Delivery (U-APSD)	Allows the phone to be in power save mode yet receive queued packets from AP.	When the Cisco Unified Wireless IP Phone 7921G can use U-APSD, battery life is substantially improved.
User Datagram Protocol (UDP)	Connectionless messaging protocol for delivery of data packets.	Cisco Unified IP Phones receive and process UDP messages. RTP voice traffic runs over UDP.
Wi-Fi (802.11)	An open standard that defines wireless methods of transmitting Ethernet traffic and is commonly called Wi-Fi. This standard defines radio frequencies (RF) and data speed for wireless LAN communications.	Cisco Unified Wireless IP Phone 7921G supports the Wi-Fi standards. See Table 2-1 for more information.

Table 2-3 Supported Networking Protocols on the Cisco Unified Wireless IP Phone 7921G

Networking Protocol	Purpose	Usage Notes
Wired Equivalent Privacy (WEP)	Wireless security protocol for encrypting data that uses an encryption key stored on the phone and access point.	Cisco Unified Wireless IP Phone 7921G can use either static WEP or dynamic WEP keys for encryption, depending on the network security configuration.
Wireless Protected Access (WPA)	Provides stronger authentication, encryption key management and alternative encryption and message integrity methods.	Cisco Unified Wireless IP Phone 7921G supports WPA, WPA2, and WPA Pre-shared key authentication, including encryption using TKIP and MIC (message integrity check).

Related Topics

- Understanding the Phone Startup Process, page 3-26
- Components of the VoIP Wireless Network, page 2-8
- Configuring DHCP Settings, page 5-8

Interacting with Cisco Unified Wireless Access Points

Wireless voice devices use the same access points as wireless data devices. However, voice traffic over a WLAN requires different equipment configurations and layouts than a WLAN that is used exclusively for data traffic. Data transmission can tolerate a higher level of RF noise, packet loss, and channel contention than voice transmission. Packet loss during voice transmission can cause choppy or broken audio and make the phone call inaudible.

Wireless voice users are mobile and often roam across a campus or between floors in a building while they are connected to a call. In contrast, data users remain in one place or occasionally move to another location. The ability to roam while maintaining voice session continuity is one of the advantages of wireless voice; therefore, RF coverage needs to include areas not usually covered for data, such as stairwells, elevators, quiet corners outside conference rooms, and passage ways.

To assure good voice quality and optimal RF signal coverage, you must perform a site survey that determines settings suitable to wireless voice. The survey results provide information for the design and layout of the WLAN for voice, such as access point placement, power levels, and channel assignments.

After deploying and using wireless voice, you should continue to perform post installation site surveys. When you add a group of new users or install more equipment or stack large amounts of inventory, you are changing the wireless environment. You must verify that the access point coverage is still adequate for optimal voice communications. See the "Site Survey Verification" section on page 2-31 for more information.

Associating to an Access Point

At startup, the Cisco Unified Wireless IP Phone 7921G uses its radio to scan for access points with Service Set Identifiers (SSIDs) and encryption types that it recognizes. The phone builds and maintains a list of eligible access point targets and uses the following variables to determine the best access point with which to associate.

- Received Signal Strength Indicator (RSSI)—The phone uses this value to determine the signal strength of available access points within the RF coverage area. The phone attempts to associate with the access point with the highest RSSI value.
- QoS Basic Service Set (QBSS)—The access point uses this beacon information element (IE) to send the channel utilization of the access point to the unified IP phone. The phone uses the QBSS value to determine whether the access point can effectively handle more traffic.

Note QBSS is not supported when using Wi-Fi 802.11a.

- Traffic Specification (TSpec)—The TSpec value is used to calculate call limits and WLAN load balancing. The TSpec value of each voice stream allows the system to allocate bandwidth to voice devices on a first-come, first-served basis. For more information, see "Voice Quality in a Wireless Network" section on page 2-16.

The unified IP phone associates with the access point with the highest RSSI and lowest channel utilization values (QBSS) that have matching SSID and encryption types.To insure that voice traffic will be handled properly, you must configure the correct QoS in the access point. For configuration information, see "Wireless Network Requirements for VoIP" section on page 2-27.

