



An Overview of the Wireless Network

With the introduction of wireless communication, mobile wireless IP phones can provide voice communication within the corporate wireless local area network (WLAN). The Cisco Wireless IP Phone 7920 depends upon and interacts with wireless access points and key Cisco IP telephony components, including Cisco CallManager, to provide wireless voice communication.

This chapter provides you with an overview of the interaction between the Cisco Wireless IP Phone 7920 and other key components of the Voice-over-IP (VoIP) network in the WLAN environment.

- [Understanding the Wireless LAN, page 2-1](#)
- [Components of the VoIP Wireless Network, page 2-5](#)
- [Wireless Network and Access Point Configuration, page 2-19](#)
- [Understanding the Phone Startup Process, page 2-21](#)

Understanding the Wireless LAN

This section includes the following topics about WLANs.

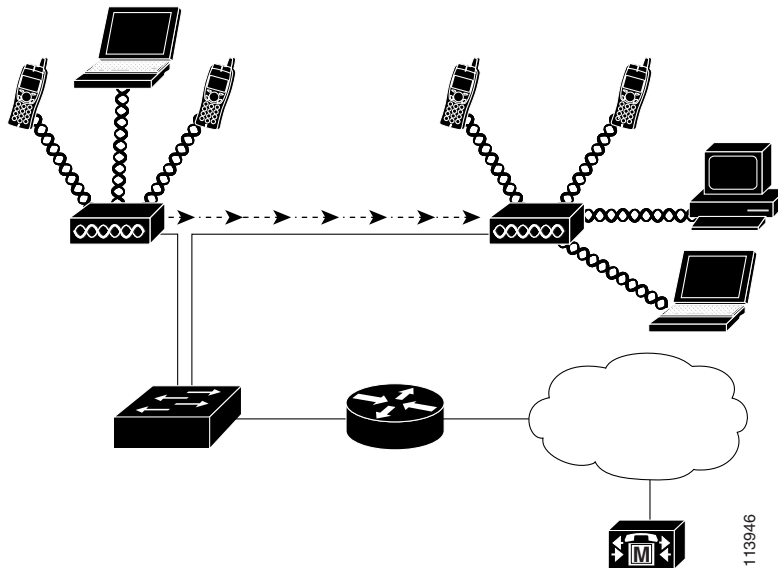
- [The 802.11 Standards for Wireless LAN Communications, page 2-2](#)
- [Connecting to the Wireless Network, page 2-3](#)
- [Securing Voice Communications, page 2-4](#)

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 Cisco Wireless IP Phone 7920 models.

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 packets are sent to the Cisco CallManager server for call processing and routing.

Figure 2-1 Wireless LAN with Cisco Wireless IP Phone 7920s



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 802.11b standard is the most prevalent standard in wireless

LAN communications and is commonly called WiFi. The 802.11b standard specifies the radio frequency (RF) of 2.4 GHz for both transmitting and receiving data at speeds of 1, 2, 5.5 and 11 Mbps.

The 2.4 GHz RF range is an open frequency range that does not require licensing. 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.

To help prevent interference, direct-sequence spread spectrum (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 products use DSSS technology to support multiple devices on the WLAN.

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 12.2(15)JA or later. Cisco IOS provides features for managing voice traffic. The Cisco Aironet Access Points that support IOS include the following access point series:

- Cisco Aironet Access Point 350
- Cisco Aironet Access Point 1100
- Cisco Aironet Access Point 1200

Each access point has a hard-wired connection to a network layer switch, such as a Cisco Catalyst 4000, that is configured on the LAN. The switch provides access to gateways and the Cisco CallManager server to support wireless IP telephony (WIPT).

Access points transmit and receive RF signals over channels within the 2.4 GHz frequency band. Regulatory domains determine the number of channels that wireless communications can use within the 2.4 GHz frequency band. The Cisco Aironet Access Points support up to 11 communication channels in North America, 13 channels in Europe (ETSI) and 14 channels in Japan. 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 are 1, 6, and 11 in North America.

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, 50, and 100mW. 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 network devices use a service set identifier (SSID). The SSID provides a way to group a set of user devices that can associate with a set of access points. Each wireless device that can use the access point is configured with the same SSID as the access point. For more information about configuring the access points, refer to the *Cisco Wireless IP Phone 7920 Design and Deployment Guide*.

