Wi-Fi Network Setup

Network Requirements

For the device to successfully operate as an endpoint in your network, your network must meet the following requirements:

- VoIP Network
  - VoIP is configured on your Cisco routers and gateways.
  - Cisco Unified Communications Manager is installed in your network and is configured to handle call processing.
- IP network that supports DHCP or manual assignment of IP address, gateway, and subnet mask

Note The device displays the date and time from Cisco Unified Communications Manager. If the user unchecks **Automatic Date & time** in the Settings application, the time may become out of sync with the server time.

- Wireless LAN
  - Access Points (APs) are configured to support voice and video over WLAN.
  - Controllers and switches are configured to support voice and video.
  - Security is implemented for authenticating wireless voice devices and users.

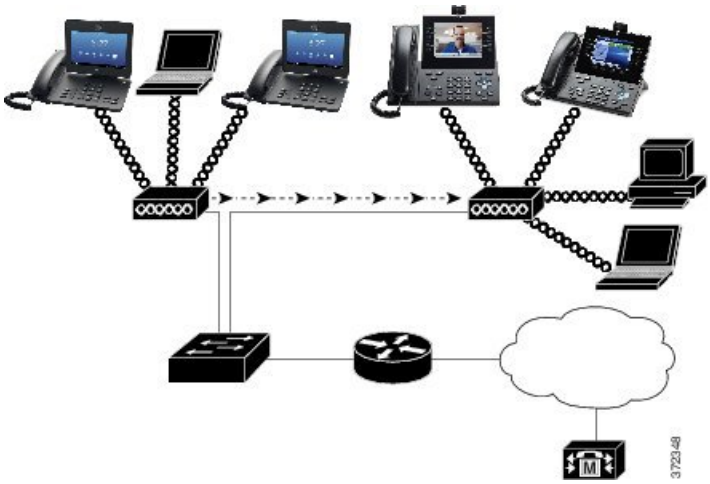
Wireless LAN

Note For instructions on deploying and configuring a wireless Cisco DX Series device, see the *Cisco DX Series Wireless LAN Deployment Guide*.

Devices with wireless capability can provide voice communication within the corporate WLAN. The device depends on and interacts with wireless access points (AP) and key Cisco IP Telephony components, including Cisco Unified Communications Manager Administration, to provide wireless voice communication.

Cisco DX Series devices exhibit Wi-Fi capabilities that can use 802.11a, 802.11b, 802.11g, and 802.11n Wi-Fi.

The following figure shows a typical WLAN topology that enables the wireless transmission of voice for wireless IP telephony.



When a Cisco DX Series device powers on, it searches for and associates with an AP if the device wireless access is set to On. If remembered networks are not within range, you can select a broadcasted network or manually add a network.

The AP uses the 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. 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 contain wired components that support wireless components. The wired components can comprise switches, routers, and bridges with special modules to enable wireless capability.

For more information about Cisco Unified Wireless Networks, see http://www.cisco.com/c/en/us/products/wireless/index.html.

Wi-Fi Network Components

The device must interact with several network components in the WLAN to successfully place and receive calls.

AP Channel and Domain Relationships

Access points (APs) transmit and receive RF signals over channels within the 2.4 GHz or 5 GHz frequency band. To provide a stable wireless environment and reduce channel interference, you must specify nonoverlapping channels for each AP.

For more information about AP channel and domain relationships, see the "Designing the Wireless LAN for Voice" section in the *Cisco DX Series Wireless LAN Deployment Guide*.

AP Interactions

Cisco DX Series devices 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 can make the call inaudible. Packet errors can also cause blocky or frozen video.

Because the device is a desktop (not mobile) endpoint, changes in the local environment can cause devices to roam between access points and can affect the voice and video performance. 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 passageways.

To ensure good voice quality and optimal RF signal coverage, you must perform a site survey. The site survey determines settings that are suitable to wireless voice and assists 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 postinstallation 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 postinstallation survey verifies that the AP coverage is still adequate for optimal voice communications.

Note Packet loss occurs during roaming; however, the security mode and the presence of fast roaming determines how many packets are lost during transmission. Cisco recommends implementation of Cisco Centralized Key Management (CCKM) to enable fast roaming.

For more information about Voice QoS in a wireless network, see the *Cisco DX Series Wireless LAN Deployment Guide*.