Related Topics

- Roaming in a Wireless Network, page 2-14
- Security for Voice Communications, page 2-6
- Voice Over IP Wireless Network Configuration, page 2-27

Roaming in a Wireless Network

Wireless IP phones provide communication mobility to users within the enterprise WLAN environment. Unlike cellular phones that have broad coverage, the coverage area for the unified IP phone is smaller; therefore, phone users frequently roam from one access point to another. To understand some of the limitations of roaming with wireless IP phones, these examples provide information about the WLAN environment.

- Pre-call Roaming—A wireless IP phone user powers on the phone in the office, and the phone associates with the nearby access point. The user leaves the building, moves to another building, and then places a call. The phone associates with a different access point in order to place the call from the new location. If the associated access point is within the same Layer 2 VLAN, the IP address remains the same for the phone. But, if the roaming phone crosses a Layer 3 boundary with DHCP enabled, the phone recognizes that it is no longer in the same subnet. The phone requests a new IP address before it can connect to the network and place the call.

Note If a user leaves the WLAN coverage area and then comes back into the *same* WLAN area, the phone must reconnect to the network. By pressing a key on the phone, the user activates the phone and increases the scanning rate to speed up reconnecting to the network.

- Mid-call Roaming—A wireless IP phone user is actively engaged in a call and moves from one building to another. The roaming event occurs when the phone moves into the range of a different access point, and then the phone authenticates and associates with the new access point. The previous access point hands the call over to the new access point while maintaining continuous audio connection without user intervention. As long as the access points are in the same Layer 2 subnet, the unified IP phone keeps the same IP address and the call continues. As a unified IP phone roams between access points, it must re-authenticate with each new access point. See the "Authentication Mechanisms in the Wireless Network" section on page 2-19 for information about authentication.

  If the unified IP phone user moves from an access point that covers IP Subnet A to an access point that covers IP Subnet B, the phone no longer has an IP address or gateway that is valid within the new subnet and the call can disconnect.

- Layer 3 Roaming—With the release of the Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM), the Cisco Unified Wireless IP Phone 7921G now supports Layer 3 roaming for autonomous mode access points. For details about the Cisco WLSM, refer to the product documentation available at:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/wlsm_1_1/index.htm

  Layer 3 roaming with lightweight mode access points is accomplished by controllers that use dynamic interface tunneling. Clients that roam across controllers and VLANS can keep their IP address when using the same SSID.

- Fast and Secure Roaming—Cisco Centralized Key Management (CCKM) enables authenticated client devices to roam securely from one access point to another without any perceptible delay during reassociation. With the support of CCKM protocol, the wireless IP phone is able to negotiate the handoff from one access point to another more easily. During the roaming process, the phone must scan for the nearby access points, determine which

access point can provide the best service, and then reassociate with the new access point. When implementing stronger authentication methods, such as WPA and EAP, the number of information exchanges increases and causes more delay during roaming. To avoid additional delays, use CCKM to manage authentication.

CCKM, a centralized key management protocol, provides a cache of session credentials on the wireless domain server (WDS). As the phone roams from one access point to the next, CCKM compresses the number of message exchanges during roaming by providing a master key stored on the WDS for the access point to use. The reassociation exchange is reduced to two messages, thereby reducing the roaming time.

For details about CCKM, refer to the "Cisco Fast Secure Roaming Application Note" at:
http://www.cisco.com/en/US/products/hw/wireless/ps4570/prod_technical_reference09186a00801c5223.html

Note In dual band WLANs, it is possible to roam between 2.4 GHz bands (802.11b/g) and 5 GHz bands (802.11a). The phone moves out of range of one AP using one band and into the range of another that has the same SSID but is using a different band. This can cause gaps in voice communications. To avoid these communication gaps, try to use only one band for voice communications.

