Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 8.5 (SIP)

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
        800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-20862-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

The Java logo is a trademark or registered trademark of Sun Microsystems, Inc. in the U.S. or other countries.

Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 8.5 (SIP)
© 2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Overview

Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 8.5 (SIP) provides the information you need to understand, install, configure, manage, and troubleshoot the phones on a Voice-over-IP (VoIP) network.

Because of the complexity of an IP telephony network, this guide does not provide complete and detailed information for procedures that you need to perform in Cisco Unified Communications Manager or other network devices. See the "Related Documentation" section on page xiii.

Audience

Network engineers, system administrators, or telecom engineers should review this guide to learn the steps required to properly set up the Cisco Unified IP Phone on the network.

The tasks described are administration-level tasks and are not intended for end-users of the phones. Many of the tasks involve configuring network settings and affect the phone's ability to function in the network.

Because of the close interaction between the Cisco Unified IP Phone and Cisco Unified Communications Manager, many of the tasks in this manual require familiarity with Cisco Unified Communications Manager.

Organization

This manual is organized as follows:

Chapter	Description
Chapter 1, "An Overview of the Cisco Unified IP Phone"	Provides a conceptual overview and description of the Cisco Unified IP Phone.
Chapter 2, "Preparing to Install the Cisco Unified IP Phone on Your Network"	Describes how the Cisco Unified IP Phone interacts with other key IP telephony components, and provides an overview of the tasks required prior to installation.

Related Documentation

For more information about Cisco Unified IP Phones or Cisco Unified Communications Manager, refer to the following publications:

Cisco Unified IP Phones 8961, 9951, and 9971

These publications are available at the following URL:

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

- *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager*
- *Regulatory Compliance and Safety Information for Cisco Unified IP Phones*
- *Cisco Unified IP Phones 8900 Series*

Cisco Unified Communications Manager Administration

Related publications are available at the following URL:

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

Cisco Unified Communications Manager Business Edition

Related publications are available at the following URL:

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.

Document Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x	y	z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x	y	z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following convention:

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

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 customizeable 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.711µ-law, G.722, G.729a, G.729ab, and iLBC, and decode G.711a-law, G.711µ-law, G.722, G.729, G.729a, G.729b, G.729ab, and iLBC.

This chapter includes the following topics:

⚠ **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 *flash* (blink on and off rapidly), *pulse* (alternately dim and brighten), or appear *solid* (glow without interruption).
		• 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:
		• 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
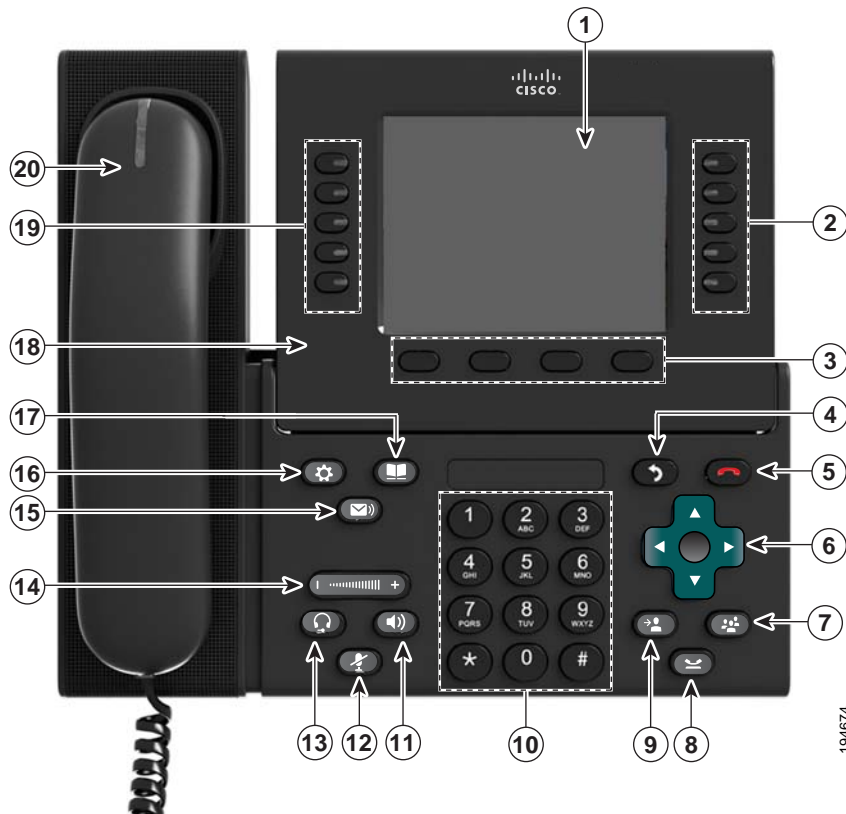
Table 1-2 describes the buttons on the Cisco Unified IP Phone 9951.

