



CHAPTER 1

An Overview of the Cisco Unified IP Phone

The Cisco Unified IP Phone 8961, 9951, and 9971 provide voice communication over an Internet Protocol (IP) network. The Cisco Unified IP Phone functions much like a digital business phone, allowing you to place and receive phone calls and to access features such as mute, hold, transfer, speed dial, call forward, and more. In addition, because the phone is connected to your data network, it offers enhanced IP telephony features, including access to network information and services, and customizable features and services.

The Cisco Unified IP Phone 8961, 9951, and 9971 have the following features:

- 24-bit color phone screen (Cisco Unified IP Phone 9971 has touchscreen support)
- Programmable feature buttons that support up to 5 lines (6 lines for the Cisco Unified IP Phone 9971) or can be programmed for other features
- Full video capabilities (Cisco Unified IP Phone 9951 and 9971 only)
- Gigabit ethernet connectivity
- Support for an external microphone and speakers
- Bluetooth support for wireless headsets (Cisco Unified IP Phone 9951 and 9971 only)
- Network connectivity by Wi-Fi (Cisco Unified IP Phone 9971 only)
- 2 USB ports for Cisco Unified IP Phones 9951 and 9971 and one USB port for Cisco Unified IP Phone 8961

A Cisco Unified IP Phone, like other network devices, must be configured and managed. These phones encode G.711a-law, G.711 μ -law, G.722, G.729a, G.729ab, and iLBC, and decode G.711a-law, G.711 μ -law, G.722, G.729, G.729a, G.729b, G.729ab, and iLBC.

This chapter includes the following topics:

- [Understanding the Cisco Unified IP Phone 8961, 9951, and 9971, page 1-2](#)
- [What Networking Protocols are Used?, page 1-10](#)
- [What Features are Supported on the Cisco Unified IP Phone 8961, 9951, and 9971?, page 1-13](#)
- [Understanding Security Features for Cisco Unified IP Phones, page 1-15](#)
- [Overview of Configuring and Installing Cisco Unified IP Phones, page 1-23](#)
- [Terminology Information, page 1-30](#)



Caution

Using a cell, mobile, or GSM phone, or two-way radio in close proximity to a Cisco Unified IP Phone might cause interference. For more information, refer to the manufacturer's documentation of the interfering device.

Understanding the Cisco Unified IP Phone 8961, 9951, and 9971

Figure 1-1 shows the main components of the Cisco Unified IP Phone 8961.

Figure 1-1 Cisco Unified IP Phone 8961

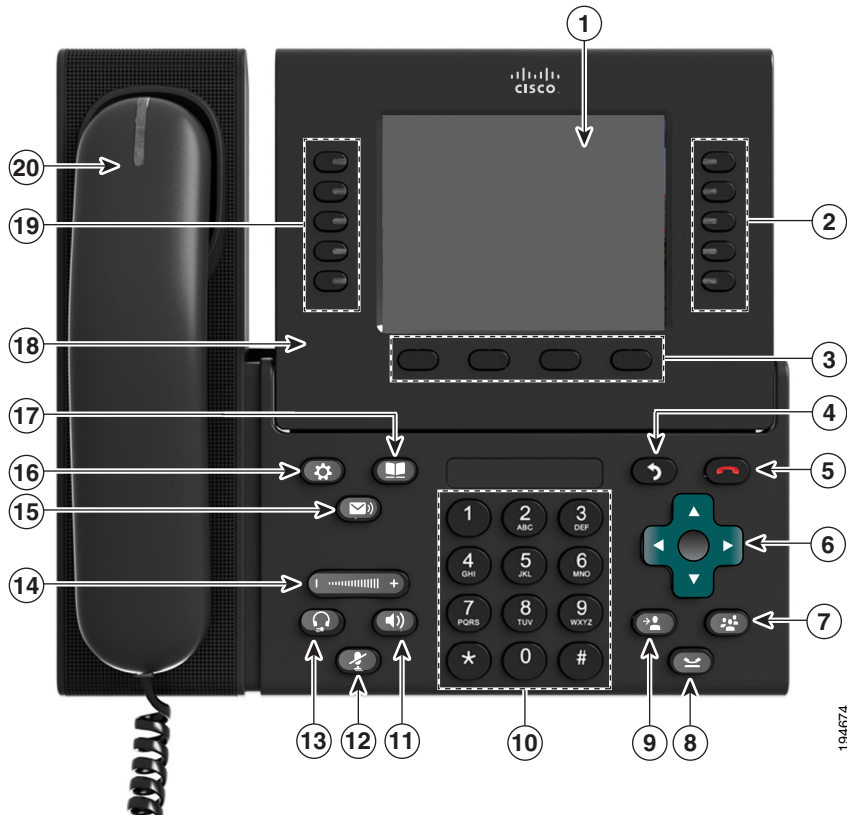


Table 1-1 describes the buttons on the Cisco Unified IP Phone 8961.

Table 1-1 Features on the Cisco Unified IP Phone 8961


1	Phone screen	Shows information about your phone, including directory number, call information (for example caller ID, icons for an active call or call on hold) and available softkeys.
2	Session buttons 	Each represents a call session and takes the default action for that session. For example, pressing the session button for a ringing call answers the call, while pressing the session button for a held call resumes the call. Color LEDs reflect the call state. LEDs can <i>flash</i> (blink on and off rapidly), <i>pulse</i> (alternately dim and brighten), or appear <i>solid</i> (glow without interruption). <ul style="list-style-type: none"> • Flashing amber—Ringing call • Solid green—Connected call or an outgoing call that is not yet connected • Pulsing green—Held call • Solid red—Shared line in-use remotely • Pulsing red—Shared line call put on hold remotely (when Privacy is off) (The position of session buttons may be reversed with that of programmable feature buttons on phones using a locale with a right-to-left reading orientation, such as Hebrew and Arabic.)

Table 1-1 Features on the Cisco Unified IP Phone 8961 (continued)














3	Softkey buttons 	Allow you to access the softkey options displayed on your phone screen.
4	Back button 	Returns to the previous screen or menu.
5	Release button 	Ends a connected call or session.
6	Navigation pad and Select button 	The four-way Navigation pad allows you to scroll through menus, highlight items, and move within a text input field. The Select button (center of the Navigation pad) allows you to select a highlighted item, disable the phone screen for cleaning, or enable the phone screen if it is in power-save mode. The Select button is lit (white) when the phone is in power-save mode.
7	Conference button 	Creates a conference call.
8	Hold button 	Places a connected call on hold.
9	Transfer button 	Transfers a call.
10	Keypad	Allows you to dial phone numbers, enter letters, and choose menu items (by entering the item number).
11	Speakerphone button 	Selects the speakerphone as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. The speakerphone audio path does not change until a new default audio path is selected (for example, by picking up the handset). If external speakers are connected, the Speakerphone button selects them as the default audio path.
12	Mute button 	Toggles the microphone on or off during a call. When the microphone is muted, the button is lit red.
13	Headset button 	Selects the wired headset as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. A headset icon in the phone screen header line indicates the headset is the default audio path. This audio path does not change until a new default audio path is selected (for example, by picking up the handset).
14	Volume button 	Controls the handset, headset, and speakerphone volume (off-hook) and the ringer volume (on-hook). Silences the ringer on the phone if an incoming call is ringing.
15	Messages button 	Auto-dials your voicemail system (varies by system).
16	Applications button 	Opens the Applications menu. Depending on how your system administrator sets up the phone, use it to access applications such as call history, preferences, and phone information.