Related Topics

- Voice Quality in a Wireless Network, page 2-16
- Interacting with Cisco Unified Wireless Access Points, page 2-12
- Voice Over IP Wireless Network Configuration, page 2-27

Voice Quality in a Wireless Network

Voice traffic on the Wireless LAN, like data traffic, is susceptible to delay, jitter, and packet loss. These issues do not impact the data end user, but have serious implications for a voice call. To ensure that voice traffic receives timely and reliable treatment with low delay and low jitter, you must use Quality of Service (QoS), and use separate virtual LANs (VLANs) for voice and data. By isolating the voice traffic onto a separate VLAN, you can use QoS to provide priority

treatment for voice packets when traveling across the network. Also, use a separate VLAN for data traffic, not the default native VLAN which is typically used for all network devices.

You need the following VLANs on the network switches and the access points that support voice connections on the WLAN.

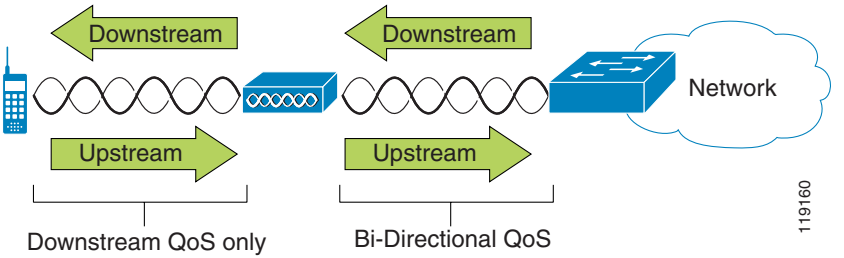
- Voice VLAN—Voice traffic to and from the wireless IP phone
- Data VLAN—Data traffic to and from the wireless PC
- Native VLAN—Data traffic to and from other wireless devices

Assign separate SSIDs to the voice and to the data VLANs. If you configure a separate management VLAN in the WLAN, do not associate an SSID with the management VLAN.

By separating the phones onto a voice VLAN and marking voice packets with higher CoS, you can ensure that voice traffic gets priority treatment over data traffic resulting in lower packet delay and fewer lost packets.

Unlike wired networks with dedicated bandwidths, wireless LANs have to consider traffic direction when implementing QoS. Traffic is classified as upstream or downstream from the point of view of the access point as shown in Figure 2-2.

Figure 2-2 Voice Traffic in a Wireless Network



Beginning with Cisco IOS release 12.2(11)JA, Cisco Aironet APs support the contention-based channel access mechanism called Enhanced Distributed Coordination Function (EDCF). The EDCF-type of QoS has up to eight queues for downstream (toward the 802.11b/g clients) QoS. You can allocate the queues based on these options:

- QoS or Differentiated Services Code Point (DSCP) settings for the packets
- Layer 2 or Layer 3 access lists

- VLANs for specific traffic
- Dynamic registration of devices

Although you can have up to eight queues on the access point, you should use only two queues for voice traffic to ensure the best possible voice QoS. Place voice (RTP) and signaling (SCCP) traffic in the highest priority queue, and place data traffic in a best-effort queue.Although 802.11b/g EDCF does not guarantee that voice traffic is protected from data traffic, you should get the best statistical results by using this queuing model.

Note The Cisco Unified Wireless IP Phone 7921G marks the SCCP signaling packets with a DSCP value of 24 and RTP packets with DSCP value of 46.

To improve reliability of voice transmissions in a nondeterministic environment, the Cisco Unified Wireless IP Phone 7921G supports the IEEE 802.11e industry standard and is Wi-Fi Multimedia (WMM) capable. WMM enables differentiated services for voice, video, best effort data and other traffic. However, in order for these differentiated services to provide sufficient QoS for voice packets, only a certain amount of voice bandwidth can be serviced or admitted on a channel at one time. If the network can handle “N” voice calls with reserved bandwidth, when the amount of voice traffic is increased beyond this limit, (to N+1 calls), the quality of all calls suffers.

To help address the problems of VoIP stability and roaming, an initial Call Admission Control (CAC) scheme is required. With CAC, QoS is maintained in a network overload scenario by ensuring that the number of active voice calls does not exceed the configured limits on the access point. The Cisco Unified Wireless IP Phone 7921G can integrate layer 2 TSpec admission control with layer 3 Cisco Unified CallManager admission control (RSVP). During times of network congestion, calling or called parties receive a fast busy indication. The system maintains a small bandwidth reserve so wireless phone clients can roam into a neighboring access point (AP), even when the AP is at “full capacity”. After reaching the voice bandwidth limit, the next call is load-balanced to a neighboring AP without affecting the quality of the existing calls on the channel.