Access Point Association

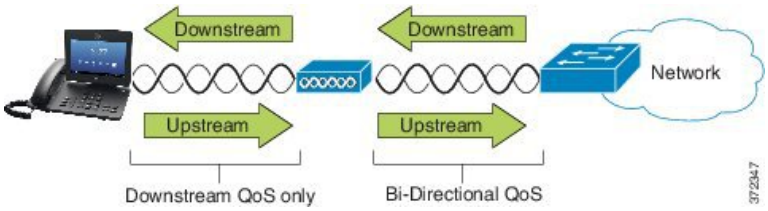
At startup, the device scans for APs with SSIDs and encryption types that it recognizes. The device builds and maintains a list of eligible APs and selects the best AP based on the current configuration.

QoS in Wireless Network

Voice and video 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 can seriously impact a voice or video call. To ensure that voice and video traffic receives timely and reliable treatment with low delay and low jitter, you must use Quality of Service (QoS).

By separating the devices into a voice VLAN and marking voice packets with higher QoS, you can ensure that voice traffic gets priority treatment over data traffic, which results 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 relative to the AP as shown in the following figure.



The Enhanced Distributed Coordination Function (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 up to eight queues on the AP can be set up, you should use only three queues for voice, video, and signaling traffic to ensure the best possible QoS. Place voice in the Voice queue (UP6), video in the Video queue (UP5), signaling (SIP) traffic in the Video queue (UP4), and place data traffic in a best-effort queue (UP0). 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.

The queues are:

- Best Effort (BE) - 0, 3
- Background (BK) - 1, 2
- Video (VI) - 4, 5
- Voice (VO) - 6, 7

Note The device marks the SIP signaling packets with a DSCP value of 24 (CS3) and RTP packets with DSCP value of 46 (EF).

Note Call Control (SIP) is sent as UP4 (VI). Video is sent as UP5 (VI) when Admission Control Mandatory (ACM) is disabled for video (Traffic Specification [TSpec] disabled). Voice is sent as UP6 (VO) when ACM is disabled for voice (TSpec disabled).

The following table provides a QoS profile on the AP that gives priority to voice, video, and call control (SIP) traffic.

Table 1: QoS Profile and Interface Settings

Traffic Type	DSCP	802.1p	WMM UP	Port Range
Voice	EF (46)	5	6	UDP 16384-32767
Interactive Video	AF41 (34)	4	5	UDP 16384-32767
Call Control	CS3 (24)	3	4	TCP 5060-5061

To improve reliability of voice transmissions in a nondeterministic environment, the device 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. 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 issues with call quality, an initial Call Admission Control (CAC) scheme is required. With SIP CAC enabled on the WLAN, QoS is maintained in a network overload scenario by limiting the number of active voice calls so as not to exceed the configured limits on the AP. During times of network congestion, the system maintains a small bandwidth reserve so wireless device clients can roam into a neighboring AP, even when the AP is at “full capacity.” After the voice bandwidth limit is reached, the next call is load-balanced to a neighboring AP so as not to affect the quality of the existing calls on the channel.

Note Cisco DX Series devices use TCP for SIP communications, and Cisco Unified Communications Manager registrations can potentially be lost if an AP is at full capacity. Frames to or from a client that has not been "authorized" through the CAC can be dropped, leading to Cisco Unified Communications Manager deregistration. Therefore, Cisco recommends that you disable SIP CAC.

Note The DSCP, COS, and WMM UP markings correctly display for the optimum transmission of video frames. The device does not support Voice and Video CAC; Cisco recommends that you implement SOP CAC.

The devices use the Flexible DSCP and Video Promotion feature to resolve inconsistent QoS and inconsistent bandwidth accounting when a video occurs with a different type of device.

Set Up Flexible DSCP

Procedure

Step 1 In Cisco Unified Communications Manager Administration, go to **System** > **Service Parameters**.

Step 2 In Clusterwide Parameters (System - Location and Region), set Use Video BandwidthPool for Immersive Video Calls to **False**.

Step 3 In Clusterwide Parameters (Call Admission Control), set Video Call QoS Marking Policy to **Promote to Immersive**.

Step 4 Save your changes.

Cisco Unified Communications Manager Interaction

Cisco Unified Communications Manager manages the components of the IP telephony system (the endpoints, access gateways, and the resources) for such features as call conferencing and route planning.

Cisco DX Series devices are supported by Cisco Unified Communications Manager Release 8.5(1), 8.6(2), 9.1(2), 10.5(1) and later.

Cisco Unified Communications Manager cannot recognize a device until the device is registered and configured in the database.

You can find more information about configuring Cisco Unified Communications Manager to work with IP devices in the *Cisco Unified Communications Manager Administration Guide*, the *Cisco Unified Communications Manager System Guide*, and the *Cisco DX Series Wireless LAN Deployment Guide*.