Table 1-1 Features on the Cisco Unified IP Phone 8961 (continued)



17	Contacts button 	Opens the Contacts menu. Depending on how your system administrator sets up the phone, use it to access personal directory, corporate directory, or call history.
18	Phone display	Phone display that can be positioned to your preferred viewing angle.
19	Programmable feature buttons 	Programmable feature buttons that correspond to phone lines, speed dials, and calling features. Pressing a button for a phone line displays the active calls for that line. If you have multiple lines, you might have an All Calls feature button that displays a consolidated list of calls from all lines. Color LEDs indicate the line state: <ul style="list-style-type: none"> • Amber—Ringing call on this line • Green—Active or held call on this line • Red—Shared line in-use remotely (The position of programmable feature buttons may be reversed with that of session buttons on phones using a locale with a right-to-left reading orientation, such as Hebrew and Arabic.)
20	Handset with light strip	The handset light strip lights up to indicate a ringing call (flashing red) or a new voice message (steady red).

Figure 1-2 shows the main components of the Cisco Unified IP Phone 9951.

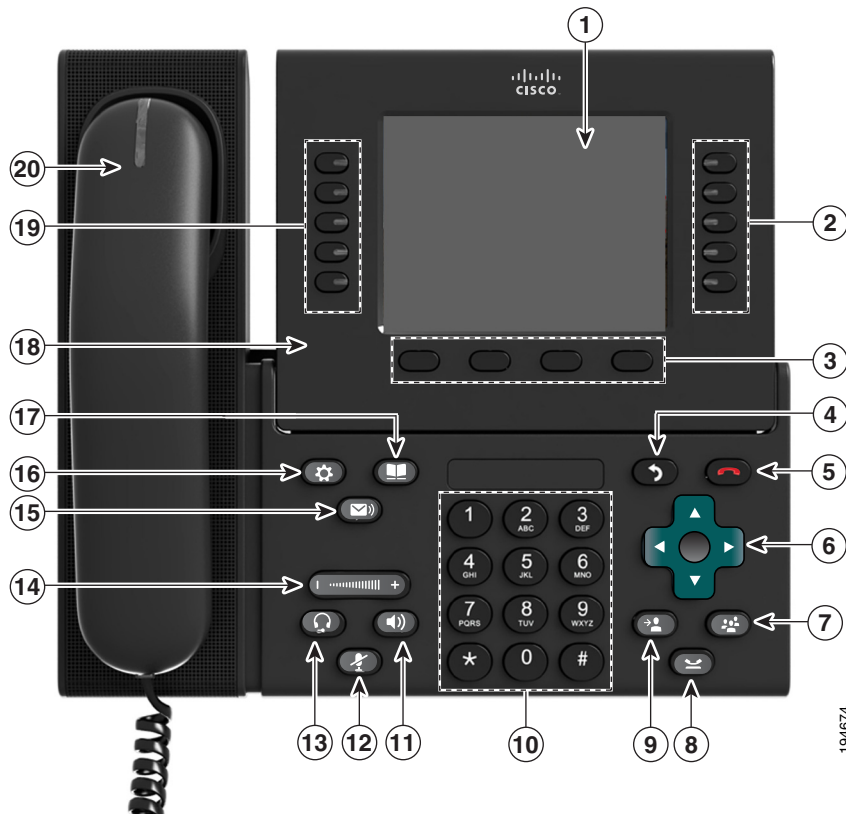
Figure 1-2 Cisco Unified IP Phone 9951

Table 1-2 describes the buttons on the Cisco Unified IP Phone 9951.

Table 1-2 Features on the Cisco Unified IP Phone 9951









1	Phone screen	Shows information about your phone, including directory number, call information (for example caller ID, icons for an active call or call on hold) and available softkeys.
2	Session buttons 	<p>Each represents a call session and takes the default action for that session. For example, pressing the session button for a ringing call answers the call, while pressing the session button for a held call resumes the call.</p> <p>Color LEDs reflect the call state. LEDs can <i>flash</i> (blink on and off rapidly), <i>pulse</i> (alternately dim and brighten), or appear <i>solid</i> (glow without interruption).</p> <ul style="list-style-type: none"> Flashing amber—Ringing call Solid green—Connected call or an outgoing call that is not yet connected Pulsing green—Held call Solid red—Shared line in-use remotely Pulsing red—Shared line call put on hold remotely <p>(The position of session buttons may be reversed with that of programmable feature buttons on phones using a locale with a right-to-left reading orientation, such as Hebrew and Arabic.)</p>
3	Softkey buttons 	Allow you to access the softkey options displayed on your phone screen.
4	Back button 	Returns to the previous screen or menu.
5	Release button 	Ends a connected call or session.
6	Navigation pad and Select button 	<p>The four-way Navigation pad allows you to scroll through menus, highlight items, and move within a text input field.</p> <p>The Select button (center of the Navigation pad) allows you to select a highlighted item, disable the phone screen for cleaning, or enable the phone screen if it is in power-save mode. The Select button is lit (white) when the phone is in power-save mode.</p>
7	Conference button 	Creates a conference call.
8	Hold button 	Places a connected call on hold.
9	Transfer button 	Transfers a call.
10	Keypad	Allows you to dial phone numbers, enter letters, and choose menu items (by entering the item number).

Table 1-2 Features on the Cisco Unified IP Phone 9951 (continued)









11	Speakerphone button 	Selects the speakerphone as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. The speakerphone audio path does not change until a new default audio path is selected (for example, by picking up the handset). If external speakers are connected, the Speakerphone button selects them as the default audio path.
12	Mute button 	Toggles the microphone on or off during a call. When the microphone is muted, the button is lit red.
13	Headset button 	Selects the wired headset as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. A headset icon in the phone screen header line indicates the headset is the default audio path. This audio path does not change until a new default audio path is selected (for example, by picking up the handset).
14	Volume button 	Controls the handset, headset, and speakerphone volume (off-hook) and the ringer volume (on-hook). Silences the ringer on the phone if an incoming call is ringing.
15	Messages button 	Auto-dials your voicemail system (varies by system).
16	Applications button 	Opens the Applications menu. Depending on how your system administrator sets up the phone, use it to access applications such as call history, preferences, and phone information.
17	Contacts button 	Opens the Contacts menu. Depending on how your system administrator sets up the phone, use it to access personal directory, corporate directory, or call history.
18	Phone display	Phone display that can be positioned to your preferred viewing angle.
19	Programmable feature buttons 	Programmable feature buttons that correspond to phone lines, speed dials, and calling features. Pressing a button for a phone line displays the active calls for that line. If you have multiple lines, you might have an All Calls feature button that displays a consolidated list of calls from all lines. Color LEDs indicate the line state: <ul style="list-style-type: none"> • Amber—Ringing call on this line • Green—Active or held call on this line • Red—Shared line in-use remotely (The position of programmable feature buttons may be reversed with that of session buttons on phones using a locale with a right-to-left reading orientation, such as Hebrew and Arabic.)
20	Handset with light strip	The handset light strip lights up to indicate a ringing call (flashing red) or a new voice message (steady red).

Figure 1-3 shows the main components of the Cisco Unified IP Phone 9971.