Implementing Quality of Service in the connected Ethernet switch is highly desirable to maintain good voice quality. The COS and DSCP values that the Cisco Unified Wireless IP Phone 7921G sets do not need to be modified. To configure QoS correctly on the access point, see the “Configuring the Wireless Network for Voice” section on page 2-28.

Related Topics

- Authentication Mechanisms in the Wireless Network, page 2-19
- Interacting with Cisco Unified CallManager, page 2-24
- Voice Over IP Wireless Network Configuration, page 2-27

Authentication Mechanisms in the Wireless Network

Before a wireless device can communicate on the network, it must authenticate with the access point or the network by using an authentication method. The wireless IP phone can use these authentication methods in the WLAN:

- Open Authentication—Any wireless device can request authentication in an open system. The access point that receives the request may grant authentication to any requestor or only to requestors on a list of users. Communication between the wireless device and access point could be non-encrypted or devices can use WEP keys to provide security. Devices that are using WEP only attempt to authenticate with an access point that is using WEP.
- Shared Key Authentication—The access point sends an unencrypted challenge text string to any device attempting to communicate with the access point. The device that is requesting authentication uses a pre-configured WEP key to encrypt the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. A device can authenticate only if its WEP key matches the WEP key on the access points.

  Shared key authentication can be less secure than open authentication with WEP because someone can monitor the challenges. An intruder can calculate the WEP key by comparing the unencrypted and encrypted challenge text strings.
- WPA Pre-Shared Key (PSK) Authentication—The access point and the phone are configured with the same authentication key. The pre-shared key is used to create unique pair-wise keys that are exchanged between each phone and the access point. You can configure the pre-shared key as a hexadecimal or ASCII character string. Because the pre-shared key is stored on the phone, it might be compromised if the phone is lost or stolen.

- EAP-FAST Authentication—This client server security architecture encrypts EAP transactions within a Transport Level Security (TLS) tunnel between the access point and the Remote Authentication Dial-in User Service (RADIUS) server such as the Cisco Access Control Server (ACS).

  The TLS tunnel uses Protected Access Credentials (PACs) for authentication between the client (phone) and the RADIUS server. The server sends an Authority ID (AID) to the client (phone), which in turn selects the appropriate PAC. The client (phone) returns a PAC-Opaque to the RADIUS server. The server decrypts the PAC with its master-key. Both end points now have the PAC key and a TLS tunnel is created. EAP-FAST supports automatic PAC provisioning, but you must enable it on the RADIUS server.

Note In the Cisco ACS, by default, the PAC expires in one week. If the phone has an expired PAC, authentication with the RADIUS server takes longer while the phone gets a new PAC.
To avoid these PAC provisioning delays, set the PAC expiration period to 90 days or longer on the ACS or RADIUS server.

Authenticated Key Management

The following authentication schemes use the RADIUS server to manage authentication keys:

- Wi-Fi Protected Access (WPA)—Uses information on a RADIUS server to derive unique pair-wise keys for authentication. Because these keys are generated at the centralized RADIUS server, WPA provides more security than WPA pre-shared keys that are stored on the access point and phone.
- Cisco Centralized Key Management (CCKM)—Uses information on a RADIUS server and a wireless domain server (WDS) to manage and authenticate keys. The WDS creates a cache of security credentials for CCKM-enabled client devices for fast and secure reauthentication.

  With WPA and CCKM, encryption keys are not entered on the phone, but are automatically derived between the access point and phone. But the EAP username and password that are used for authentication must be entered on each phone.

Encryption Methods

To ensure that voice traffic is secure, the Cisco Unified Wireless IP Phone 7921G supports Wired Equivalent Privacy (WEP), Temporal Key Integrity Protocol (TKIP), and Advanced Encryption Standards (AES) for encryption. When using either of these mechanisms for encryption, both the signaling (SCCP) packets and voice (RTP) packets are encrypted between the access point and the unified IP phone.