Securing 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 Wireless IP Phone 7920 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 WiFi 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 the following additional security areas:

- Wireless network security that prevents unauthorized logins and compromised communications by using encryption and authentication with Wired Equivalent Privacy (WEP), Wireless Protected Access (WPA) and Cisco Light Extensible Authentication Protocol (LEAP)
- Password protection for directories and databases that includes a Cisco Wireless IP Phone 7920 phone lock password.

Related Topics

- [Networking Protocols Used with Cisco Wireless IP Phones, page 2-6](#)
- [Security Mechanisms in the Wireless Network, page 2-13](#)

Components of the VoIP Wireless Network

The Cisco Wireless IP Phone 7920 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 Wireless IP Phones, page 2-6](#)
- [Interacting with the Cisco Aironet Access Point, page 2-8](#)
- [Roaming in a Wireless Network, page 2-10](#)
- [Voice Quality in a Wireless Network, page 2-12](#)
- [Security Mechanisms in the Wireless Network, page 2-13](#)
- [Interacting with Cisco CallManager, page 2-17](#)
- [Interacting with the DHCP Server, page 2-18](#)

Networking Protocols Used with Cisco Wireless IP Phones

Cisco IP Phones support several industry-standard and Cisco networking protocols for voice communication. [Table 2-1](#) provides an overview of the networking protocols that the Cisco Wireless IP Phone 7920 supports.

Table 2-1 Supported Networking Protocols on the Cisco Wireless IP Phone 7920

Networking Protocol	Purpose	Usage Notes
Cisco Centralized Key Management (CCKM)	Key generation protocol used for fast authentication in wireless networks.	Cisco Wireless IP Phone 7920 uses CCKM for fast, secure roaming between access points.
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.	The Cisco IP Phone uses 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.
Cisco Light Extensible Authentication Protocol (LEAP)	Proprietary password-based mutual authentication scheme between the client (phone) and a RADIUS server.	Cisco Wireless IP Phone 7920 uses LEAP 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 <i>Cisco CallManager System Guide</i> .

Table 2-1 Supported Networking Protocols on the Cisco Wireless IP Phone 7920 (continued)

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 IP Phone with DHCP. If you are not using DHCP, you must manually assign these properties to each phone locally.
Real-Time Transport (RTP)	Standard for transporting real-time data, such as interactive voice and video, over data networks.	Cisco 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 CallManager.	Cisco 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 Wireless IP Phone 7920 uses TKIP/MIC algorithms to secure and preserve the integrity of voice communications.
Transmission Control Protocol (TCP)	Connection-oriented transport protocol.	Cisco IP Phones use TCP to connect to Cisco CallManager and to access XML services.
Trivial File Transfer Protocol (TFTP)	Method for transferring files over the network. On the Cisco 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.
User Datagram Protocol (UDP)	Connectionless messaging protocol for delivery of data packets.	Cisco IP Phones receive and process UDP messages. RTP voice traffic runs over UDP.

Table 2-1 Supported Networking Protocols on the Cisco Wireless IP Phone 7920 (continued)

Networking Protocol	Purpose	Usage Notes
Wi-Fi (802.11b)	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 Wireless IP Phone 7920 uses the 802.11b standard with a range of 2.4-2.497 GHz RF and dynamic data rate scaling of 1, 2, 5.5, and 11 Mbps.
Wired Equivalent Privacy (WEP)	Wireless security protocol for encrypting data that uses an encryption key stored on the phone and access point.	Cisco Wireless IP Phone 7920 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 Wireless IP Phone 7920 supports both WPA and WPA Pre-shared key authentication, including encryption using TKIP and MIC (message integrity check)

Related Topics

- [Understanding the Phone Startup Process, page 2-21](#)
- [Components of the VoIP Wireless Network, page 2-5](#)
- [Modifying DHCP Settings, page 5-4](#)
- [Configuring TFTP Option, page 5-9](#)

Interacting with the Cisco Aironet Access Point

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 while searching a web page might

cause the page to display slowly and might annoy the end user. However, packet loss during voice transmission can cause choppy or broken audio and make the phone call inaudible.