Figure 1-3 Cisco Unified IP Phone 9971

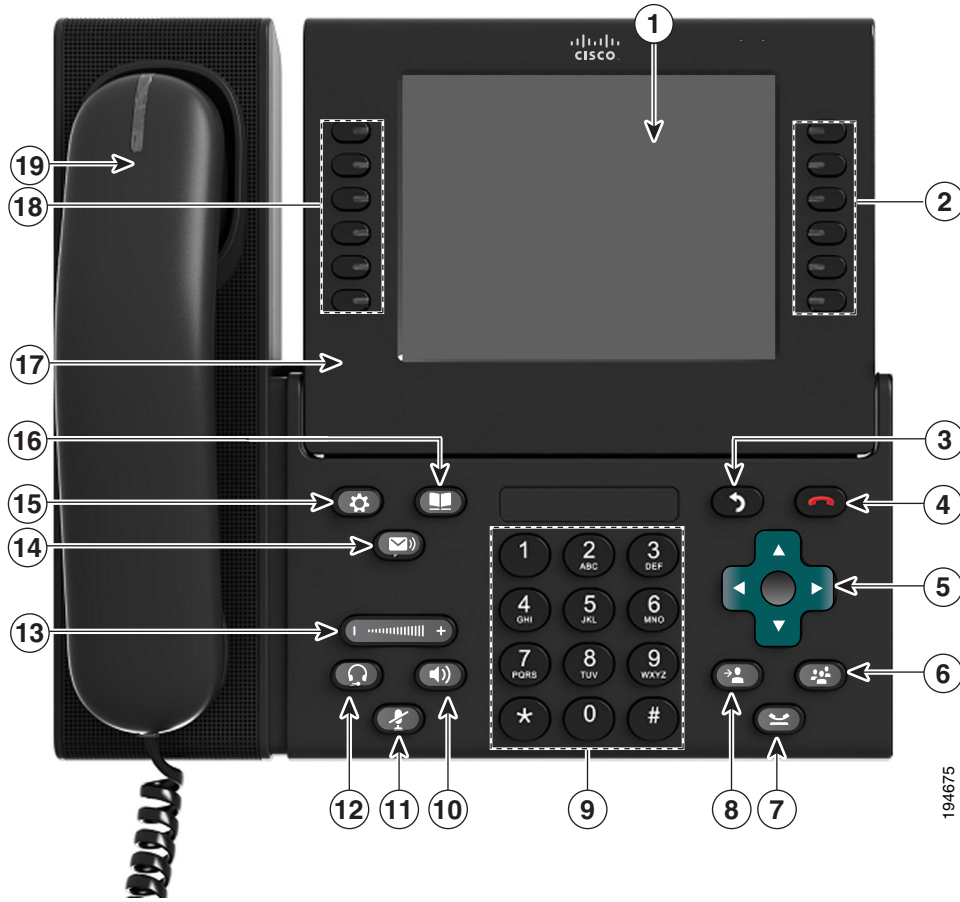


Table 1-3 describes the buttons on the Cisco Unified IP Phone 9971.

Table 1-3 Features on the Cisco Unified IP Phone 9971
















1	Phone screen	Shows information about your phone, including directory number, call information (for example caller ID, icons for an active call or call on hold) and available softkeys. Phone screen items, such as menu options and softkeys, are touch-sensitive.
2	Session buttons 	Each represents a call session and takes the default action for that session. For example, pressing the session button for a ringing call answers the call, while pressing the session button for a held call resumes the call. Color LEDs reflect the call state. LEDs can <i>flash</i> (blink on and off rapidly), <i>pulse</i> (alternately dim and brighten), or appear <i>solid</i> (glow without interruption). <ul style="list-style-type: none"> • Flashing amber—Ringing call • Solid green—Connected call or an outgoing call that is not yet connected • Pulsing green—Held call • Solid red—Shared line in-use remotely • Pulsing red—Shared line call put on hold remotely (The position of session buttons may be reversed with that of programmable feature buttons on phones using a locale with a right-to-left reading orientation, such as Hebrew and Arabic.)
3	Back button 	Returns to the previous screen or menu.
4	Release button 	Ends a connected call or session.
5	Navigation pad and Select button 	The four-way Navigation pad allows you to scroll through menus, highlight items, and move within a text input field. The Select button (center of the Navigation pad) allows you to select a highlighted item, disable the phone screen for cleaning, or enable the phone screen if it is in power-save mode. The Select button is lit (white) when the phone is in power-save mode.
6	Conference button 	Creates a conference call.
7	Hold button 	Places a connected call on hold.
8	Transfer button 	Transfers a call.
9	Keypad	Allows you to dial phone numbers, enter letters, and choose menu items (by entering the item number).
10	Speakerphone button 	Selects the speakerphone as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. The speakerphone audio path does not change until a new default audio path is selected (for example, by picking up the handset). If external speakers are connected, the Speakerphone button selects them as the default audio path.

Table 1-3 Features on the Cisco Unified IP Phone 9971 (continued)

11	Mute button 	Toggles the microphone on or off during a call. When the microphone is muted, the button is lit red.
12	Headset button 	Selects the wired headset as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. A headset icon in the phone screen header line indicates the headset is the default audio path. This audio path does not change until a new default audio path is selected (for example, by picking up the handset).
13	Volume button 	Controls the handset, headset, and speakerphone volume (off-hook) and the ringer volume (on-hook). Silences the ringer on the phone if an incoming call is ringing.
14	Messages button 	Auto-dials your voicemail system (varies by system).
15	Applications button 	Opens the Applications menu. Depending on how your system administrator sets up the phone, use it to access applications such as call history, preferences, and phone information.
16	Contacts button 	Opens the Contacts menu. Depending on how your system administrator sets up the phone, use it to access personal directory, corporate directory, or call history.
17	Phone display	Phone display that can be positioned to your preferred viewing angle.
18	Programmable feature buttons 	Programmable feature buttons that correspond to phone lines, speed dials, and calling features. Pressing a button for a phone line displays the active calls for that line. If you have multiple lines, you might have an All Calls feature button that displays a consolidated list of calls from all lines. Color LEDs indicate the line state: <ul style="list-style-type: none"> • Amber—Ringing call on this line • Green—Active or held call on this line • Red—Shared line in-use remotely (The position of programmable feature buttons may be reversed with that of session buttons on phones using a locale with a right-to-left reading orientation, such as Hebrew and Arabic.)
19	Handset with light strip	The handset light strip lights up to indicate a ringing call (flashing red) or a new voice message (steady red).

What Networking Protocols are Used?

Cisco Unified IP Phones support several industry-standard and Cisco networking protocols required for voice communication. [Table 1-4](#) provides an overview of the networking protocols that the Cisco Unified IP Phone 8961, 9951, and 9971 support.

Table 1-4 Supported Networking Protocols on the Cisco Unified IP Phone

Networking Protocol	Purpose	Usage Notes
Bluetooth	Bluetooth is a wireless personal area network (WPAN) protocol that specifies how devices communicate over short distances.	Cisco Unified IP Phone 9951 and 9971 support Bluetooth 2.1
Bootstrap Protocol (BootP)	BootP enables a network device such as the Cisco Unified IP Phone to discover certain startup information, such as its IP address.	—
Cisco Audio Session Tunnel (CAST)	The CAST protocol allows the Cisco Unified IP Phones and associated applications to discover and communicate with the remote IP phones without requiring changes to the traditional signaling components such as Cisco Unified CM and gateways.	The Cisco Unified IP Phone uses CAST as an interface between CUIVA and Unified CM using the Cisco IP Phone as a SIP proxy.
Cisco Discovery Protocol (CDP)	CDP is a 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 Unified 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 Peer-to-Peer Distribution Protocol (CPPDP)	CPPDP is a Cisco proprietary protocol used to form a peer to peer hierarchy of devices. This hierarchy is used to distribute firmware files from peer devices to their neighboring devices.	CPPDP is used by the Peer Firmware Sharing feature.
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect an IP phone into the network and have the phone become operational without your needing to manually assign an IP address or to configure additional network parameters.	DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each phone locally. Cisco recommends that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, go to the Dynamic Host Configuration Protocol chapter and the Cisco TFTP chapter in the <i>Cisco Unified Communications Manager System Guide</i> . Note If you cannot use option 150, you may try using DHCP option 66.