- WEP—When using WEP in the wireless network, authentication happens at the access point by using open or shared-key authentication. The WEP key that is setup on the phone must match the WEP key that is configured at the access point for successful connections. The Cisco Unified Wireless IP Phone 7921G supports WEP keys that use 40-bit encryption or a 128-bit encryption and remain static on the phone and access point.

  EAP and CCKM authentication can use WEP keys for encryption. The RADIUS server manages the WEP key and passes a unique key to the access point after authentication for encrypting all voice packets; consequently, these WEP keys can change with each authentication.

- TKIP—WPA and CCKM use TKIP encryption that has several improvements over WEP. TKIP provides per-packet key ciphering and longer initialization vectors (IVs) that strengthen encryption. In addition, a message integrity check (MIC) ensures that encrypted packets are not being altered. TKIP removes the predictability of WEP that helps intruders decipher the WEP key.

- AES—An encryption method used for WPA2 authentication. This national standard for encryption uses a symmetrical algorithm that has the same key for encryption and decryption. AES uses Cipher Blocking Chain (CBC) encryption of 128 bits in size, supporting key sizes of 128, 192 and 256 bits, as a minimum.

Note The Cisco Unified Wireless IP Phone 7921G does not support Cisco Key Integrity Protocol (CKIP) with CMIC.

Choosing Authentication and Encryption Methods

Authentication and encryption schemes are setup within the wireless LAN. VLANS are configured in the network and on the access points and specify different combinations of authentication and encryption. An SSID is associated

with a VLAN and its particular authentication and encryption scheme. In order for wireless client devices to authenticate successfully, you must configure the same SSIDs with their authentication and encryption schemes on the access points and on the unified IP phone.

Some authentication schemes require specific types of encryption. With Open authentication, you have the option to use static WEP for encryption for added security. But if you are using Shared Key authentication, you must set static WEP for encryption, and you must configure a WEP key on the phone.

When using Authenticated Key Management (AKM) for the Cisco Unified Wireless IP Phone 7921G, several choices for both authentication and encryption can be set up on the access points with different SSIDs. When the unified IP phone attempts to authenticate, it chooses the access point that advertises the authentication and encryption scheme that the phone can support. Auto (AKM) mode can authenticate by using WPA, WPA2, WPA Pre-shared key, or CCKM.

Note

- When using WPA Pre-shared key or WPA2 Pre-shared key, the pre-shared key must be statically set on the phone.These keys must match the keys configured on the access point.
- When using Auto (AKM), encryption options are automatically configured for WPA, WPA2, WPA Pre-shared key, WPA2 Pre-shared key, or CCKM.

For more information about configuring authentication and encryption schemes on access points, refer to the *Cisco Aironet Configuration Guide* for your model and release at this URL:

http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_installation_and_configuration_guides_list.html

Table 2-4 provides a list of authentication and encryption schemes configured on the Cisco Aironet Access Points supported by the Cisco Unified Wireless IP Phone 7921G. The table shows the network configuration option for the phone that corresponds to the access point configuration.

Table 2-4 Authentication and Encryption Schemes

Cisco Access Point Configuration			Cisco Unified Wireless IP Phone 7921G
Authentication	**Key Management**	**Common Encryption**	**Authentication**
Open	None	None	Open (optional)
Open (Static WEP)	None	WEP	Open+WEP
Shared key (Static WEP)	None	Static WEP	Shared Key+WEP
LEAP Open and Network EAP—can use both	Optional CCKM	WEP	LEAP
EAP-FAST Open and Network EAP—can use both	Optional CCKM	WEP	EAP-FAST
EAP-FAST with WPA Open and Network EAP—can use both	WPA/ Optional CCKM	TKIP	EAP-FAST
EAP-FAST with WPA2 Open and Network EAP—can use both	WPA	AES	EAP-FAST
WPA Open and Network EAP—can use both Optional CCKM	WPA/ Optional CCKM	TKIP	Auto (AKM) with WPA
WPA-PSK Open and Network EAP—can use both Optional CCKM	WPA	TKIP	Auto (AKM) with WPA-PSK

Table 2-4 Authentication and Encryption Schemes (continued)