Wireless voice users are mobile and can roam across a campus or between floors in a building while they are connected to a call. Alternately, data users might move their PC to another location, but they reconnect at the new 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; for example, power levels, channel assignments, and access point placement. For more information about the site survey, refer to the *Cisco Wireless IP Phone 7920 Design and Deployment Guide*.

After deploying and using wireless voice, you should continue to perform post installation site surveys to verify that the locations of the access points and their configuration continues to meet the needs of your wireless voice users. 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 “Performing a Site Survey Verification” section on page 6-7 for more information.

Associating to an Access Point

At startup, the Cisco Wireless IP Phone 7920 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 two 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 Basis Service Set (QBSS)—The access point uses this beacon information element (IE) to send the channel utilization of the access point to the Cisco Wireless IP Phone. The phone uses the QBSS value to determine whether the access point can effectively handle more traffic.

The Cisco Wireless IP Phone associates with the access point with the highest RSSI and lowest channel utilization values (QBSS) that have matching SSID and encryption types.

Related Topics

- [Roaming in a Wireless Network, page 2-10](#)
- [Securing Voice Communications, page 2-4](#)
- [Wireless Network and Access Point Configuration, page 2-19](#)

Roaming in a Wireless Network

Cisco Wireless IP Phone users have the ability to move from one location in the premises to another while conversing on the phone. Unlike cellular phones that have broad coverage, the coverage area for the Cisco Wireless IP Phone is smaller; therefore, phone users must roam from one access point to another more frequently. To understand some of the limitations of roaming with wireless IP phones, the following examples provide information about roaming in the WLAN.

- Pre-call Roaming—A Cisco Wireless IP Phone 7920 user powers on the phone in the office, and the phone associates with the nearby access point. The user leaves the building and moves to another building where he 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.
- Mid-call Roaming—A Cisco Wireless IP Phone 7920 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 the phone authenticates and associates with the new access point. The current 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 Cisco Wireless IP Phone keeps the same IP address and the call continues. As a Cisco Wireless IP Phone roams between access points, it must re-authenticate with each new access point. See the “[Security Mechanisms in the Wireless Network](#)” section on page 2-13 for information about authentication.

If the Cisco Wireless 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.

With the release of the Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM), the Cisco Wireless IP Phone 7920 now supports Layer 3 roaming. 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/wlm_1_1/index.htm

- **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 Cisco Wireless IP Phone 7920 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, then reassociate with the new access point. When implementing stronger authentication methods, such as WPA and LEAP, the number of information exchanges increases and causes more delay during roaming. 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

To solve this issue, 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.

Related Topics

- [Voice Quality in a Wireless Network, page 2-12](#)

- [Interacting with the Cisco Aironet Access Point, page 2-8](#)
- [Wireless Network and Access Point Configuration, page 2-19](#)

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. 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
- Native VLAN—Data traffic to and from the wireless PC (native VLAN)

Assign separate SSIDs to the voice and to the data VLANs. You can also configure a separate management VLAN in the WLAN, but 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. You can management traffic resulting in lower delay and fewer lost packets.

For more information, refer to the *Cisco Wireless IP Phone 7920 Design and Deployment Guide*.

Related Topics

- [Security Mechanisms in the Wireless Network, page 2-13](#)
- [Interacting with Cisco CallManager, page 2-17](#)
- [Wireless Network and Access Point Configuration, page 2-19](#)

Security 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 Cisco Wireless IP Phone 7920 can use these authentication methods in the WLAN:

- **Open Authentication**—In an Open system, any wireless device can request authentication. 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**—During 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 encrypts the challenge text using a pre-configured WEP key 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 keys match the WEP keys 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 (or password phrase) is used to create unique pair-wise keys that are exchanged between each phone and the access point. You can configure the password phrase as a 64-character hexadecimal string or as an ASCII password of from 8 to 63 characters in length. Because the pre-shared key password is stored on the phone, it can be compromised if the phone is lost or stolen.
- **LEAP Authentication**—For maximum security, client devices can authenticate to the network by using a Remote Authentication Dial-in User Service (RADIUS) server such as the Cisco Access Control Server (ACS).

