CHAPTER 2

Overview of the VoIP Wireless Network

This chapter provides an overview of the interaction between the Cisco Unified Wireless IP Phone 7925G and other key components of a VoIP network in a wireless local area network (WLAN) environment. It contains the following sections:

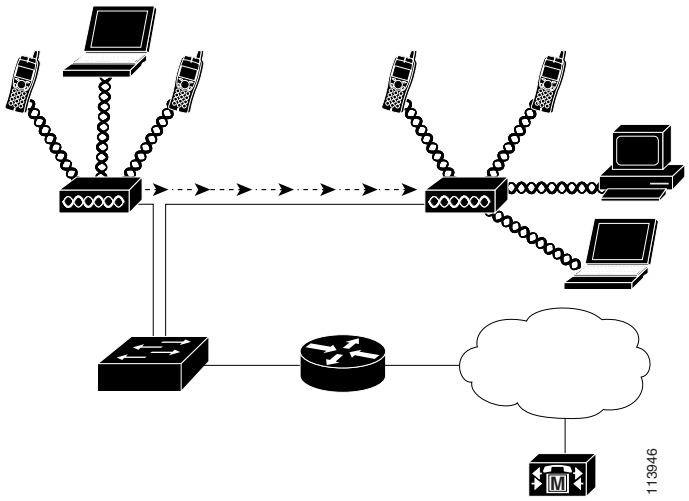
Understanding the Wireless LAN

With the introduction of wireless communication, wireless IP phones can provide voice communication within the corporate WLAN. The Cisco Unified Wireless IP Phone 7925G depends upon and interacts with wireless access points (APs) and key Cisco IP telephony components, including Cisco Unified Communications Manager Administration, to provide wireless voice communication.

In a traditional LAN, IP phones and computers use cables to transmit messages and data packets. Cisco Unified WLAN delivers security, scalability, reliability, ease of deployment, and management similar to wired LANs. It includes RF capabilities that enable real-time access to core business applications and provides proven enterprise-class secure connectivity. The WLAN is an integrated end-to-end solution that uses wireless IP phones and APs, network infrastructure, network management, and mobility services.

Figure 2-1 shows a typical WLAN topology that enables the wireless transmission of voice for wireless IP telephony.

Figure 2-1 WLAN with Wireless IP Phones



When a wireless IP phone powers on, it searches for and becomes associated with an AP. As users move from one location to another, the wireless IP phone roams out-of-range of one AP into the range of another AP. The wireless IP phone builds and maintains a list of eligible APs and reconnects to an AP in that list. See "Associating to APs" section on page 2-12 for more information.

The AP uses its connection to the wired network to transmit data and voice packets to and from the switches and routers. Voice signaling is transmitted to the Cisco Unified Communications Manager server for call processing and routing.

APs are critical components in a WLAN because they provide the wireless links or "hot spots" to the network. Cisco requires that the APs supporting voice communications use Cisco IOS Release 12.3(8)JA or later. Cisco IOS software provides features for managing voice traffic.

In some WLANs, each AP has a wired connection to an Ethernet switch, such as a Cisco Catalyst 3750, that is configured on a LAN. The switch provides access to gateways and the Cisco Unified Communications Manager server to support wireless IP telephony.

Some networks have wired components that support wireless components. The wired components could consist of switches, routers, and bridges with special modules to enable wireless capability.

The Cisco Unified WLAN can have the following components:

- Cisco Aironet Series Access Points—802.11a/b/g enterprise-class access points with integrated antennas or antenna connections for easy deployment.
- Cisco 2000 Series Wireless LAN Controller—For small to medium sized networks, such as branch offices. Works with Cisco lightweight access points.
- Cisco 4100 Series Wireless LAN Controller—For medium to large deployments. Works with Cisco lightweight access points.
- Cisco 4400 Series Wireless LAN Controller—For large enterprise facilities. The Cisco 4402 and 4404 models support a maximum of 50 and 100 access points respectively.
- Cisco Wireless LAN Controller Module for Integrated Services Routers—Enables small-to-medium businesses and enterprises to deploy and manage secure WLANs at branch offices.
- Cisco Catalyst 6500 Series Wireless Services Module (WiSM)—Provides security, mobility, redundancy, and ease of use for WLAN administrators.

- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers—Adds wireless LAN controller functions to the stackable Cisco Catalyst 3750G Series Switches to improve operating efficiency, security, mobility, and ease of use for WLAN administrators.
- Wireless Control System (WCS)—Provides a powerful systems management. System administrators can design, control, and monitor enterprise WLANs from a centralized location.
- Cisco 2700 Series Wireless Location Appliance—802.11 based location tracking solution for asset tracking, IT management, and location based security. An open API is included.
- Cisco Wireless LAN Client Adapters—Available in CardBus, PCMCIA and PCI form factors, Cisco Aironet Wireless LAN Client Adapters connect desktop and mobile computing devices to the WLAN in 802.11b-compliant or 802.11a-compliant network.

For more information about Cisco Unified Wireless Networks, refer to http://www.cisco.com/en/US/products/hw/wireless/index.html

Understanding WLAN Standards and Technologies

This section describes the following concepts:

802.11 Standards for WLAN 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 7925G supports the following standards:

- 802.11b—Specifies the radio frequency (RF) of 2.4 GHz for both transmitting and receiving data. Commonly called the Wi-Fi standard.
- 802.11g—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. OFDM is a physical–layer encoding technology for transmitting signals by using RF.
- 802.11a—Uses the 5 GHz band that provides more channels and improved data rates by using OFDM technology. Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) supports this standard.
- 802.11d—Enables APs to communicate available radio channels and acceptable power levels. The Cisco Unified Wireless IP Phone 7925G will always give precedence to 802.11d to determine which channels and powers to use. If the information is unavailable, then the phone will fallback to the locally configured regulatory domain.

Radio Frequency Ranges

WLAN communications use the following RF ranges:

- 2.4 GHz—Does not require licensing. To reduce interference within this bandwidth, WLANs transmit on non-overlapping channels, which are typically limited to three channels, although Japan uses four channels.

  Many devices operate in the 2.4 GHz bandwidth including cordless phones and microwave ovens and can interfere with wireless communications. Interference does not destroy the signal, but can reduce the transmission speed from 11 Mbps to 1 Mbps. RF interference can affect voice quality over the wireless network.

- 5 GHz—Divided into several sections called Unlicensed National Information Infrastructure (UNII) bands and has four channels each. The channels are spaced at 20 MHz to provide non-overlapping channels and more channels than 802.11b or 802.11g.

Table 2-1 lists frequency band ranges and operating channels by regulatory domain.

Table 2-1 Frequency Bands and Operating Channels by Regulatory Domain

Regulatory Domain	Frequency Band Range	Operating Channels
Federal Communications Commission (FCC)	2.412-2.462 GHz	11 channels
Product number is CP-7925GA-K9	5.15-5.25 GHz (UNII-1)	8 of 11 channels
	5.25-5.35 GHz (UNII-2)	
	5.725-5.825 (UNII-3)	
	5.470 - 5.725 (DFS)	
	5.47-5.725 GHz (pending approval	11 channels
ETSI (Europe)	2.412-2.472 GHz	13 channels
Product number is CP-7925GE-K9	5.15-5.725 GHz	19 channels
Japan	2.412-2.472 GHz	13 channels (ODFM)
Product number is CP-7925GPC-CH1-K9	2.412-2.484 GHz	14 channels (CCK)
	5.15-5.35 GHz	8 channels
World Product number is CP-7925GW-K9	—	Uses 802.11d to identify band ranges and channels

802.11 Data Rates, Tx Power, Ranges, and Decibel Tolerances

Table 2-2 lists the Tx power capacities, data rates, ranges in feet and meters, and decibels tolerated by the receiver by 801.11 standard.