Cisco Access Point Configuration			Cisco Unified Wireless IP Phone 7921G
Authentication	**Key Management**	**Common Encryption**	**Authentication**
WPA2 Open and Network EAP—can use both	WPA	AES	Auto (AKM) with WPA2
WPA2-PSK Open and Network EAP—can use both	WPA	AES	Auto (AKM) with WPA2-PSK

Related Topics

- Interacting with Cisco Unified CallManager, page 2-24
- Components of the VoIP Wireless Network, page 2-8
- Voice Over IP Wireless Network Configuration, page 2-27

Interacting with Cisco Unified CallManager

Cisco Unified CallManager is the call control component in the network that handles and routes calls for the wireless IP phones. Cisco Unified CallManager manages the components of the IP telephony system—the phones, access gateways, and the resources—for such features as call conferencing and route planning. When deploying Cisco Unified Wireless IP Phone 7921G, you must use Cisco Unified CallManager Release 4.1, 4.2, 5.0 or later and SCCP protocol.

Before Cisco Unified CallManager can recognize a phone, it must register with Cisco Unified CallManager and be configured in the database. For information about setting up phones in Cisco Unified CallManager, see the "Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager" section on page 1-17.

You can find more information about configuring Cisco Unified CallManager to work with the IP phones and IP devices in the *Cisco Unified CallManager Administration Guide* and *Cisco Unified CallManager System Guide.*

Related Topics

- Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager, page 1-17
- Phone Configuration Files and Profile Files, page 2-25

Phone Configuration Files and Profile Files

Configuration files for a phone define parameters for connecting to Cisco Unified CallManager and are stored on the TFTP server. In general, any time you make a change in Cisco Unified CallManager Administration that requires resetting the phone, the phone configuration file changes automatically.

Configuration files also contain information about the correct image load for the phone. If this image load differs from the one currently loaded on a phone, the phone contacts the TFTP server to request the new image file.

The phone first requests the configuration file SEP*xxxxxxxxxxxx*.cnf.xml, where each *xx* is the two-digit lowercase hexadecimal representation of each integer in the phone's MAC address. If the phone cannot find this file, it requests the configuration file XMLDefault.cnf.xml.

After the phone obtains the *.cnf.xml files, it requests a phone-specific profile file. If a phone cannot find this profile file, it requests the appropriate common profile file.

After the phone finds one of the profile files, or if it cannot find a profile file, it continues with its startup process.

Related Topic

Understanding the Phone Startup Process, page 3-26

Interacting with the DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage and automate the assignment of Internet Protocol (IP) addresses in a network. When an IP device is added to the network, it must have a unique IP address. Without DHCP, the IP address must be entered manually at each device. DHCP allocates IP addresses dynamically and reuses IP addresses when devices no longer need them.

If DHCP is enabled in the network, the Cisco Unified Wireless IP Phone 7921G uses the DHCP scope settings in the DHCP server to perform the phone provisioning bootup process. You must configure the settings of the DHCP server in the Cisco Unified CallManager network.

The DHCP scope settings include the following:

- TFTP servers
- DNS server IP address (optional unless using host names)
- Pool and range of the subnet mask, IP address, and gateway

The priority of the DHCP settings for the TFTP server is unique to the Cisco Unified Wireless IP Phone 7921G, as shown in Table 2-5.

Table 2-5 DHCP Settings Priority

Priority	DHCP Settings
1st	DHCP option 150
2nd	DHCP option 66
3rd	SIADDR
4th	ciscoCM1

If DHCP is disabled, the Cisco Unified Wireless IP Phone 7921G uses the following network settings in Table 2-6 to perform the phone provisioning bootup process. You must configure these static parameters for each Cisco Unified Wireless IP Phone 7921G.

Table 2-6 Static IP Addresses When DHCP is Disabled

Static Setting	Description
IP Address	IP address, the unique identifier assigned by the system administrator for the phone.
Subnet Mask	Used to partition the IP address into a network identifier and host identifier so TCP/IP can distinguish between them.
Default Router 1	Identifies the gateway that provides connectivity to the IP network beyond the subnet to which the phone belongs.