Cisco LEAP is a proprietary authentication protocol that requires a LEAP-compliant RADIUS server. LEAP allows wireless devices to mutually authenticate by using a username and password through a centralized RADIUS server user database.

When a Cisco Wireless IP Phone roams from one access point to another, the next access point requires LEAP authentication, also. The voice stream will not flow until the LEAP authentication is completed at the next access point through the centralized RADIUS server.

To reduce the amount of delay between the access point and the RADIUS server, carefully plan where to locate the RADIUS server. A local RADIUS server introduces less delay during roaming than a remote RADIUS server. Small, remote offices can use a RADIUS server on the Cisco access point to authenticate up to 50 users.

Authenticated Key Management

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

- **WiFi 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 LEAP 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 Wireless IP Phone 7920 supports Wired Equivalent Privacy (WEP) and Temporal Key Integrity Protocol (TKIP) for encryption. When you use either mechanism for encryption, both the signaling (SCCP) packets and voice (RTP) packets are encrypted between the access point and the Cisco Wireless 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 with the WEP key that is configured at the access point for successful connections. The Cisco Wireless IP Phone 7920 supports WEP keys that use 40-bit encryption or a 128-bit encryption and remain static on the phone and access point.

LEAP 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.

- Temporal Key Integrity Protocol (TKIP)—WPA and CCKM use TKIP encryption that has several improvements over WEP. TKIP provides per-packet key cipherng 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.

**Note**

The Cisco Wireless IP Phone 7920 does not support Cisco Key Integrity Protocol (CKIP) with CMIC or Advanced Encryption Standard (AES) encryption.

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 scheme requirements on the access points and on the wireless client devices, such as the Cisco Wireless IP Phone.

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

When using Authenticated Key Management (AKM) for the Cisco Wireless IP Phone 7920, several choices for both authentication and encryption can be set up on the access points with different SSIDs. When the Cisco Wireless IP Phone attempts to authenticate, it chooses the access point that advertises the authentication and encryption scheme that the phone can support. AKM can authenticate by using WPA Pre-shared key, WPA, or CCKM.

When you set up AKM on the phone, the access point can provide the encryption key when using WPA Pre-shared key or the key can be configured on the phone when using WEP. When using AKM, encryption options include WPA Pre-shared key, TKIP for WPA authentication, and TKIP or WEP for CCKM authentication.

For more information about authentication and encryption schemes and how they are configured, 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 2-2 provides a list of authentication and encryption schemes configured on the Cisco Aironet Access Points supported by the Cisco Wireless IP Phone 7920. The table shows the network configuration option for the phone that corresponds to the access point configuration.

Table 2-2 Authentication and Encryption Schemes

Access Point Configuration		Cisco Wireless IP Phone 7920	
Authentication	Encryption	Authentication	Encryption
Open	Static WEP (optional)	Open (optional)	None or Static WEP
Shared key	Static WEP (mandatory)	Shared Key	Static WEP (mandatory)
Network EAP	WEP	LEAP	WEP
Network EAP	TKIP or WEP (WDS required for CCKM)	AKM with CCKM	TKIP or WEP
Network EAP,	TKIP with WPA	AKM with WPA	TKIP
Open	TKIP with WPA or WPA Pre-shared Key	AKM with WPA Pre-shared Key	TKIP

Related Topics

- [Interacting with Cisco CallManager, page 2-17](#)
- [Components of the VoIP Wireless Network, page 2-5](#)
- [Wireless Network and Access Point Configuration, page 2-19](#)

Interacting with Cisco CallManager

Cisco CallManager is the call control component in the network that handles and routes calls for the Cisco Wireless IP Phone 7920. Cisco 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. You must use Cisco CallManager Release 3.3(3) SR1 or later for wireless voice deployments.

Before Cisco CallManager can recognize a phone, it must register with Cisco CallManager and be configured in the database. For information about setting up phones in Cisco CallManager, see the “[Configuring IP Phones in Cisco CallManager](#)” section on page 3-6.