Table 2-2 Tx Power, Data Rates, Ranges, and Decibels by Standard

Standard	Maximum Tx Power[1]	Data Rate[2]	Range	Receiver Sensitivity
802.11a				
	40mW	6 Mbps	610 ft (186 m)	-89 dBm
		9 Mbps	610 ft (186 m)	-88 dBm
		12 Mbps	558 ft (170 m)	-86 dBm
		18 Mbps	541 ft (165 m)	-85 dBm
		24 Mbps	508 ft (155 m)	-82 dBm
		36 Mbps	426 ft (130 m)	-80 dBm
		48 Mbps	328 ft (100 m)	-76 dBm
		54 Mbps	295 ft (90 m)	-74 dBm
802.11g				
	40mW	6 Mbps	722 ft (220 m)	-90 dBm
		9 Mbps	656 ft (200 m)	-89 dBm
		12 Mbps	623 ft (190 m)	-87 dBm
		18 Mbps	623 ft (190 m)	-85 dBm
		24 Mbps	623 ft (190 m)	-82 dBm
		36 Mbps	492 ft (150 m)	-78 dBm
		48 Mbps	410 ft (125 m)	-74 dBm
		54 Mbps	394 ft (120 m)	-73 dBm
802.11b				
	50mW	1 Mbps	1,027 ft (313 m)	-95 dBm
		2 Mbps	951 ft (290 m)	-89 dBm
		5.5 Mbps	853 ft (260 m)	-89 dBm
		11 Mbps	787 ft (240 m)	-85 dBm

1. Adjusts dynamically when associating with an AP if the AP client setting is enabled.
2. Advertised rates by the APs are used. If the Restricted Data Rates functionality is enabled in the Cisco Unified Communications Manager Administration phone configuration, then the Traffic Stream Rate Set IE (CCX V4) is used.

Wireless Modulation Technologies

Wireless communications uses the following modulation technologies for signaling:

- Direct-Sequence Spread Spectrum (DSSS)—Prevents interference by spreading the signal 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 identifies its data packets and all others are ignored. Cisco wireless 802.11b/g products use DSSS technology to support multiple devices on the WLAN.

- Orthogonal Frequency Division Multiplexing (OFDM)—Transmits signals by using RF. OFDM is a physical–layer encoding technology that breaks one high-speed data carrier into several lower-speed carriers to transmit in parallel across the RF spectrum. OFDM, when used with 802.11g and 802.11a, can support data rates as high as 54 Mbps.

Table 2-3 provides a comparison of data rates, number of channels, and modulation technologies by standard.

Table 2-3 Data Rates, Number of Channels, and Modulation Technologies by IEEE Standard

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

AP, Channel, and Domain Relationships

APs transmit and receive RF signals over channels within the 2.4 GHz or 5.1 to 5.8 GHz frequency band. To provide a stable wireless environment and reduce channel interference, you must specify non-overlapping channels for each AP. The recommended channels for 802.11b and 802.11g in North America are 1, 6, and 11.

Regulatory domains determine the number of channels that wireless communications can use within the frequency band. Table 2-1 lists the frequency ranges, operating channels, and product numbers for four regulatory domains. The Cisco Unified Wireless IP Phone 7925G uses the fourth domain for all other regions in the world. Wireless LANs in the rest of the world use 802.11d to identify band ranges and channels.

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

The AP coverage area depends on its type of antenna and transmission power. The AP 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, APs need a range overlap of approximately 20 percent to allow uninterrupted connections as phone users roam from one AP to another.

Wireless networks use a service set identifier (SSID). The SSID differentiates one WLAN from another, so all APs and all devices attempting to connect to a specific WLAN must use the same SSID. The SSID groups user devices and associates the group with the APs.

For more information about wireless network components and design, refer to the *Overview: Cisco Unified Wireless Network* at http://www.cisco.com/en/US/solutions/ns175/networking_solutions_products_genericcontent0900aecd80529a5f.html.

For more information about APs, see the "VoIP WLAN Configuration" section on page 2-21.

WLANs and Roaming

Wireless IP phones provide communication mobility to users within the WLAN environment. Unlike cellular phones that have broad coverage, the coverage area for the wireless IP phone is smaller; therefore, phone users frequently roam from one AP 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 AP. The user leaves the building, moves to another building, and then places a call. The phone associates with a different AP in order to place the call from the new location. If the associated AP 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 AP, and then the phone authenticates and associates with the new AP. The previous AP hands the call over to the new AP while maintaining continuous audio connection without user intervention. As long as the APs are in the same Layer 2 subnet, the wireless IP phone keeps the same IP address and the call continues. As a wireless IP phone roams between APs, it must re-authenticate with each new AP. See the "Authentication Methods" section on page 2-16 for information about authentication.