Table 1-4 Supported Networking Protocols on the Cisco Unified IP Phone (continued)

Networking Protocol	Purpose	Usage Notes
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Cisco Unified IP Phones use HTTP for the XML services and for troubleshooting purposes
Hypertext Transfer Protocol Secure (HTTPS)	Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of servers.	Web applications with both HTTP and HTTPS support have two URLs configured. Cisco Unified IP Phones that support HTTPS choose the HTTPS URL.
IEEE 802.1X	The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.	The Cisco Unified IP Phone implements the IEEE 802.1X standard by providing support for the following authentication methods: EAP-FAST, EAP-TLS, and EAP-MD5. When 802.1X authentication is enabled on the phone, you should disable the PC port and voice VLAN. Refer to the “Supporting 802.1X Authentication on Cisco Unified IP Phones” section on page 1-22 for additional information.
IEEE 802.11a/b/g	The IEEE 802.11 standard specifies how devices communication over a wireless local area network (WLAN). 802.11a operates at the 5 GHz band and 802.11b and 802.11g operate at the 2.4 GHz band	(Cisco Unified IP Phone 9971 only) The 802.11 interface is a deployment option for cases when Ethernet cabling is unavailable or undesirable.
Internet Protocol (IP)	IP is a 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, subnets, and gateways identifications are automatically assigned if you are using the Cisco Unified IP Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally.
Link Layer Discovery Protocol (LLDP)	LLDP is a standardized network discovery protocol (similar to CDP) that is supported on some Cisco and third-party devices.	The Cisco Unified IP Phone supports LLDP on the PC port.

Table 1-4 Supported Networking Protocols on the Cisco Unified IP Phone (continued)

Networking Protocol	Purpose	Usage Notes
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard developed for voice products.	<p>The Cisco Unified IP Phone supports LLDP-MED on the SW port to communicate information such as:</p> <ul style="list-style-type: none"> • Voice VLAN configuration • Device discovery • Power management • Inventory management <p>For more information about LLDP-MED support, see the <i>LLDP-MED and Cisco Discovery Protocol</i> white paper:</p> <p>http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml</p>
Real-Time Transport Protocol (RTP)	RTP is a standard protocol 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.
Real-Time Control Protocol (RTCP)	RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round trip delay) on RTP streams.	RTCP is disabled by default, but you can enable it on a per phone basis by using Cisco Unified Communications Manager.
Session Description Protocol (SDP)	SDP is the portion of the SIP protocol that determines which parameters are available during a connection between two endpoints. Conferences are established by using only the SDP capabilities that are supported by all endpoints in the conference.	SDP capabilities, such as codec types, DTMF detection, and comfort noise, are normally configured on a global basis by Cisco Unified Communications Manager or Media Gateway in operation. Some SIP endpoints may allow these parameters to be configured on the endpoint itself.
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.	Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Cisco Unified IP Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.
Transport Layer Security	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.

Table 1-4 Supported Networking Protocols on the Cisco Unified IP Phone (continued)

Networking Protocol	Purpose	Usage Notes
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the Cisco Unified IP Phone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server. If you want a phone to use a TFTP server other than the one specified by the DHCP server, you must manually assign the IP address of the TFTP server by using the Network Configuration menu on the phone. For more information, go to the Cisco TFTP chapter in the <i>Cisco Unified Communications Manager System Guide</i> .
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	Cisco Unified IP Phones transmit and receive RTP streams, which utilize UDP.

Related Topics

- [Understanding Interactions with Other Cisco Unified IP Telephony Products, page 2-1](#)
- [Understanding the Phone Startup Process, page 2-7](#)
- [Ethernet Setup Menu, page 7-4](#)

What Features are Supported on the Cisco Unified IP Phone 8961, 9951, and 9971?

Cisco Unified IP Phones function much like a digital business phone, allowing you to place and receive phone calls. In addition to traditional telephony features, the Cisco Unified IP Phone includes features that enable you to administer and monitor the phone as a network device.

This section includes the following topics:

- [Feature Overview, page 1-13](#)
- [Configuring Telephony Features, page 1-14](#)
- [Configuring Network Parameters Using the Cisco Unified IP Phone, page 1-14](#)
- [Providing Users with Feature Information, page 1-15](#)

Feature Overview

Cisco Unified IP Phones provide traditional telephony functionality, such as call forwarding and transferring, redialing, speed dialing, conference calling, and voice messaging system access. Cisco Unified IP phones also provide a variety of other features. For an overview of the telephony features that the Cisco Unified IP Phone supports and for tips on configuring them, see the [“Telephony Features Available for the Cisco Unified IP Phone”](#) section on page 8-2.

As with other network devices, you must configure Cisco Unified IP Phones to prepare them to access Cisco Unified Communications Manager and the rest of the IP network. By using DHCP, you have fewer settings to configure on a phone, but if your network requires it, you can manually configure an IP

address, TFTP server, subnet information, and so on. For instructions on configuring the network settings on the Cisco Unified IP Phones, see [Chapter 7, “Configuring Settings on the Cisco Unified IP Phone.”](#)

Cisco Unified IP Phones can interact with other services and devices on your IP network to provide enhanced functionality. For example, you can integrate Cisco Unified Communications Manager with the corporate Lightweight Directory Access Protocol 3 (LDAP3) standard directory to enable users to search for co-worker contact information directly from their IP phones. You can also use XML to enable users to access information such as weather, stocks, quote of the day, and other web-based information. For information about configuring such services, see the [“Configuring Corporate and Personal Directories”](#) section on page 8-27 and the [“Setting Up Services”](#) section on page 8-32.

Finally, because the Cisco Unified IP Phone is a network device, you can obtain detailed status information from it directly. This information can assist you with troubleshooting any problems users might encounter when using their IP phones. See [Chapter 10, “Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone,”](#) for more information.

Related Topics

- [Configuring Settings on the Cisco Unified IP Phone, page 7-1](#)
- [Configuring Features, Templates, Services, and Users, page 8-1](#)
- [Troubleshooting and Maintenance, page 12-1](#)

Configuring Telephony Features

You can modify additional settings for the Cisco Unified IP Phone from Cisco Unified Communications Manager Administration. Use this web-based application to set up phone registration criteria and calling search spaces, to configure corporate directories and services, and to modify phone button templates, among other tasks. See the [“Telephony Features Available for the Cisco Unified IP Phone”](#) section on page 8-2 and the Cisco Unified Communications Manager documentation for additional information.

For more information about Cisco Unified Communications Manager Administration, refer to Cisco Unified Communications Manager documentation, including *Cisco Unified Communications Manager Administration Guide*. You can also use the context-sensitive help available within the application for guidance.

You can access Cisco Unified Communications Manager documentation at this location:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

You can access Cisco Unified Communications Manager Business Edition documentation at this location:

http://www.cisco.com/en/US/products/ps7273/tsd_products_support_series_home.html

Related Topic

- [Telephony Features Available for the Cisco Unified IP Phone, page 8-2](#)

Configuring Network Parameters Using the Cisco Unified IP Phone

You can configure parameters such as DHCP, TFTP, and IP settings on the phone itself. You can also obtain statistics about a current call or firmware versions on the phone.

For more information about configuring features and viewing statistics from the phone, see [Chapter 7, “Configuring Settings on the Cisco Unified IP Phone”](#) and see [Chapter 10, “Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone.”](#)

Providing Users with Feature Information

If you are a system administrator, you are likely the primary source of information for Cisco Unified IP Phone users in your network or company. To ensure that you distribute the most current feature and procedural information, familiarize yourself with Cisco Unified IP Phone documentation. Make sure to visit the Cisco Unified IP Phone web site:

http://www.cisco.com/en/US/products/ps10453/products_user_guide_list.html

From this site, you can view various user guides.

In addition to providing documentation, it is important to inform users of available Cisco Unified IP Phone features, including those specific to your company or network, and of how to access and customize those features, if appropriate.