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. Cisco DX Series devices support the following standards:

- 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) support this standard.
- 802.11b: Specifies the radio frequency (RF) of 2.4 Ghz for both transmission and receipt of data at lower data rates (1, 2, 5.5, 11 Mbps).
- 802.11d: Enables access points to advertise their currently supported radio channels and transmit power levels. The 802.11d-enabled client then uses that information to determine the channels and powers to use. The device requires World mode (802.11d) to determine which channels are legally allowed for any given country. For supported channels, see the table that follows. Ensure that 802.11d is properly configured on the Cisco IOS Access Points or Cisco Unified Wireless LAN Controller.

- 802.11e: Defines a set of Quality of Service (QoS) enhancements for wireless LAN applications.
- 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 transmission of signals through use of RF.
- 802.11h: 5 GHz spectrum and transmit power management. Provides DFS and TPC to the 802.11a Media Access Control (MAC).
- 802.11i: Specifies security mechanisms for wireless networks.
- 802.11n: Uses the radio frequency of 2.4 GHz or 5 GHz for both transmission and receipt of data, and enhances data transfer through the use of multiple input, multiple output (MIMO) technology, channel bonding, and payload optimization.

Note Cisco DX Series devices have a single antenna and use the Single Input Single Output (SISO) system, which supports MCS 0 to MCS 7 data rates only (72 Mbps with 20 MHz channels and 150 Mbps 40 MHz channels). Optionally, you can enable MCS 8 to MCS 15 if 802.11n clients are using MIMO technology that can take advantage of those higher data rates.

Table 2: Supported Channels for Cisco DX Series Devices

Band Range	Available Channels	Channel Set
2.412 - 2.472 GHz	13	1 - 13
5.180 - 5.240 GHz	4	36, 40, 44, 48
5.260 - 5.320 GHz	4	52, 56, 60, 64
5. 500 - 5.700 GHz	11	100 - 140
5.745 - 5.825 GHz	5	149, 153, 157, 161, 165

Note Channels 120, 124, 128 are not supported in the Americas, Europe, or Japan, but may be in other regions around the world.

For information about supported data rates, Tx power and Rx sensitivity for WLANs, see the *Cisco DX Series Wireless LAN Deployment Guide*.

World Mode (802.11d)

Cisco DX Series devices use 802.11d to determine the channels and transmit power levels to use. The device inherits its client configuration from the associated AP. Enable World mode (802.11d) on the AP to use the

device in World mode. For more information on enabling World mode, see the *Cisco DX Series Wireless LAN Deployment Guide*

Note Enablement of World mode (802.11d) may not be necessary if the frequency is 2.4GHz and the current access point is transmitting on a channel from 1 to 11.

Because all countries support these frequencies, you can attempt to scan these channels regardless of World mode (802.11d) support. For the countries that support 2.4GHz, see the *Cisco DX Series Wireless LAN Deployment Guide*.

Enable World mode (802.11d) for the corresponding country where the access point is located. World mode is enabled automatically for the Cisco Unified Wireless LAN Controller.

Wireless Modulation Technologies

Wireless communications use 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 the data packets for the device; all other data packets 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. When used with 802.11g and 802.11a, OFDM can support data rates as high as 54 Mbps.

The following table provides a comparison of data rates, number of channels, and modulation technologies by standard.

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

Item	802.11b	802.11g	802.11a	802.11n
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	• 20 MHz Channels: 7 - 72 Mbps • 40 MHz Channels: 15 - 150 Mbps
Nonoverlapping channels	3	3	Up to 24	Up to 24

Item	802.11b	802.11g	802.11a	802.11n
Wireless modulation	DSSS	OFDM	OFDM	OFDM

Radio Frequency Ranges

WLAN communications use the following radio frequency (RF) ranges:

- 2.4 GHz: Many devices that use 2.4 GHz can potentially interfere with the 802.11b/g connection. Interference can produce a Denial of Service (DoS) scenario, which may prevent successful 802.11 transmissions.
- 5 GHz: This range divides into several sections called Unlicensed National Information Infrastructure (UNII) bands, each of which has four channels. The channels are spaced at 20 MHz to provide nonoverlapping channels and more channels than 2.4 GHz provides.

Security for Communications in WLANs

Because all WLAN devices that are within range can receive all other WLAN traffic, security of voice communications is critical in WLANs. To ensure that intruders do not manipulate or intercept voice traffic, the Cisco SAFE Security Architecture supports Cisco DX Series devices and Cisco Aironet APs. For more information about security in networks, see http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html.