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	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 *flash* (blink on and off rapidly), *pulse* (alternately dim and brighten), or appear *solid* (glow without interruption).
		• 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	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).

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:
		• 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).

■   **Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 8.5 (SIP)**

1-6   OL-20861-01

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

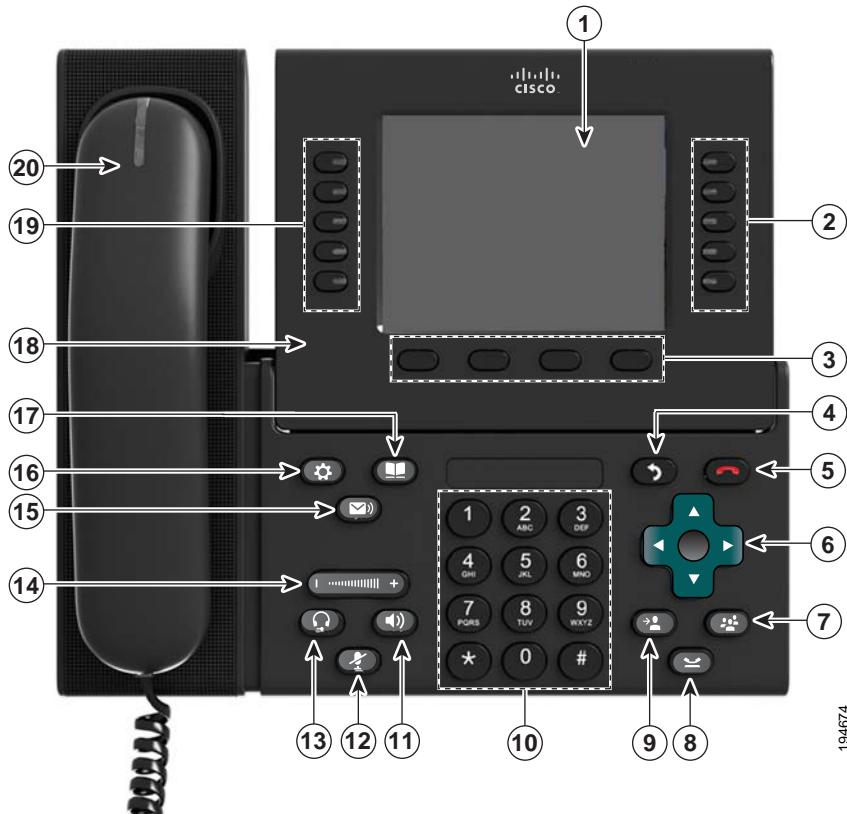*Figure 1-3*   **Cisco Unified IP Phone 9971**
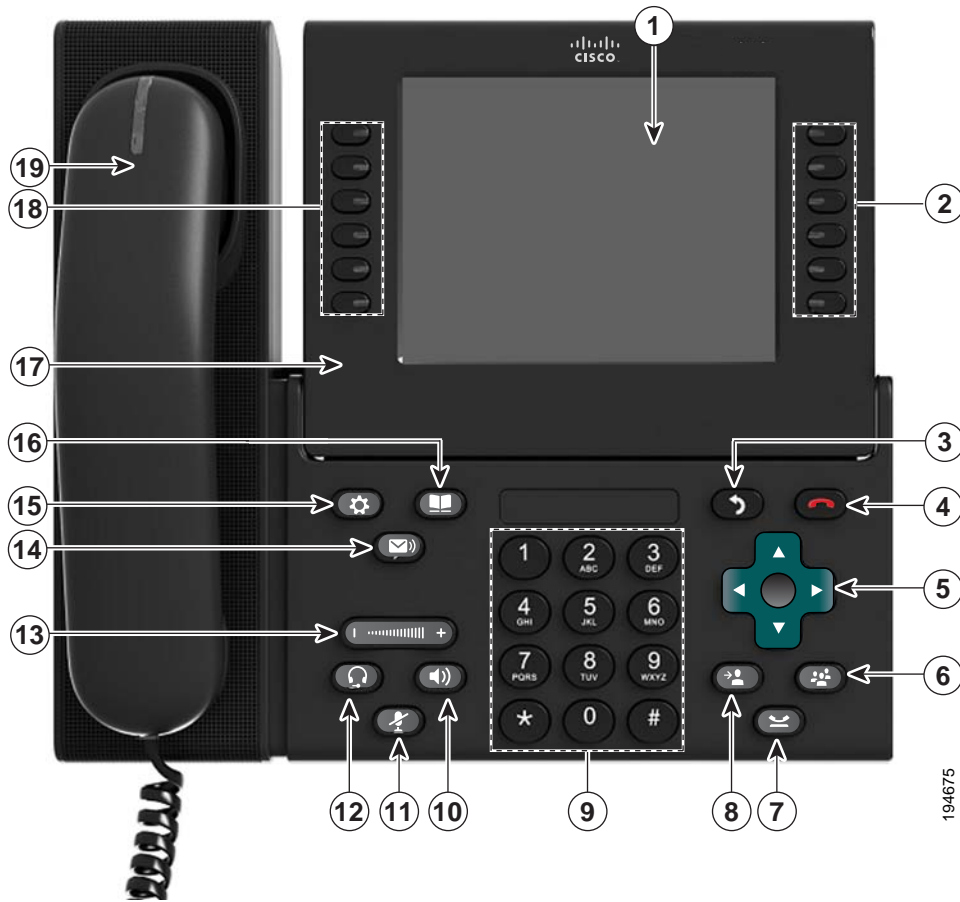
Table 1-3 describes the buttons on the Cisco Unified IP Phone 9971.