For a summary of some of the key information that phone users need their system administrators to provide, see [Appendix A, “Providing Information to Users Via a Website.”](#)

Understanding Security Features for Cisco Unified IP Phones

Implementing security in the Cisco Unified Communications Manager system prevents identity theft of the phone and Cisco Unified Communications Manager server, prevents data tampering, and prevents call signaling and media stream tampering.

To alleviate these threats, the Cisco IP telephony network establishes and maintains secure (encrypted) communication streams between a phone and the server, digitally signs files before they are transferred to a phone, and encrypts media streams and call signaling between Cisco Unified IP phones.

The Cisco Unified IP Phone 8961, 9951, and 9971 use the Phone security profile, which defines whether the device is nonsecure or secure. For information on applying the security profile to the phone, refer to the *Cisco Unified Communications Manager Security Guide*.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file will contain sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For detailed information, refer to the “Configuring Encrypted Phone Configuration Files” chapter in *Cisco Unified Communications Manager Security Guide*.

[Table 1-5](#) shows where you can find information about security in this and other documents.

Table 1-5 Cisco Unified IP Phone and Cisco Unified Communications Manager Security Topics

Topic	Reference
Detailed explanation of security, including set up, configuration, and troubleshooting information for Cisco Unified Communications Manager and Cisco Unified IP Phones	Refer to the <i>Cisco Unified Communications Manager Security Guide</i> .
Security features supported on the Cisco Unified IP Phone	See the “ Overview of Supported Security Features ” section on page 1-16
Restrictions regarding security features	See the “ Security Restrictions ” section on page 1-23

Table 1-5 Cisco Unified IP Phone and Cisco Unified Communications Manager Security Topics (continued)

Topic	Reference
Viewing a security profile name	Table 1-6 provides an overview of the security features that the Cisco Unified IP Phone 8961, 9951, and 9971 support. For more information about these features and about Cisco Unified Communications Manager and Cisco Unified IP Phone security, refer to the <i>Cisco Unified Communications Manager Security Guide</i> .
Identifying phone calls for which security is implemented	See the “Identifying Secure (Encrypted) Phone Calls” section on page 1-19
Extension Mobility HTTPS Support	See the “What Networking Protocols are Used?” section on page 1-10
TLS connection	<ul style="list-style-type: none"> • See the “What Networking Protocols are Used?” section on page 1-10 • See the “Adding Phones to the Cisco Unified Communications Manager Database” section on page 2-9
Security and the phone startup process	See the “Understanding the Phone Startup Process” section on page 2-7
Security and phone configuration files	See the “Adding Phones to the Cisco Unified Communications Manager Database” section on page 2-9
Changing the TFTP Server 1 or TFTP Server 2 option on the phone when security is implemented.	See the “IPv4 Setup Menu Options” section on page 7-10
Items on the Security Setup menu that you access from the phone	See the “Security Setup Menu” section on page 7-13
Disabling access to a phone’s web pages	See the “Enabling and Disabling Web Page Access” section on page 11-3
Troubleshooting	<ul style="list-style-type: none"> • See the “Troubleshooting Cisco Unified IP Phone Security” section on page 12-9 • Refer to the <i>Troubleshooting Guide for Cisco Unified Communications Manager</i>
Deleting the CTL file from the phone	See the “Resetting the Cisco Unified IP Phone” section on page 12-15
Resetting or restoring the phone	See the “Resetting the Cisco Unified IP Phone” section on page 12-15
802.1X Authentication for Cisco Unified IP Phones	See these sections: <ul style="list-style-type: none"> • “Supporting 802.1X Authentication on Cisco Unified IP Phones” section on page 1-22 • “Security Setup Menu” section on page 7-13 • “Status Menu” section on page 10-2 • “Troubleshooting Cisco Unified IP Phone Security” section on page 12-9

Overview of Supported Security Features

[Table 1-6](#) provides an overview of the security features that the Cisco Unified IP Phone 8961, 9951, and 9971 support. For more information about these features and about Cisco Unified Communications Manager and Cisco Unified IP Phone security, refer to *Cisco Unified Communications Manager Security Guide*.


For information about current security settings on a phone, press  and choose **Administrator Settings > Security Setup**. For more information, see the “[Security Setup Menu](#)” section on page 7-13.

Table 1-6 Overview of Security Features

Feature	Description
Image authentication	Signed binary files (with the extension .sbn) prevent tampering with the firmware image before it is loaded on a phone. Tampering with the image causes a phone to fail the authentication process and reject the new image.
Image Encryption	Encrypted binary files (with the extension .sebn) prevent tampering with the firmware image before it is loaded on a phone. Tampering with the image causes a phone to fail the authentication process and reject the new image.
Customer-site certificate installation	Each Cisco Unified IP Phone requires a unique certificate for device authentication. Phones include a manufacturing installed certificate (MIC), but for additional security, you can specify in Cisco Unified Communications Manager Administration that a certificate be installed by using the Certificate Authority Proxy Function (CAPF). Alternatively, you can install a Locally Significant Certificate (LSC) from the Security Configuration menu on the phone. See the “ Configuring Security on the Cisco Unified IP Phone ” section on page 3-21 for more information.
Device authentication	Occurs between the Cisco Unified Communications Manager server and the phone when each entity accepts the certificate of the other entity. Determines whether a secure connection between the phone and a Cisco Unified Communications Manager should occur; and, if necessary, creates a secure signaling path between the entities by using TLS protocol. Cisco Unified Communications Manager will not register phones unless they can be authenticated by the Cisco Unified Communications Manager.
File authentication	Validates digitally signed files that the phone downloads. The phone validates the signature to make sure that file tampering did not occur after the file creation. Files that fail authentication are not written to Flash memory on the phone. The phone rejects such files without further processing.
File encryption	Encryption prevents sensitive information from being revealed while the file is in transit to the phone. In addition the phone validates the signature to make sure that file tampering did not occur after the file creation. Files that fail authentication are not written to Flash memory on the phone. The phone rejects such files without further processing.
Signaling Authentication	Uses the TLS protocol to validate that no tampering has occurred to signaling packets during transmission.
Manufacturing installed certificate	Each Cisco Unified IP Phone contains a unique manufacturing installed certificate (MIC), which is used for device authentication. The MIC is a permanent unique proof of identity for the phone, and allows Cisco Unified Communications Manager to authenticate the phone.
Media encryption	Uses SRTP to ensure that the media streams between supported devices proves secure and that only the intended device receives and reads the data. Includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport.

Table 1-6 Overview of Security Features (continued)

Feature	Description
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure that are too processing-intensive for the phone, and interacts with the phone for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the phone, or it can be configured to generate certificates locally.
Security profiles	Defines whether the phone is nonsecure, authenticated, encrypted, or protected. See Table 1-6 , which provides an overview of the security features that the Cisco Unified IP Phone 9971 supports. For more information about these features and about Cisco Unified Communications Manager and Cisco Unified IP Phone security, refer to the <i>Cisco Unified Communications Manager Security Guide</i> .
Encrypted configuration files	Lets you ensure the privacy of phone configuration files.
Optional disabling of the web server functionality for a phone	For security purposes, you can prevent access to a phone's web page (which displays a variety of operational statistics for the phone) and user options pages. For more information, see the “Enabling and Disabling Web Page Access” section on page 11-3.
Phone hardening	Additional security options, which you control from Cisco Unified Communications Manager Administration: <ul style="list-style-type: none"> • Disabling PC port • Disabling Gratuitous ARP (GARP) • Disabling PC Voice VLAN access • Disabling access to the Setting menus, or providing restricted access that allows access to the Preferences menu and saving volume changes only • Disabling access to web pages for a phone • Disabling Bluetooth Accessory Port
802.1X Authentication	The Cisco Unified IP Phone can use 802.1X authentication to request and gain access to the network. See the “Supporting 802.1X Authentication on Cisco Unified IP Phones” section on page 1-22 for more information.
Secure SIP Failover for SRST	After you configure an SRST reference for security and then reset the dependent devices in Cisco Unified CM Administration, the TFTP server adds the SRST certificate to the phone cnf.xml file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router.
Signaling encryption	Ensures that all SCCP and SIP signaling messages that are sent between the device and the Cisco Unified CM server are encrypted.