  If the wireless IP phone user moves from an AP that covers IP Subnet A to an AP 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 7925G now supports Layer 3 roaming for autonomous mode APs. 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 APs 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 AP 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 AP to another more easily. During the roaming process, the phone must scan for the nearby APs, determine which AP can provide the best service, and then reassociate with the new AP. 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 AP to the next, CCKM compresses the number of message exchanges during roaming by providing a master key stored on the WDS for the AP 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 QoS in a Wireless Network, page 2-12
- Configuring the Wireless Network for Voice, page 2-22
- VoIP WLAN Configuration, page 2-21

Bluetooth Wireless Technology

Bluetooth Class 2.0 with Extended Data Rate (EDR) is a short-range wireless technology that is supported by the Cisco Unified Wireless IP Phone 7925G. It supports the Hands-Free Profile version 1.5.

Your Cisco Unified Wireless IP Phone 7925G is a qualified Bluetooth wireless device (Qualified Device ID (QDID) B014396) and provides voice communication over the same wireless LAN that your computer uses.

Bluetooth enables low bandwidth wireless connections within a range of 10 meters. The best performance is in the 1 to 2 meter range. Synchronous voice channels are provided by using circuit switching and asynchronous data channels are provided by using packet switching.

Bluetooth wireless technology operates in the 2.4 GHz band which is the same as the 802.11b/g band. There can be a potential interference issues. It is recommended that you:

- Use 802.11a that operates in the 5 GHz band.
- Reduce the proximity of other 802.11b/g devices, Bluetooth devices, microwave ovens, and large metal objects.
- Use the Cisco Unified Wireless IP Phone 7925G on the same side of the body as the Bluetooth-enabled headset.

Pairing Headsets

The Cisco Unified Wireless IP Phone 7925G pairs with headsets using a shared key authentication and encryption method. The authentication process can require a personal identification number (PIN) specific to the headset, commonly "0000." The Cisco Unified Wireless IP Phone 7925G can be paired with more than one headset at a time. Pairing is typically performed once for each headset.

Once a device has been paired, its Bluetooth connection is maintained as long as both devices (phone and headset) are enabled and within range of each other. The connection re-establishes itself automatically if either of the devices powers down then powers up. The green-dotted Bluetooth icon indicates whether or not a device is connected.

When headsets are more than 10 meters away from Cisco Unified Wireless IP Phone 7925G, Bluetooth drops the connection after a 15 to 20 second timeout. If the paired headset comes back into range of the Cisco Unified Wireless IP Phone 7925G and the phone is not connected to another Bluetooth headset, then the in-range Bluetooth headset automatically reconnects. For certain phone types that operate in power-save modes, the user may have to "wake-up" the headset by tapping on its operational button to initiate the reconnect.

Note It is recommended that users read the headset user guide for more information about pairing and connecting the headsets.

Components of the VoIP Wireless Network

The wireless IP phone must interact with several network components in the WLAN to successfully place and receive calls. The following topics describe network components:

- Networking Protocols Used with Cisco Unified Wireless IP Phones, page 2-9
- Interacting with Cisco Unified Wireless APs, page 2-11
- Voice QoS in a Wireless Network, page 2-12
- Interacting with Cisco Unified Communications Manager, page 2-14
- Interacting with the Dynamic Host Configuration Protocol Server, page 2-15

Networking Protocols Used with Cisco Unified Wireless IP Phones

Cisco Unified IP Phones support several networking protocols for voice communication. Table 2-4 describes the networking protocols that the Cisco Unified Wireless IP Phone 7925G supports.

Table 2-4 Supported Networking Protocols

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 QoS configuration information with the Cisco Catalyst switch.
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 Communications Manager System Guide*.
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.
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.
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.
SCCP	Uses Cisco-proprietary messages to communicate between IP devices and Cisco Unified Communications Manager, Release 4.x, 5.1, 6.0, 6.1, and 7.0.	Cisco Unified IP Phones use SCCP protocol for VoIP call signaling and enhanced features such as Message Waiting Indication (MWI).

Table 2-4 Supported Networking Protocols (continued)

Networking Protocol	Purpose	Usage Notes
TCP	Connection-oriented transport protocol.	Cisco Unified IP Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.
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.
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 Communications Manager.
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.

Related Topics

- Understanding the Phone Startup Process, page 3-17
- Components of the VoIP Wireless Network, page 2-9
- Configuring DHCP Settings, page 5-6

Interacting with Cisco Unified Wireless APs

Wireless IP phones use the same APs 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 IP Phones users are mobile and often roam across a campus or between floors in a building while connected to a call. In contrast, data users remain in one place or occasionally move to another location. The ability to roam while maintaining a call is one of the advantages of wireless voice so RF coverage needs to include stairwells, elevators, quiet corners outside conference rooms, and passage ways.