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 *flash* (blink on and off rapidly), *pulse* (alternately dim and brighten), or appear *solid* (glow without interruption).
		• 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:
		• 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 CUVA 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 *Cisco Unified Communications Manager System Guide*. **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.	The Cisco Unified IP Phone supports LLDP-MED on the SW port to communicate information such as: • Voice VLAN configuration • Device discovery • Power management • Inventory management For more information about LLDP-MED support, see the *LLDP-MED and Cisco Discovery Protocol* white paper: http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml
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.

Chapter 1   An Overview of the Cisco Unified IP Phone

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

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 *Cisco Unified Communications Manager System Guide*.
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

Chapter 1   An Overview of the Cisco Unified IP Phone

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

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 *Cisco Unified Communications Manager Security Guide*.
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 *Cisco Unified Communications Manager Security Guide*.
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	• 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	• See the "Troubleshooting Cisco Unified IP Phone Security" section on page 12-9 • Refer to the *Troubleshooting Guide for Cisco Unified Communications Manager*
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: • "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 [icon] 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 *Cisco Unified Communications Manager Security Guide*.
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: • 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.

4. 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:

1. A user initiates the call from a secured phone (secured security mode).

2. 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.

3. 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.	Gather the following information about the phone: • 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 Provides list of configuration requirements for setting up phones. Identifies preliminary configuration that you need to perform before configuring individual phones, such as phone button templates.	For more information, go to the "Cisco Unified IP Phones chapter in the *Cisco Unified Communications Manager System Guide.* See the "Telephony Features Available for the Cisco Unified IP Phone" section on page 8-2.
2.	Verify that you have sufficient unit license for your phone.	For more information, go to the "Licensing" section in the *Cisco Unified Communications Manager System Guide*.
3.	Customize phone button templates (if required). 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.	For more information, go to the Phone Button Template Configuration chapter in the *Cisco Unified Communications Manager Administration Guide*. See the "Modifying Phone Button Templates" section on page 8-29.

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.	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. Adds the device with its default settings to the Cisco Unified Communications Manager database.	For more information, go to the Cisco Unified IP Phone Configuration chapter in the *Cisco Unified Communications Manager Administration Guide*. For information about Product Specific Configuration fields, refer to "?" Button Help in the Phone Configuration window. **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 *Cisco Unified Communications Manager Administration Guide*.
5.	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. Adds primary and secondary directory numbers and features associated with directory numbers to the phone.	For more information, go to the "Directory Number Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*. See the "Telephony Features Available for the Cisco Unified IP Phone" section on page 8-2.
6.	Configure speed-dial buttons and assign speed-dial numbers (optional). Adds speed-dial buttons and numbers. Users can change speed-dial settings on their phones by using Cisco Unified CM User Options.	For more information, go to the "Configuring Speed-Dial Buttons or Abbreviated Dialing" section in the "Cisco Unified IP Phone Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.
7.	Configure Cisco Unified IP Phone services and assign services (optional). Provides IP Phone services. Users can add or change services on their phones by using the Cisco Unified CM User Options. **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. **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.	For more information, go to the "IP Phone Services Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*. See the "Setting Up Services" section on page 8-32.

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 *Cisco Unified Communications Manager Administration Guide*.
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 *Cisco Unified Communications Manager Administration Guide*. 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 *Cisco Unified Communications Manager Administration Guide*.
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 *Cisco Unified Communications Manager Administration Guide*: • "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 *Cisco Unified Communications Manager Administration Guide*.