Related Topics

- [Identifying Secure \(Encrypted\) Phone Calls, page 1-19](#)
- [Security Restrictions, page 1-23](#)

Understanding Security Profiles

All Cisco Unified IP Phones that support Cisco Unified Communications Manager use a security profile, which defines whether the phone is nonsecure, authenticated, or encrypted. For information about configuring the security profile and applying the profile to the phone, refer to *Cisco Unified Communications Manager Security Guide*.

To view the security mode that is set for the phone, look at the Security Mode setting in the Security Configuration menu. For more information, see the “[Security Setup Menu](#)” section on page 7-13.

Related Topics

- [Identifying Secure \(Encrypted\) Phone Calls](#), page 1-19
- [Security Restrictions](#), page 1-23

Identifying Secure (Encrypted) Phone Calls

When security is implemented for a phone, you can identify secure phone calls by icons on the phone screen. You can also determine if the connected phone is secure and protected if a security tone plays at the beginning of the call.

In a secure call, all call signaling and media streams are encrypted. A secure call offers a high level of security, providing integrity and privacy to the call. When a call in progress is being encrypted, the call progress icon to the right of the call duration timer in the phone screen changes to the following icon:



Note

If the call is routed through non-IP call legs, for example, PSTN, the call may be nonsecure even though it is encrypted within the IP network and has a lock icon associated with it.

In a secure call, a security tone plays at the beginning of a call to indicate that the other connected phone is also receiving and transmitting secure audio and video (if video is involved). If your call is connected to a non-secure phone, the security tone does not play.



Note

Secure calling is supported for connections between two phones only. Some features, such as conference calling, shared lines, and Extension Mobility are not available when secure calling is configured.


Related Topic

- [Understanding Security Features for Cisco Unified IP Phones](#), page 1-15
- [Security Restrictions](#), page 1-23

Establishing and Identifying Secure Conference Calls

You can initiate a secure conference call and monitor the security level of participants. A secure conference call is established using this process:

1. A user initiates the conference from a secure phone.
2. Cisco Unified Communications Manager assigns a secure conference bridge to the call.
3. As participants are added, Cisco Unified Communications Manager verifies the security mode of each phone and maintains the secure level for the conference.

- The phone displays the security level of the conference call. A secure conference displays  icon to the right of “Conference” on the phone screen.


**Note**

There are interactions, restrictions, and limitations that affect the security level of the conference call depending on the security mode of the participant’s phones and the availability of secure conference bridges. See [Table 1-7](#) and [Table 1-8](#) for information about these interactions.

Establishing and Identifying Secure Calls

A secure call is established when your phone, and the phone on the other end, is configured for secure calling. The other phone can be in the same Cisco IP network, or on a network outside the IP network. Secured calls can only be made between two phones. Conference calls and other multiple-line calls are not supported.

A secured call is established using this process:

- A user initiates the call from a secured phone (secured security mode).
- The phone displays the  icon (secure) on the phone screen. This icon indicates that the phone is configured for secure calls, but this does not mean that the other connected phone is also secured.
- A security tone plays if the call is connected to another secured phone, indicating that both ends of the conversation are encrypted and secured. If the call is connected to a non-secured phone, then the secure tone is not played.

**Note**

Secured calling is supported for conversations between two phones. Some features, such as conference calling, shared lines, and Cisco Extension Mobility are not available when secured calling is configured.

Call Security Interactions and Restrictions

Cisco Unified Communications Manager checks the phone security status when conferences are established and changes the security indication for the conference or blocks the completion of the call to maintain integrity and also security in the system. [Table 1-7](#) provides information about changes to call security levels when using Barge.

Table 1-7 Call Security Interactions When Using Barge

Initiator’s Phone Security Level	Feature Used	Call Security Level	Results of Action
Non-secure	Barge	Encrypted call	Call barged and identified as non-secure call
Secure	Barge	Encrypted call	Call barged and identified as secure call

[Table 1-8](#) provides information about changes to conference security levels depending on the initiator’s phone security level, the security levels of participants, and the availability of secure conference bridges.

Table 1-8 *Security Restrictions with Conference Calls*

Initiator's Phone Security Level	Feature Used	Security Level of Participants	Results of Action
Non-secure	Conference	Secure	Non-secure conference bridge Non-secure conference
Secure	Conference	At least one member is non-secure.	Secure conference bridge Non-secure conference
Secure	Conference	Secure.	Secure conference bridge Secure encrypted level conference
Non-secure	MeetMe	Minimum security level is encrypted	Initiator receives message "Does not meet Security Level, call rejected."
Secure	MeetMe	Minimum security level is non-secure	Only secure conference bridge available and used Conference accepts all calls

Supporting 802.1X Authentication on Cisco Unified IP Phones

These sections provide information about 802.1X support on the Cisco Unified IP Phones:

- [Overview, page 1-22](#)
- [Required Network Components, page 1-22](#)
- [Best Practices—Requirements and Recommendations, page 1-22](#)

Overview

Cisco Unified IP phones and Cisco Catalyst switches have traditionally used Cisco Discovery Protocol (CDP) to identify each other and determine parameters such as VLAN allocation and inline power requirements. However, CDP is not used to identify any locally attached PCs; therefore, Cisco Unified IP Phones provide an EAPOL pass-through mechanism, whereby a PC locally attached to the IP phone, may pass through EAPOL messages to the 802.1X authenticator in the LAN switch. This prevents the IP phone from having to act as the authenticator, yet allows the LAN switch to authenticate a data endpoint prior to accessing the network.

In conjunction with the EAPOL pass-through mechanism, Cisco Unified IP Phones provide a proxy EAPOL-Logoff mechanism. In the event that the locally attached PC is disconnected from the IP phone, the LAN switch would not see the physical link fail, because the link between the LAN switch and the IP phone is maintained. To avoid compromising network integrity, the IP phone sends an EAPOL-Logoff message to the switch, on behalf of the downstream PC, which triggers the LAN switch to clear the authentication entry for the downstream PC.

The Cisco Unified IP phones also contain an 802.1X supplicant, in addition to the EAPOL pass-through mechanism. This supplicant allows network administrators to control the connectivity of IP phones to the LAN switch ports. The current release of the phone 802.1X supplicant uses the EAP-FAST, EAP-TLS, and EAP-MD5 options for network authentication.

Required Network Components

Support for 802.1X authentication on Cisco Unified IP Phones requires several components, including:

- Cisco Unified IP Phone—The phone acts as the 802.1X *supplicant*, which initiates the request to access the network.
- Cisco Secure Access Control Server (ACS) (or other third-party authentication server)—The authentication server and the phone must both be configured with a shared secret that is used to authenticate the phone.
- Cisco Catalyst Switch (or other third-party switch)—The switch must support 802.1X, so it can act as the *authenticator* and pass the messages between the phone and the authentication server. When the exchange is completed, the switch then grants or denies the phone access to the network.

Best Practices—Requirements and Recommendations

- Enable 802.1X Authentication—If you want to use the 802.1X standard to authenticate Cisco Unified IP Phones, be sure that you have properly configured the other components before enabling it on the phone. See the [“802.1X Authentication and Transaction Status” section on page 7-15](#) for more information.