To ensure good voice quality and optimal RF signal coverage, you must perform a site survey. The site survey will determine settings suitable to wireless voice and assist in the design and layout of the WLAN; for example AP 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, install more equipment, or stack large amounts of inventory, you are changing the wireless environment. A post installation survey will verify that the AP coverage is still adequate for optimal voice communications. See the "Site Survey Verification" section on page 2-22 for more information.

Associating to APs

At startup, the Cisco Unified Wireless IP Phone 7925G scans for APs with SSIDs and encryption types that it recognizes. The phone builds and maintains a list of eligible APs and uses the following variables to determine the best AP.

- Received Signal Strength Indicator (RSSI)—Signal strength of available APs within the RF coverage area. The phone attempts to associate with the AP with the highest RSSI value.
- QoS Basic Service Set (QBSS)—Beacon information element (IE) that sends the channel usage of the AP to the wireless IP phone. The phone uses the QBSS value to determine whether the AP can effectively handle more traffic.

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

- Traffic Specification (TSpec)—Calculation of 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 QoS in a Wireless Network" section on page 2-12.

The wireless IP phone associates with the AP with the highest RSSI and lowest channel usage values (QBSS) that have matching SSID and encryption types.To ensure that voice traffic is handled properly, you must configure the correct QoS in the AP. For configuration information, see "Wireless Network Requirements for VoIP" section on page 2-21.

Related Topics

- Security for Voice Communications in WLANs, page 2-16
- VoIP WLAN Configuration, page 2-21

Voice QoS 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 APs that support voice connections on the WLAN.

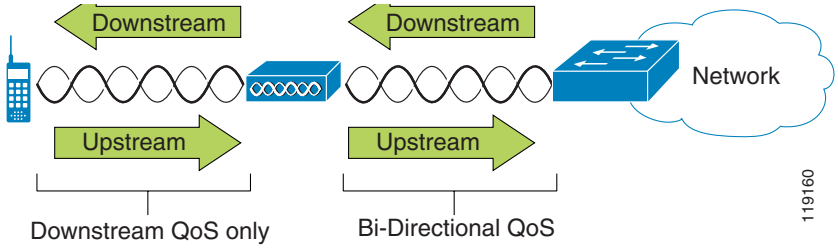
- Voice VLAN—Voice traffic to and from the wireless IP phone
- Data VLAN—Data traffic to and from the wireless PC
- Native VLAN—Data traffic to and from other wireless devices

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 into a voice VLAN and marking voice packets with higher QoS, 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 consider traffic direction when implementing QoS. Traffic is classified as upstream or downstream from the point of view of the AP 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 AP, 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 7925G 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 7925G 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 AP. The Cisco Unified Wireless IP Phone 7925G can integrate layer 2 TSpec admission control with layer 3 Cisco Unified Communications Manager 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 AP (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 QoS 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 7925G sets do not need to be modified. To configure QoS correctly on the AP, see the "Wireless Network Requirements for VoIP" section on page 2-21.

Related Topics

- Authentication Methods, page 2-16
- Interacting with Cisco Unified Communications Manager, page 2-14
- VoIP WLAN Configuration, page 2-21

Interacting with Cisco Unified Communications Manager

Cisco Unified Communications Manager is the call control component in the network that handles and routes calls for the wireless IP phones. Cisco Unified Communications Manager 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 7925G, you must use Cisco Unified Communications Manager Release 4.1, 4.2, 4.3, 5.1, 6.0(1), 6.1(1) or 7.0(1) and SCCP protocol.

Before Cisco Unified Communications Manager can recognize a phone, it must register with Cisco Unified Communications Manager and be configured in the database. For information about setting up phones in Cisco Unified Communications Manager, see the "Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7925G" section on page 1-14.

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

Related Topics

- Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7925G, page 1-14
- Phone Configuration Files and Profile Files, page 2-14

Phone Configuration Files and Profile Files

Configuration files for a phone define parameters for connecting to Cisco Unified Communications Manager and are stored on the TFTP server. In general, any time you make a change in Cisco Unified Communications Manager 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 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 3-17

Interacting with the Dynamic Host Configuration Protocol Server

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage and automate the assignment of 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 7925G 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 Communications Manager 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 7925G, 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 7925G 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 7925G.