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 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: • 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.	If you choose to deploy the Cisco Unified IP Phone 9971 on a wireless network, skip to Task 5.	See the "Configuring Startup Network Settings" section on page 3-21.
	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.	See the "Ethernet Setup Menu" section on page 7-4.
	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:	
	• 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.	
	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.	
	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**:	
	To disable DHCP and manually set an IP address:	
	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.	
	You must also enter the domain name where the phone resides. Press **Applications** and choose **Administrator Settings > Network Setup> Ethernet Setup**.	
5.	(Cisco Unified IP Phone 9971 only)	See Chapter 6, "Understanding the VoIP Wireless Network."
	If you choose to deploy the phone on the wireless network, you must configure the following:	
	• Configure the wireless network.	
	• Enable wireless LAN for phones on Cisco Unified Communications Administration.	
	• Configure a wireless network profile on the phone.	
	Note The wireless LAN on the phone does not activate when there are ethernet cables connected on the phone.	

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 *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide* 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

Preparing to Install the Cisco Unified IP Phone on Your Network

Cisco Unified IP Phones enable you to communicate by using voice over a data network. To provide this capability, the IP Phones depend upon and interact with several other key Cisco Unified IP Telephony components, including Cisco Unified Communications Manager.

This chapter focuses on the interactions between the Cisco Unified IP Phone 8961, 9951, and 9971 and Cisco Unified Communications Manager, DNS and DHCP servers, TFTP servers, and switches. It also describes options for powering phones.

For related information about voice and IP communications, refer to this URL:

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

This chapter provides an overview of the interaction between the Cisco Unified IP Phone and other key components of the Voice over IP (VoIP) network. It includes the following topics:

- Understanding Interactions with Other Cisco Unified IP Telephony Products, page 2-1
- Providing Power to the Cisco Unified IP Phone, page 2-3
- Understanding Phone Configuration Files, page 2-6
- Understanding the Phone Startup Process, page 2-7
- Adding Phones to the Cisco Unified Communications Manager Database, page 2-9
- Determining the MAC Address for a Cisco Unified IP Phone, page 2-13

Understanding Interactions with Other Cisco Unified IP Telephony Products

To function in the IP telephony network, the Cisco Unified IP Phone must be connected to a networking device, such as a Cisco Catalyst switch. You must also register the Cisco Unified IP Phone with a Cisco Unified Communications Manager system before sending and receiving calls.

This section includes the following topics:

- Understanding How the Cisco Unified IP Phone Interacts with Cisco Unified Communications Manager, page 2-2
- Understanding How the Cisco Unified IP Phone Interacts with the VLAN, page 2-2

Understanding How the Cisco Unified IP Phone Interacts with Cisco Unified Communications Manager

Cisco Unified Communications Manager is an open and industry-standard call processing system. Cisco Unified Communications Manager software sets up and tears down calls between phones, integrating traditional PBX functionality with the corporate IP network. Cisco Unified Communications Manager manages the components of the IP telephony system, such as the phones, the access gateways, and the resources necessary for features such as call conferencing and route planning. Cisco Unified Communications Manager also provides:

- Firmware for phones

- Configuration file, CTL, and Identity Trust List (ITL) files via the TFTP service

- Phone registration

- Call preservation, so that a media session continues if signaling is lost between the primary Communications Manager and a phone

For information about configuring Cisco Unified Communications Manager to work with the IP devices described in this chapter, go to the Cisco Unified IP Phone Configuration chapter in the *Cisco Communications Manager Administration Guide*.

For an overview of security functionality for the Cisco Unified IP Phone, see the "Understanding Security Features for Cisco Unified IP Phones" section on page 1-15.

Note   If the Cisco Unified IP Phone model that you want to configure does not appear in the Phone Type drop-down list in Cisco Unified Communications Manager Administration, go to the following URL and install the latest support patch for your version of Cisco Unified Communications Manager: http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

Related Topic
- Telephony Features Available for the Cisco Unified IP Phone, page 8-2

Understanding How the Cisco Unified IP Phone Interacts with the VLAN

The Cisco Unified IP Phone 8961, 9951, and 9971 have an internal Ethernet switch, enabling forwarding of packets to the phone, and to the Computer (access) port and the Network port on the back of the phone.

If a computer is connected to the Computer (access) port, the computer and the phone share the same physical link to the switch and share the same port on the switch. This shared physical link has the following implications for the VLAN configuration on the network:

- The current VLANs might be configured on an IP subnet basis. However, additional IP addresses might not be available to assign the phone to the same subnet as other devices connected to the same port.