- Configure PC Port—The 802.1X standard does not take into account the use of VLANs and thus recommends that only a single device should be authenticated to a specific switch port. However, some switches (including Cisco Catalyst switches) support multi-domain authentication. The switch configuration determines whether you can connect a PC to the phone's PC port.
 - Enabled—If you are using a switch that supports multi-domain authentication, you can enable the PC port and connect a PC to it. In this case, Cisco Unified IP Phones support proxy EAPOL-Logoff to monitor the authentication exchanges between the switch and the attached PC. For more information about IEEE 802.1X support on the Cisco Catalyst switches, refer to the Cisco Catalyst switch configuration guides at:
http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
 - Disabled—If the switch does not support multiple 802.1X-compliant devices on the same port, you should disable the PC Port when 802.1X authentication is enabled. See the “Ethernet Setup Menu” section on page 7-4 for more information. If you do not disable this port and subsequently attempt to attach a PC to it, the switch will deny network access to both the phone and the PC.
- Configure Voice VLAN—Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.
 - Enabled—If you are using a switch that supports multi-domain authentication, you can continue to use the voice VLAN.
 - Disabled—If the switch does not support multi-domain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN. See the “Ethernet Setup Menu” section on page 7-4 for more information.
- Enter MD5 Shared Secret—If you disable 802.1X authentication or perform a factory reset on the phone, the previously configured MD5 shared secret is deleted. See the “802.1X Authentication and Transaction Status” section on page 7-15 for more information.

Security Restrictions

A user cannot barge into an encrypted call if the phone that is used to barge is not configured for encryption. When barge fails in this case, a reorder tone (fast busy tone) plays on the phone on which the user initiated the barge.

If the initiator phone is configured for encryption, the barge initiator can barge into a nonsecure call from the encrypted phone. After the barge occurs, Cisco Unified Communications Manager classifies the call as nonsecure.

If the initiator phone is configured for encryption, the barge initiator can barge into an encrypted call, and the phone indicates that the call is encrypted.

Overview of Configuring and Installing Cisco Unified IP Phones

When deploying a new IP telephony system, system administrators and network administrators must complete several initial configuration tasks to prepare the network for IP telephony service. For information and a checklist for setting up and configuring a Cisco IP telephony network, go to the [System Configuration Overview](#) chapter in *Cisco Unified Communications Manager System Guide*.

After you have set up the IP telephony system and configured system-wide features in Cisco Unified Communications Manager, you can add IP phones to the system.

The following topics provide an overview of procedures for adding Cisco Unified IP Phones to your network:

- [Configuring Cisco Unified IP Phones in Cisco Unified Communications Manager, page 1-24](#)
- [Installing Cisco Unified IP Phones, page 1-28](#)

Configuring Cisco Unified IP Phones in Cisco Unified Communications Manager

To add phones to the Cisco Unified Communications Manager database, you can use:

- Auto-registration
- Cisco Unified Communications Manager Administration
- Bulk Administration Tool (BAT)
- BAT and the Tool for Auto-Registered Phones Support (TAPS)

For more information about these choices, see the [“Adding Phones to the Cisco Unified Communications Manager Database”](#) section on page 2-9.

For general information about configuring phones in Cisco Unified Communications Manager, refer to the following documentation:

- [Cisco Unified IP Phones](#), *Cisco Unified Communications Manager System Guide*
- [Cisco Unified IP Phone Configuration](#), *Cisco Unified Communications Manager Administration Guide*.
- [Autoregistration Configuration](#), *Cisco Unified Communications Manager Administration Guide*.
- *Cisco Unified Communications Manager Bulk Administration Guide*.

Checklist for Configuring the Cisco Unified IP Phone 8961, 9951, and 9971 in Cisco Unified Communications Manager

Table 1-9 provides a checklist of configuration tasks for the Cisco Unified IP Phone 8961, 9951, and 9971 in Cisco Unified Communications Manager Administration. The list presents a suggested order to guide you through the phone configuration process. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, refer to the sources in the list.

Table 1-9 Checklist for Configuring the Cisco Unified IP Phone 8961, 9951, and 9971 in Cisco Unified Communications Manager

Task	Purpose	For More Information
1.	<p>Gather the following information about the phone:</p> <ul style="list-style-type: none"> • Phone Model • MAC address • Physical location of the phone • Name or user ID of phone user • Device pool • Partition, calling search space, and location information • Number of lines and associated directory numbers (DNs) to assign to the phone • Cisco Unified Communications Manager user to associate with the phone • Phone usage information that affects phone button template, phone features, IP Phone services, or phone applications <p>Provides list of configuration requirements for setting up phones.</p> <p>Identifies preliminary configuration that you need to perform before configuring individual phones, such as phone button templates.</p>	<p>For more information, go to the “Cisco Unified IP Phones” chapter in the <i>Cisco Unified Communications Manager System Guide</i>.</p> <p>See the “Telephony Features Available for the Cisco Unified IP Phone” section on page 8-2.</p>
2.	Verify that you have sufficient unit license for your phone.	For more information, go to the “ Licensing ” section in the <i>Cisco Unified Communications Manager System Guide</i> .
3.	<p>Customize phone button templates (if required).</p> <p>Changes the number of line buttons, speed-dial buttons or service URL buttons. You can add a Privacy, All Calls, or Mobility button to meet user needs.</p>	<p>For more information, go to the Phone Button Template Configuration chapter in the <i>Cisco Unified Communications Manager Administration Guide</i>.</p> <p>See the “Modifying Phone Button Templates” section on page 8-29.</p>

Table 1-9 Checklist for Configuring the Cisco Unified IP Phone 8961, 9951, and 9971 in Cisco Unified Communications Manager (continued)

Task	Purpose	For More Information
4.	<p>Add and configure the phone by completing the required fields in the Phone Configuration window. Required fields are indicated by an asterisk (*) next to the field name; for example, MAC address and device pool.</p> <p>Adds the device with its default settings to the Cisco Unified Communications Manager database.</p>	<p>For more information, go to the Cisco Unified IP Phone Configuration chapter in the <i>Cisco Unified Communications Manager Administration Guide</i>.</p> <p>For information about Product Specific Configuration fields, refer to “?” Button Help in the Phone Configuration window.</p> <p>Note If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, go to the User/Phone Add Configuration chapter in the <i>Cisco Unified Communications Manager Administration Guide</i>.</p>
5.	<p>Add and configure directory numbers (lines) on the phone by completing the required fields in the Directory Number Configuration window. Required fields are indicated by an asterisk (*) next to the field name; for example, directory number and presence group.</p> <p>Adds primary and secondary directory numbers and features associated with directory numbers to the phone.</p>	<p>For more information, go to the “Directory Number Configuration” chapter in the <i>Cisco Unified Communications Manager Administration Guide</i>.</p> <p>See the “Telephony Features Available for the Cisco Unified IP Phone” section on page 8-2.</p>
6.	<p>Configure speed-dial buttons and assign speed-dial numbers (optional).</p> <p>Adds speed-dial buttons and numbers.</p> <p>Users can change speed-dial settings on their phones by using Cisco Unified CM User Options.</p>	<p>For more information, go to the “Configuring Speed-Dial Buttons or Abbreviated Dialing” section in the “Cisco Unified IP Phone Configuration” chapter in the <i>Cisco Unified Communications Manager Administration Guide</i>.</p>
7.	<p>Configure Cisco Unified IP Phone services and assign services (optional).</p> <p>Provides IP Phone services.</p> <p>Users can add or change services on their phones by using the Cisco Unified CM User Options.</p> <p>Note Users can subscribe to the IP phone service only if the Enterprise Subscription check box is unchecked when the IP phone service is first configured in Cisco Unified Communications Manager Administration.</p> <p>Note Some Cisco-provided default services are classified as enterprise subscriptions, so the user cannot add them through the user options pages. They are on the phone by default, and they can only be removed from the phone if you disable them in Cisco Unified Communications Manager administration.</p>	<p>For more information, go to the “IP Phone Services Configuration” chapter in the <i>Cisco Unified Communications Manager Administration Guide</i>.</p> <p>See the “Setting Up Services” section on page 8-32.</p>