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.

Security for Voice Communications in WLANs

Because all WLAN devices that are within range can receive all other WLAN traffic, securing voice communications is critical in WLANs. To ensure that voice traffic is not manipulated or intercepted by intruders, the Cisco Unified Wireless IP Phone 7925G and Cisco Aironet APs are supported in the Cisco SAFE Security architecture. For more information about security in networks, refer to http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html.

This section contains the following items:

Authentication Methods

The Cisco Wireless IP telephony solution provides wireless network security that prevents unauthorized logins and compromised communications by using the following authentication methods.

- Open Authentication—Any wireless device can request authentication in an open system. The AP 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 AP could be non-encrypted or devices can use Wired Equivalent Privacy (WEP) keys to provide security. Devices that are using WEP only attempt to authenticate with an AP that is using WEP.
- Shared Key Authentication—The AP sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device that is requesting authentication uses a pre-configured WEP key to encrypt the challenge text and sends it back to the AP. If the challenge text is encrypted correctly, the AP allows the requesting device to authenticate. A device can authenticate only if its WEP key matches the WEP key on the APs.

  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.
- Wireless Protected Access (WPA) Pre-Shared Key (PSK) Authentication—The AP 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 AP. 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.

- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) Authentication—This client server security architecture encrypts EAP transactions within a Transport Level Security (TLS) tunnel between the AP and the 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 the PAC provisioning delays, set the PAC expiration period to 90 days or longer on the ACS or RADIUS server.

- Extended Authentication Protocol Transport Level Security (EAP-TLS) Authentication—EAP–TLS/RFC 2716 uses the TLS protocol (RFC 2246), which is the latest IETF version of the SSL security protocol. TLS provides a way to use certificates for both user and server authentication, and for dynamic session key generation.

  Microsoft Windows XP provides support for 802.1x, allowing EAP authentication protocols (including EAP-TLS) to be used for authentication. The authentication used in EAP-TLS is mutual: the server authenticates the user and the user authenticates the server. Mutual authentication is required in a WLAN. EAP-TLS provides excellent security but requires client certificate management.

  EAP-TLS uses Public Key Infrastructure (PKI) with the following conditions:

  - Wireless LAN client (user machine) requires a valid certificate to authenticate to the WLAN network.
  - AAA server requires a “server” certificate to validate its identity to the clients.
  - Certificate Authority (CA) server infrastructure issues certificates to the AAA server and the clients.

- Protected Extensible Authentication Protocol (PEAP) Authentication—PEAP uses server-side public key certificates to authenticate clients by creating an encrypted SSL/TLS tunnel between the client and the authentication server.
- PEAP with Server Certificate Authentication—The Cisco Unified Wireless IP Phone 7925G can validate the server certificate during the authentication handshakes over an 802.11 wireless link. This functionality is disabled by default and is enabled in Cisco Unified Communications Manager Administration.

  The exchange of authentication information is encrypted and the user credentials are safe from eavesdropping. MS-CHAP v2 is the supported inner authentication protocol.
- 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 7925G can use LEAP for authentication with the wireless network.

This section describes the following concepts:

- Authenticated Key Management, page 2-18
- Encryption Methods, page 2-18

Authenticated Key Management

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

- WPA—Uses information on a RADIUS server to generate unique 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 AP 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 AP 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 7925G supports WEP, TKIP, and Advanced Encryption Standards (AES) for encryption. When using these mechanisms for encryption, both the signaling Skinny Client Control Protocol (SCCP) packets and voice Real-Time Transport Protocol (RTP) packets are encrypted between the AP and the wireless IP phone.

- WEP—When using WEP in the wireless network, authentication happens at the AP 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 AP for successful connections. The Cisco Unified Wireless IP Phone 7925G supports WEP keys that use 40-bit encryption or a 128-bit encryption and remain static on the phone and AP.

  EAP and CCKM authentication can use WEP keys for encryption. The RADIUS server manages the WEP key and passes a unique key to the AP 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 7925G does not support Cisco Key Integrity Protocol (CKIP) with CMIC.