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

Related Topics

- [Configuring Cisco Wireless IP Phones in Cisco CallManager, page 7-2](#)
- [Phone Configuration Files and Profile Files, page 2-17](#)

Phone Configuration Files and Profile Files

Configuration files for a phone define parameters for connecting to Cisco CallManager and are stored on the TFTP server. In general, any time you make a change in Cisco 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 `SEPxxxxxxxxxxxx.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 2-21](#)

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 Wireless IP Phone 7920 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 CallManager network.

The DHCP scope settings include the following:

- TFTP server
- 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 Wireless IP Phone 7920, as shown in [Table 2-3](#).

Table 2-3 DHCP Settings Priority

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

If DHCP is disabled, the Cisco Wireless IP Phone 7920 uses the following network settings to perform the phone provisioning bootup process. You must configure these static parameters for each Cisco Wireless IP Phone 7920.

- Primary TFTP server IP
- Primary DNS server IP
- Secondary DNS server IP
- IP address
- Subnet mask IP
- Primary gateway IP

Wireless Network and Access Point Configuration

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 installing 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.

When configuring a wireless voice LAN, use access points that run Cisco IOS Version 12.2(15)JA or later. The access points that run IOS include the following:

- Cisco Aironet Access Point 350 series
- Cisco Aironet Access Point 1100 series
- Cisco Aironet Access Point 1200 series

- Cisco Aironet Access Point 1300 series

Table 2-4 explains and provides references for many of the configuration activities for the Cisco Aironet Access Point.

Table 2-4 Cisco Aironet Access Point Configuration Tasks

Activity	Explanation	Reference
Check that the Cisco IOS version is the recommended version	Under System Software, check for Cisco IOS version 12.2(15)JA or later.	Refer to the <i>Cisco Wireless IP Phone 7920 Design and Deployment Guide</i> Interacting with the Cisco Aironet Access Point, page 2-8
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.	Refer to the <i>Cisco Wireless IP Phone 7920 Design and Deployment Guide</i> Voice Quality in a Wireless Network, page 2-12
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.	Refer to the <i>Cisco Wireless IP Phone 7920 Design and Deployment Guide</i> Interacting with the Cisco Aironet Access Point, page 2-8
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.	Refer to the <i>Cisco Wireless IP Phone 7920 Design and Deployment Guide</i> Voice Quality in a Wireless Network, page 2-12
Enable ARP caching	Enable this option to ensure two-way audio. The access point has ARP caching disabled by default.	Refer to the <i>Cisco Wireless IP Phone 7920 Design and Deployment Guide</i>

Table 2-4 Cisco Aironet Access Point Configuration Tasks (continued)

Activity	Explanation	Reference
Configure radio (802.11b) settings	<p>Data Rate—Allow only 11 Mbps unless you have special device requirements.</p> <p>Client Transmit Power—After a site survey, determine the appropriate power requirements and set a specific Client Transmit Power setting. The Cisco Wireless IP Phone 7920 uses the same setting as the access point.</p> <p>Note If set for Max, the access point does not advertise Client Transmit Power setting.</p>	Refer to the <i>Cisco Wireless IP Phone 7920 Design and Deployment Guide</i>
Configure Security for the voice VLANs	<p>Use one of these authentication and encryption options for the SSID that corresponds to the voice VLAN:</p> <ul style="list-style-type: none"> • Open • Shared Key • LEAP • AKM 	Refer to the <i>Cisco Wireless IP Phone 7920 Design and Deployment Guide</i> Choosing Authentication and Encryption Methods, page 2-15

Related Topics

- [Network Requirements, page 3-2](#)
- [Configuring IP Phones in Cisco CallManager, page 3-6](#)
- [Installing the Cisco Wireless IP Phone 7920, page 3-13](#)

Understanding the Phone Startup Process

When connecting to the wireless VoIP network, the Cisco Wireless IP Phone 7920 goes through a standard startup process, as described in [Table 2-5](#). Depending on your specific network configuration, not all of these steps may occur on your Cisco Wireless IP Phone.