Table 1-9 Checklist for Configuring the Cisco Unified IP Phone 8961, 9951, and 9971 in Cisco Unified Communications Manager (continued)

Task	Purpose	For More Information
8.	Assign services to programmable buttons (optional). Provides access to an IP phone service or URL.	For more information, go to the “ Adding a Service URL Button ” section in the Cisco Unified IP Phone Configuration chapter in the <i>Cisco Unified Communications Manager Administration Guide</i> .
9.	Add user information by configuring required fields. Required fields are indicated by an asterisk (*); for example, User ID and last name. Note Assign a password (for User Options web pages) and PIN (for Cisco Extension Mobility and Personal Directory) Adds user information to the global directory for Cisco Unified Communications Manager.	For more information, go to the End User Configuration chapter in the <i>Cisco Unified Communications Manager Administration Guide</i> . See the “ Adding Users to Cisco Unified Communications Manager ” section on page 8-33. Note If your company uses a a Lightweight Directory Access Protocol (LDAP) directory to store information on users, you can install and configure Cisco Unified Communications to use your existing LDAP directory, refer to the “ Configuring Corporate Directories ” section on page 8-27. Note If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, go to the User/Phone Add Configurations chapter in the <i>Cisco Unified Communications Manager Administration Guide</i> .
10.	Associate a user to a user group. Assigns users a common list of roles and permissions that apply to all users in a user group. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users. For example, you must add users to the standard Cisco CCM End Users group so users can access Cisco Unified CM User Options.	Refer to the following sections in the <i>Cisco Unified Communications Manager Administration Guide</i> : <ul style="list-style-type: none"> • “End User Configuration Settings” section in the “End User Configuration” chapter. • “Adding Users to a User Group” section in the “User Group Configuration” chapter.
11.	Associate a user with a phone (optional). Provides users with control over their phone such a forwarding calls or adding speed-dial numbers or services. Note Some phones, such as those in conference rooms, do not have an associated user.	For more information, go to the “ Associating Devices to an End User ” section in the End User Configuration chapter in the <i>Cisco Unified Communications Manager Administration Guide</i> .

Installing Cisco Unified IP Phones

After you have added the phones to the Cisco Unified Communications Manager database, you can complete the phone installation. You (or the phone users) can install the phone at the users's location. The Cisco Unified IP Phone Installation Guide, which is provided on the [cisco.com](http://www.cisco.com) web site, provides directions for connecting the phone handset, cables, and other accessories.



Note

Before you install a phone, even if it is new, upgrade the phone to the current firmware image. For information about upgrading, refer to the Readme file for your phone, which is located at:

<http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240>

After the phone is connected to the network, the phone startup process begins, and the phone registers with Cisco Unified Communications Manager. To finish installing the phone, configure the network settings on the phone depending on whether you enable or disable DHCP service.

If you used auto-registration, you need to update the specific configuration information for the phone such as associating the phone with a user, changing the button table, or directory number.

Checklist for Installing the Cisco Unified IP Phone 8961, 9951, and 9971

Table 1-10 provides an overview and checklist of installation tasks for the Cisco Unified IP Phone 8961, 9951, and 9971. The list presents a suggested order to guide you through the phone installation. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, refer to the sources in the list.

Table 1-10 Installation Checklist for the Cisco Unified IP Phone 8961, 9951, and 9971

Task	Purpose	For More Information
1.	Choose the power source for the phone: <ul style="list-style-type: none"> • Power over Ethernet (PoE) • External power supply Determines how the phone receives power. Note The Cisco Unified IP Phone 9971, when being used in a WLAN environment, requires an external power supply.	See the “ Providing Power to the Cisco Unified IP Phone ” section on page 2-3.
2.	Assemble the phone, adjust phone placement, and connect the network cable. (If you are using the Cisco Unified IP Phone 9971 in a WLAN environment, refer to Task 5 .) Locates and installs the phone in the network.	See the “ Installing the Cisco Unified IP Phone ” section on page 3-11. See the “ Connecting the Footstand ” section on page 3-19.
3.	Monitor the phone startup process. Adds primary and secondary directory numbers and features associated with directory numbers to the phone. Verifies that phone is configured properly.	See the “ Verifying the Phone Startup Process ” section on page 3-21.

Table 1-10 Installation Checklist for the Cisco Unified IP Phone 8961, 9951, and 9971 (continued)

Task	Purpose	For More Information
4.	<p>If you choose to deploy the Cisco Unified IP Phone 9971 on a wireless network, skip to Task 5.</p> <p>If you are configuring the ethernet network settings on the phone for an IP network, you can set up an IP address for the phone by either using DHCP or manually entering an IP address.</p> <p>Using DHCP—To enable DHCP and allow the DHCP server to automatically assign an IP address to the Cisco Unified IP Phone and direct the phone to a TFTP server, press Applications and choose Administrator Settings > Network Setup > Ethernet Setup > IPv4 Setup and:</p> <ul style="list-style-type: none"> • To enable DHCP, set DHCP Enabled to Yes. DHCP is enabled by default. • To use an alternate TFTP server, set Alternate TFTP Server to Yes, and enter the IP address for the TFTP Server. <p>Note Consult with the network administrator to determine whether you need to assign an alternative TFTP server instead of using the TFTP server assigned by DHCP.</p> <p>Without DHCP—You must configure the IP address, subnet mask, TFTP server, and default router locally on the phone. Press Applications and choose > Administrator Settings > Network Setup > Ethernet Setup > IPv4 Setup:</p> <p>To disable DHCP and manually set an IP address:</p> <ol style="list-style-type: none"> a. Set DHCP Enabled to No. b. Enter the static IP address for phone. c. Enter the subnet mask. d. Enter the default router IP addresses. e. Set Alternate TFTP Server to Yes, and enter the IP address for TFTP Server 1. <p>You must also enter the domain name where the phone resides. Press Applications and choose Administrator Settings > Network Setup > Ethernet Setup.</p>	<p>See the “Configuring Startup Network Settings” section on page 3-21.</p> <p>See the “Ethernet Setup Menu” section on page 7-4.</p>
5.	<p>(Cisco Unified IP Phone 9971 only)</p> <p>If you choose to deploy the phone on the wireless network, you must configure the following:</p> <ul style="list-style-type: none"> • Configure the wireless network. • Enable wireless LAN for phones on Cisco Unified Communications Administration. • Configure a wireless network profile on the phone. <p>Note The wireless LAN on the phone does not activate when there are ethernet cables connected on the phone.</p>	<p>See Chapter 6, “Understanding the VoIP Wireless Network.”</p>

Table 1-10 *Installation Checklist for the Cisco Unified IP Phone 8961, 9951, and 9971 (continued)*

Task	Purpose	For More Information
6.	Make calls with the Cisco Unified IP Phone. Verifies that the phone and features work correctly.	Refer to the <i>Cisco Unified IP Phone 8961, 9951, and 9971 User Guide</i> for Cisco Unified Communications Manager.
7.	Provide information to end users about how to use their phones and how to configure their phone options. Ensures that users have adequate information to successfully use their Cisco Unified IP Phones.	See Appendix A, “Providing Information to Users Via a Website.”

Terminology Information

[Table 1-11](#) highlights some of the differences in terminology found in the Cisco Unified IP Phone 8961, 9951, and 9971 User Guide and the Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide and Cisco Unified Communications Administration Guide.

Table 1-11 *Terminology Differences*

User Guide	Administration Guide
Line Status	Busy Lamp Field (BLF)
Message Indicators	Message Waiting Indicator (MWI) or Message Waiting Lamp
Programmable Feature Button	Programmable Button or Programmable Line Key (PLK)
Voicemail System	Voice Messaging System