Table 2-6 Static IP Addresses When DHCP is Disabled (continued)

Static Setting	Description
DNS Server 1 DNS Server 2	If the system is configured to use host names for servers instead of IP addresses, identifies the primary and secondary DNS server to resolve host names.
TFTP Server 1 TFTP Server 2	Identifies the TFTP servers that the phone uses to obtain configuration files.

Voice Over IP Wireless Network Configuration

This section provides configuration guidelines for deploying wireless IP phones in the WLAN and includes these topics:

- Wireless Network Requirements for VoIP, page 2-27
- Configuring the Wireless Network for Voice, page 2-28

Wireless Network Requirements for VoIP

When configuring voice over the wireless LAN, use access points that run Cisco IOS Version 12.3(8)JA or later. Controllers should be running version 4.0 and higher with IOS Version 12.3(8)JX or later.

The Cisco Unified Wireless IP Phone 7921G supports Cisco Aironet Access Points (APs) that can run Cisco IOS in autonomous mode and APs that run in lightweight mode with lightweight access point protocol (LWAPP) and use a wireless LAN controller. Table 2-7 lists the supported AP models and their operation mode in the WLAN.

Note Voice over the wireless LAN (VoWLAN) does not currently support MESH technology such as Cisco Aironet 1500 Series Lightweight Outdoor Mesh Access Points.

Table 2-7 Supported Access Points and Modes

Access Point Models	Autonomous Mode	Lightweight Mode
Cisco Aironet 350 Series AP	Yes	No
Cisco Aironet 1100 Series AP	Yes	Yes
Cisco Aironet 1130 Series AP	Yes	Yes
Cisco Aironet 1200 Series AP	Yes	Yes
Cisco Aironet 1240 Series AP	Yes	Yes
Cisco Aironet 1300 Series AP	Yes	Yes
Cisco 1000 Series Lightweight AP	No	Yes

Note Be aware that Wi-Fi compliant access points that are manufactured by third-party vendors can function with the Cisco Unified Wireless IP Phone 7921G, but might not support key features such as Dynamic Transmit Power Control (DTPC), ARP-caching, LEAP/EAP-FAST, QBSS, U-APSD, 802.11d and 802.11h.

Configuring the Wireless Network for Voice

This section identifies key access point (AP) configuration options that are required for optimal voice performance. This is not a complete list of configuration steps or options for deploying access points such as the Cisco Aironet Access Points. For more information about configuring your access point, refer to the appropriate *Cisco Aironet Access Point Installation and Configuration Guide* for your model or the documentation for your access point.

Note When deploying the Cisco Unified Wireless IP Phone 7921G with World regulatory domain (CP-7921G-W-K9), you must enable the access points for world mode (802.11d). The world model phone gets the channels and power information from the access point.

Table 2-8 explains and provides references for many of the configuration tasks for the Cisco Aironet Access Point, controller, and Ethernet switch when setting up VoIP on the WLAN.

Table 2-8 Checklist for Wireless Network Configuration

Tasks	Explanation	Reference
1. Check that the Cisco IOS version is the recommended version	• Under System Software, check for Cisco IOS version 12.3(8)JA or later. • For the controller, use Version 4.0 and Cisco IOS version 12.3(8)JX or later.	Interacting with Cisco Unified Wireless Access Points, page 2-12
2. Configure a VLAN for voice	To isolate voice traffic and enable QoS, you need a separate voice VLAN on the access point and network switch.	Voice Quality in a Wireless Network, page 2-16
3. Configure Service Set Identifier (SSID) for each VLAN	Identifier for a set of wireless devices to communicate with each other. Several access points can have the same SSID to support a group of wireless phones.	Interacting with Cisco Unified Wireless Access Points, page 2-12 Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA
4. Configure QoS settings for VLANs	Create a QoS policy for the voice VLAN and assign a higher CoS to voice traffic. Enable the QoS element for wireless IP phones to provide channel utilization (QBSS) information to phones.	Voice Quality in a Wireless Network, page 2-16 Configuring the Wireless Network for Voice, page 2-28 Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA
5. Enable ARP caching	Enable this option to ensure two-way audio. The access point has ARP caching disabled by default.	*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA*

Table 2-8 Checklist for Wireless Network Configuration (continued)