Authentication Methods

The Cisco Wireless IP Telephony solution provides wireless network security that prevents unauthorized sign-ins and compromised communications through use of the following authentication methods that Cisco DX Series devices support:

WLAN Authentication

- WPA (802.1x authentication + TKIP or AES encryption)
- WPA2 (802.1x authentication + AES or TKIP encryption)
- WPA-PSK (Pre-Shared key + TKIP encryption)
- WPA2-PSK (Pre-Shared key + AES encryption)
- EAP-FAST (Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling)
- EAP-TLS (Extensible Authentication Protocol – Transport Layer Security)
- PEAP (Protected Extensible Authentication Protocol) MS-CHAPv2 and GTC
- CCKM (Cisco Centralized Key Management)
- Open

WLAN Encryption

- AES (Advanced Encryption Scheme)
- TKIP / MIC (Temporal Key Integrity Protocol / Message Integrity Check)
- WEP (Wired Equivalent Protocol) 40/64 and 104/128 bit

Note Dynamic WEP with 802.1x authentication and Shared Key authentication are not supported.

For more information about authentication methods, see the "Wireless Security" section in the *Cisco DX Series Wireless LAN Deployment Guide*.

Authenticated Key Management

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

- WPA/WPA2: Uses RADIUS server information to generate unique keys for authentication. Because these keys are generated at the centralized RADIUS server, WPA/WPA2 provides more security than WPA pre-shared keys that are stored on the AP and device.
- Cisco Centralized Key Management (CCKM): Uses RADIUS server and a wireless domain server (WDS) information 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/WPA2 and CCKM, encryption keys are not entered on the device, but are automatically derived between the AP and device. But the EAP username and password that are used for authentication must be entered on each device.

Encryption Methods

To ensure that voice traffic is secure, Cisco DX Series devices support WEP, TKIP, and Advanced Encryption Standards (AES) for encryption. When these mechanisms are used for encryption, voice Real-Time Transport Protocol (RTP) packets are encrypted between the AP and the device.

WEP

When WEP is used in the wireless network, authentication happens at the AP through open or shared-key authentication. The WEP key that is set up on the device must match the WEP key that is configured at the AP for successful connections. The devices support WEP keys that use 40-bit encryption or a 128-bit encryption and remain static on the device and AP.

TKIP

WPA and CCKM use TKIP encryption, which 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 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.

For more information about encryption methods, see the “Wireless Security” section in the *Cisco DX Series Wireless LAN Deployment Guide*.

AP Authentication and Encryption Options

Authentication and encryption schemes are set up within the wireless LAN. VLANs are configured in the network and on the APs and specify different combinations of authentication and encryption. An SSID associates with a VLAN and the 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 device.

Note

- When you use WPA pre-shared key or WPA2 pre-shared key, the pre-shared key must be statically set on the device. These keys must match the keys that are on the AP.
- Cisco DX Series devices do not support auto EAP negotiation; to use EAP-FAST mode, you must specify it.

The following table provides a list of authentication and encryption schemes that are configured on the Cisco Aironet APs that the devices support. The table shows the network configuration option for the device that corresponds to the AP configuration.

Table 4: Authentication and Encryption Schemes

Cisco WLAN Configuration			**Cisco DX Series Configuration**
Authentication	Key management	Common encryption	Authentication
Open	None	None	None
Static WEP	None	WEP	WEP
EAP-FAST	WPA or WPA2 with optional CCKM	TKIP or AES	802.1x EAP > EAP-FAST
PEAP-MSCHAPv2	WPA or WPA2 with optional CCKM	TKIP or AES	802.1x EAP > PEAP > MSCHAPV2
PEAP-GTC	WPA or WPA2 with optional CCKM	TKIP or AES	802.1x EAP > PEAP > GTC
EAP-TLS	WPA or WPA2 with optional CCKM	TKIP or AES	802.1x EAP > TLS

Cisco WLAN Configuration			Cisco DX Series Configuration
WPA/WPA2-PSK	WPA-PSK or WPA2-PSK	TKIP or AES	WPA/WPA2 PSK

For additional information about Cisco WLAN Security, see http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-access-point/prod_brochure09186a00801f7d0b.html.

For more information about configuring authentication and encryption schemes on APs, see the *Cisco Aironet Configuration Guide* for your model and release under the following URL:

http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243

WLANs and Roaming

Cisco DX Series devices support Cisco Centralized Key Management (CCKM), a centralized key management protocol that provides a cache of session credentials on the wireless domain server (WDS).

For details about CCKM, see the *Cisco Fast Secure Roaming Application Note* at:

http://www.cisco.com/en/US/products/hw/wireless/ps4570/prod_technical_reference09186a00801c5223.html