Choosing AP Authentication and Encryption Methods

Authentication and encryption schemes are setup within the wireless LAN. VLANS are configured in the network and on the APs 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 APs and on the wireless 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 7925G, several choices for both authentication and encryption can be set up on the APs with different SSIDs. When the phone attempts to authenticate, it chooses the AP 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 AP.
- When using Auto (AKM), encryption options are automatically configured for WPA, WPA2, WPA Pre-shared key, WPA2 Pre-shared key, or CCKM.
- In AKM mode, the phone will authenticate with LEAP if it is configured with WPA, WPA2, or CCKM key management.
- The Cisco Unified Wireless IP Phone 7925G does not support auto EAP negotiation; to use EAP-FAST mode, you must specify it.
- If AKM and 802.1x are used, the authentication method is LEAP.
- The Cisco Unified Wireless IP Phone 7925G uses network EAP for 802.1x but you can enable open EAP.

Table 2-7 provides a list of authentication and encryption schemes configured on the Cisco Aironet APs supported by the Cisco Unified Wireless IP Phone 7925G. The table shows the network configuration option for the phone that corresponds to the AP configuration.

Table 2-7 Authentication and Encryption Schemes

Cisco AP Configuration			**Cisco Unified Wireless IP Phone 7925G Configuration**
Authentication	**Key Management**	**Common Encryption**	**Authentication**
Open		None	Open
Open (Static WEP)		WEP	Open+WEP
Shared key (Static WEP)		WEP	Shared+WEP
LEAP 802.1x	Optional CCKM	WEP	LEAP or Auto (AKM)
LEAP WPA	WPA with Optional CCKM	TKIP	LEAP or Auto (AKM)
LEAP WPA2	WPA2	AES	LEAP or Auto (AKM)
EAP-FAST 802.1x	Optional CCKM	WEP	EAP-FAST
EAP-FAST with WPA	WPA Optional CCKM	TKIP	EAP-FAST

Table 2-7 Authentication and Encryption Schemes (continued)

Cisco AP Configuration			Cisco Unified Wireless IP Phone 7925G Configuration
Authentication	**Key Management**	**Common Encryption**	**Authentication**
EAP-FAST with WPA2	WPA2	AES	EAP-FAST
EAP-TLS 802.1x	Optional CCKM	WEP	EAP-TLS
EAP-TLS WPA	WPA with optional CCKM	TKIP	EAP-TLS
EAP-TLS WPA2	WPA2	AES	EAP-TLS
PEAP 802.1x	Optional CCKM	WEP	PEAP
PEAP WPA	WPA with optional CCKM	TKIP	PEAP
PEAP WPA2	WPA2	AES	PEAP
WPA Open and Network EAP	WPA Optional CCKM	TKIP	Auto (AKM) with WPA
WPA-PSK	WPA-PSK	TKIP	Auto (AKM)
WPA2-PSK	WAP2-PSK	AES	Auto (AKM)

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

For more information about configuring authentication and encryption schemes on APs, 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

Related Topics

- Networking Protocols Used with Cisco Unified Wireless IP Phones, page 2-9
- Authentication Methods, page 2-16
- Encryption Methods, page 2-18
- Interacting with Cisco Unified Communications Manager, page 2-14
- Components of the VoIP Wireless Network, page 2-9
- VoIP WLAN Configuration, page 2-21

VoIP WLAN Configuration

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

Wireless Network Requirements for VoIP

The Cisco Unified Wireless IP Phone 7925G supports Cisco Aironet APs (APs) that can run Cisco IOS in autonomous mode and APs that run in lightweight mode with lightweight AP protocol (LWAPP) and use a Cisco Unified wireless LAN controller. Table 2-8 lists the supported AP models and operation mode in the WLAN.

When configuring VoWLAN, use APs that run Cisco IOS Release 12.3(8)JA or later. It is recommended that Cisco Aironet 1130AG, 1240AG, 1250 series APs run Cisco IOS Release 12.3(4g)JA1 or later.

Controllers should be running version 4.0217.0 (minimum) or version 4.2.61.0 or later, which is recommended. The controllers should have Cisco IOS Release 12.3(8)JX or later configured also.

Note Voice over the wireless LAN (VoWLAN) does not currently support MESH technology such as Cisco Aironet 1500 Series Lightweight Outdoor Mesh APs or third-party APs are not supported.