Table 2-5 Cisco IP Phone Startup Process

Step	Description	Related Topics
1. Powering on the phone	The Cisco Wireless IP Phone 7920 has non-volatile Flash memory in which it stores firmware images and user-defined preferences. At startup, the phone runs a bootstrap loader that loads a phone image stored in Flash memory. Using this image, the phone initializes its software and hardware.	Providing Power to the Cisco IP Phone, page 3-17 Resolving Startup and Connectivity Problems, page 9-2
2. Scanning for an access point	The Cisco Wireless IP Phone 7920 scans the RF coverage area with its radio. The phone scans its network profiles and searches for access points that have a matching SSID and authentication type. The phone associates with the access point with the highest RSSI and lowest channel utilization (QBSS) that matches with its network profile.	Interacting with the Cisco Aironet Access Point, page 2-8 Resolving Startup and Connectivity Problems, page 9-2

Table 2-5 Cisco IP Phone Startup Process (continued)

Step	Description	Related Topics
<p>3. Authenticating with access point</p>	<p>The Cisco Wireless IP Phone 7920 begins the authenticating process.</p> <ul style="list-style-type: none"> • If set for Open, then any device can authenticate to the access point. For added security, static WEP encryption might optionally be used. • If set to Shared Key, the phone encrypts the challenge text using the WEP key and the access point must verify that the WEP key was used to encrypt the challenge text before network access is available. • If set for LEAP, then the LEAP user name and password are authenticated by the RADIUS server before network access is available. • If set for AKM, the phone looks for an access point with one of the following key management options enabled: <ul style="list-style-type: none"> – WPA or CCKM—The phone authenticates with the RADIUS server. – WPA-PSK—The phone authenticates with the access point using the pre-shared key password. 	<p>Security Mechanisms in the Wireless Network, page 2-13</p>

Table 2-5 Cisco IP Phone Startup Process (continued)

Step	Description	Related Topics
4. Configuring IP network	<p>If the Cisco Wireless IP Phone is using DHCP to obtain an IP address, the phone queries the DHCP server to obtain one. If you are not using DHCP in your network, you must assign a static IP address to each phone locally.</p> <p>In addition to assigning an IP address, the DHCP server directs the Cisco Wireless IP Phone to a TFTP server. If the phone has a statically defined IP address, you must configure the TFTP server IP address locally on the phone; the phone then contacts the TFTP server directly.</p>	<ul style="list-style-type: none"> • Modifying DHCP Settings, page 5-4 • Configuring Static Settings, page 5-6 • Resolving Startup and Connectivity Problems, page 9-2
5. Downloading Load ID	<p>The Cisco Wireless IP Phone checks to verify that the proper firmware is installed or if new firmware is available to download.</p> <p>Cisco CallManager informs devices using .cnf or .cnf.xml format configuration files of their load ID. Devices using .xml format configuration files receive the load ID in the configuration file.</p>	<ul style="list-style-type: none"> • Phone Configuration Files and Profile Files, page 2-17
6. Downloading config file	<p>The TFTP server has configuration files and profile files. A configuration file includes parameters for connecting to Cisco CallManager and information about which image load a phone should be running. A profile file contains various parameters and values for phone and network settings.</p>	<ul style="list-style-type: none"> • Configuring TFTP Option, page 5-9 • Phone Configuration Files and Profile Files, page 2-17 • Resolving Startup and Connectivity Problems, page 9-2

Table 2-5 Cisco IP Phone Startup Process (continued)

Step	Description	Related Topics
7. Connecting to Cisco CallManager	The configuration file defines how the Cisco IP Phone communicates with Cisco CallManager. After obtaining the file from the TFTP server, the phone attempts to make a TCP connection to the highest priority Cisco CallManager on the list.	<ul style="list-style-type: none"> • Interacting with Cisco CallManager, page 2-17 • Resolving Startup and Connectivity Problems, page 9-2
8. Registering to Cisco CallManager	If the phone was manually added to the database, Cisco CallManager identifies and registers the phone. If the phone was not manually added to the database and auto-registration is enabled in Cisco CallManager, the phone attempts to auto-register itself in the Cisco CallManager database.	<ul style="list-style-type: none"> • Configuring IP Phones in Cisco CallManager, page 3-6 • Adding Users to Cisco CallManager, page 7-13

Related Topics

- [Configuring Cisco Wireless IP Phones in Cisco CallManager, page 7-2](#)
- [Phone Configuration Files and Profile Files, page 2-17](#)