Tasks	Explanation	Reference
6. Configure radio (802.11) settings	Data Rate—Set for11 Mbps or to the rate for the frequency band that you are using. Client Transmit Power—After a site survey, determine the appropriate power requirements and set a specific Client Transmit Power setting. The Cisco Unified Wireless IP Phone 7921G uses the same setting as the access point. **Note** If autonomous AP power is set for Max, the access point does not advertise Client Transmit Power (DTPC) setting.	*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA*
7. Configure security for the voice VLANs	Use one of these authentication and encryption options for the SSID that corresponds to the voice VLAN: • Open • Shared Key • EAP • Auto (AKM)	Choosing Authentication and Encryption Methods, page 2-21 *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA*

Configuration Tip for Cisco Airespace Access Points

If you are using EAP-FAST with Cisco Airespace technology, you must increase the EAP request (802.1x) timeout to at least 20 seconds to ensure that the phone gets the PAC credentials successfully.

To change the request timeout on the controller, follow these steps:

Procedure

Step 1 Use SSH or Telnet to access the Airespace controller or controllers.

Step 2 Enter `config advanced eap request-timeout 20`

Step 3 Enter `save config`

Step 4 Enter `y` to confirm.

Site Survey Verification

After the initial deployment of wireless phones in the WLAN, it is a good practice to perform site surveys at regular intervals to verify that the APs are providing adequate coverage and that wireless phones can roam from one AP to another with no audio problems.

You should use the wireless IP phone and the Aironet Client Utility (ACU) to verify that the signal range and transmission power provide adequate coverage for roaming phones.

Use the following topics for information about performing the site survey:

- Performing a Site Survey Verification, page 2-31
- Using the Cisco Unified Wireless IP Phone 7921G Site Survey Utility, page 2-32

Performing a Site Survey Verification

Perform these tasks to verify wireless voice network operation. Check that the wireless IP phones:

1. Associate with all APs in the WLAN.
2. Authenticate with all APs in the WLAN.
3. Register with Cisco Unified CallManager.

4. Can make stationary phone calls with good quality audio.
5. Can make roaming phone calls with good quality audio and no disconnections.
6. Can place multiple calls, especially in areas designated for high density use.

After phones are installed, request that users report any problems when using their wireless IP phones.

When you perform a site survey verification and encounter problems, see the Chapter 9, "Troubleshooting the Cisco Unified Wireless IP Phone 7921G" for assistance with finding the cause of the problem.

Related Topic

Using the Cisco Unified Wireless IP Phone 7921G Site Survey Utility, page 2-32

Using the Cisco Unified Wireless IP Phone 7921G Site Survey Utility

The Cisco Unified Wireless IP Phone 7921G includes a site survey utility within the Settings > Status menu that provides information about the access points currently within range of the phone.

To use the Site Survey utility, follow these steps:

Procedure

Step 1 Configure the Cisco Unified Wireless IP Phone 7921G with the same SSID and encryption/authentication settings as the APs.

Step 2 Power on the phone so that it associates with the WLAN.

Step 3 Choose **Settings > Status > Site Survey**.

The phone displays a list of access points within range that have the same SSID and security settings as the phone.

The display provides the following information about the APs:

SSID: abcd

Channel	BSSID	RSSI	Channel Utilization
01	19:50	-38	50
06	cf:d0	-51	38
11	7b:b0	-42	61

Step 4 To see more information about an AP, scroll to the desired line and press **Details**.

The following information appears for the specific AP:

```
SSID: abcd
Channel:06
BSSID: 00:13:1a:16:cf:d0
RSSI:-51
CU:38
```

Step 5 To verify the ability to roam between APs, walk through all areas where phones are used and take readings. Approach areas from different directions to assure successful roaming conditions.

Step 6 Adjust AP and antenna placement and AP power settings to provide approximately 20 percent coverage overlap.

In addition to the Site Survey utility in the Cisco Unified Wireless IP Phone 7921G, you can also use the Cisco Aironet Client Utility Site Survey Utility from a laptop PC. Refer to the section on “Performing a Site Survey” in the *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide* for your system.

Related Topic

Performing a Site Survey Verification, page 2-31