Table 2-8 Supported APs and Modes

AP Models	Autonomous Mode	Lightweight Mode
Cisco Aironet 500 Series	Yes	Yes
Cisco Aironet 1100 Series	Yes	Yes
Cisco Aironet 1130AG Series	Yes	Yes
Cisco Aironet 1200 Series	Yes	Yes
Cisco Aironet 1230 Series	Yes	Yes
Cisco Aironet 1240AG Series	Yes	Yes
Cisco Aironet 1250 Series	Yes	Yes
Cisco Aironet 1300 Series	Yes	Yes
Cisco 1000 Series Lightweight	No	Yes

Note Be aware that Wi-Fi compliant APs that are manufactured by third-party vendors can function with the Cisco Unified Wireless IP Phone 7925G, 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 AP configuration options that are required for optimal voice performance. This is not a complete list of configuration steps or options for deploying APs such as the Cisco Aironet APs. For more information about configuring your AP, refer to the appropriate Cisco Aironet AP installation and configuration guide for your model or the documentation for your AP.

Note When deploying the Cisco Unified Wireless IP Phone 7925G with World regulatory domain (CP-7925GW-K9), you must enable the APs for world mode (802.11d). The world model phone gets the channels and power information from the AP.

To see a list of configuration tasks for the Cisco Aironet AP, controller, and Ethernet switch when setting up VoIP on the WLAN, see the "Configuring a Wireless Network" section on page D-1.

Configuration Tip for Cisco Aironet APs

If you are using EAP-FAST, 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 Cisco Unified wireless LAN controller.

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

Step 3 Enter `save config`

Step 4 Enter `y` to confirm.

Site Survey Verification

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

From the Cisco Unified Wireless IP Phone 7925G, you can use the Neighbor List utility or Site Survey utility from the **SETTINGS > Status** menu.

The Neighbor List utility provides information about the current AP and the closest neighbors tracked by the phone. For more information see Using the Neighbor List Utility, page 2-23.

The Site Survey utility produces a report, written as a temporary HTML file, upon termination of the survey. This Site Survey Report is accessible from the phone web page for viewing or forwarding to Cisco TAC for troubleshooting purposes. For more information, see Using the Site Survey Utility, page 2-24.

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 2-23
- Using the Neighbor List Utility, page 2-23
- Using the Site Survey Utility, page 2-24

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 Communications Manager.
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 10, "Troubleshooting the Cisco Unified Wireless IP Phone 7925G" for assistance with finding the cause of the problem.

Related Topics

- Using the Neighbor List Utility, page 2-23
- Using the Site Survey Utility, page 2-24

Using the Neighbor List Utility

The Neighbor List utility displays a list of the current AP and the closest neighbors tracked by the phone. The phone typically does not scan while it is idle, so often there is only one entry, which is the currently associated AP, in the list.

To use the Neighbor List utility, follow these steps:

Procedure

Step 1 Configure the Cisco Unified Wireless IP Phone 7925G 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 > Neighbor List**.

The phone displays the current AP and the closest neighbors. For example:

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 is an example of the details for a 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.

Using the Site Survey Utility

The Site Survey utility is used to actively and passively scan the wireless medium across all channels and locate APs that belong to the Basic Service Set (BSS). The results of the scans are then used help to identify areas of low coverage, if any, and to determine whether the APs are configured consistently as recommended in the Cisco deployment guidelines.

When you start the Site Survey utility, the phone disassociates from the current AP and remains disassociated for the duration of the operation.

For more information, see Viewing the Site Survey Report on the Web, page 4-38.

Caution During Site Survey, both active and passive scans are performed at a rapid rate. These scans will result in the phone battery life depleting faster than normal and might cause disruption to the wireless medium.

To use the Site Survey utility, follow these steps:

Procedure

Step 1 Configure the Cisco Unified Wireless IP Phone 7925G 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 APs within range that have the same SSID and security settings as the phone. To see more information about an AP, scroll to the desired line and press **Details**.

Step 4 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 5 Adjust AP and antenna placement and AP power settings to provide approximately 20 percent coverage overlap.

Step 6 When you terminate the site survey, a report is generated for your viewing from the phone web page. For more information, see Viewing the Site Survey Report on the Web, page 4-38.

In addition to the Site Survey utility in the Cisco Unified Wireless IP Phone 7925G, 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 Topics

- Performing a Site Survey Verification, page 2-23
- Viewing the Site Survey Report on the Web, page 4-38