- Data traffic present on the VLAN supporting phones might reduce the quality of Voice-over-IP traffic.

- Network security may indicate a need to isolate the VLAN voice traffic from the VLAN data traffic.

You can resolve these issues by isolating the voice traffic onto a separate VLAN. The switch port that the phone is connected to would be configured to have separate VLANs for carrying:

- Voice traffic to and from the IP phone (auxiliary VLAN on the Cisco Catalyst 6000 series, for example)
- Data traffic to and from the PC connected to the switch through the Computer (access) Port of the IP phone (native VLAN)

Isolating the phones on a separate, auxiliary VLAN increases the quality of the voice traffic and allows a large number of phones to be added to an existing network where there are not enough IP addresses for each phone.

For more information, refer to the documentation included with a Cisco switch. You can also access switch information at this URL:

http://cisco.com/en/US/products/hw/switches/index.html

Related Topics

- Understanding the Phone Startup Process, page 2-7
- Ethernet Setup Menu, page 7-4

Providing Power to the Cisco Unified IP Phone

The Cisco Unified IP Phone 8961, 9951, and 9971 can be powered with external power or with Power over Ethernet (PoE). External power is provided through a separate power supply. PoE is provided by a switch through the Ethernet cable attached to a phone.

Note   When you install a phone that is powered with external power, connect the power supply to the phone and to a power outlet before you connect the Ethernet cable to the phone. When you remove a phone that is powered with external power, disconnect the Ethernet cable from the phone before you disconnect the power supply.

The following sections provide more information about powering a phone:

- Power Guidelines, page 2-4
- Power Outage, page 2-4
- Reducing Power Consumption on the Phone, page 2-4
- Power Negotiation over LLDP, page 2-5
- Obtaining Additional Information About Power, page 2-5

Power Guidelines

Table 2-1 provides guidelines for powering the Cisco Unified IP Phone 8961, 9951, and 9971.

Table 2-1   Guidelines for Powering the Cisco Unified IP Phone 8961, 9951, and 9971

Power Type	Guidelines
External power—Provided through the CP-PWR-CUBE-4= external power supply.	The Cisco Unified IP Phone 8961, 9951, and 9971 use the CP-PWR-CUBE-4 power supply. **Note** You must use the CP-PWR-CUBE-4 when you deploy the Cisco Unified IP phone 9971 on a wireless Network.
External power—Provided through the Cisco Unified IP Phone Power Injector.	The Cisco Unified IP Phone Power Injector may be used with any Cisco Unified IP Phone. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco Unified IP Phone Power Injector is connected between a switch port and the IP Phone, and supports a maximum cable length of 100m between the unpowered switch and the IP Phone.
PoE power—Provided by a switch through the Ethernet cable attached to the phone.	• Cisco Unified IP Phone 8961, 9951, and 9971 support IEEE 802.3af Class 3 power on signal pairs and spare pairs. • Cisco Unified IP Phone 8961, 9951, and 9971 support IEEE 802.3at for external add-on devices. • To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply. • Make sure that the CatOS or IOS version running on your switch supports your intended phone deployment. Refer to the documentation for your switch for operating system version information.
External power—Provided through inline power patch panel WS-PWR-PANEL	The inline power patch panel WS-PWR-PANEL is compatible with the Cisco Unified IP Phone 8961, 9951, and 9971.

Power Outage

Your accessibility to emergency service through the phone is dependent on the phone being powered. If there is an interruption in the power supply, Service and Emergency Calling Service dialing will not function until power is restored. In the case of a power failure or disruption, you may need to reset or reconfigure equipment before using the Service or Emergency Calling Service dialing.

Reducing Power Consumption on the Phone

You can reduce the amount of energy that the Cisco Unified IP Phone consumes by scheduling when the phone goes into power save mode. In power save mode, the backlight on the screen is not lit when the phone is not in use. The phone remains in power save mode for the scheduled duration or until the user lifts the handset or presses any button. In the Phone Configuration page on Cisco Unified Communications Administration, configure the following parameters.

• Days Display Not Active—Specify the days that the backlight remains inactive.

• Display on Time—Schedule the time of day that the backlight automatically activates. on the days listed in the off schedule.

- Display on Duration—Indicates the length of time that the backlight is active once the backlight is enabled by the programmed schedule

- Display Idle Timeout—Defines the period of user inactivity on the phone before the backlight is turned off.

Power Negotiation over LLDP

The phone and the switch negotiate the power that the phone can consume. Cisco Unified IP Phone 8961, 9951, 9971 operate at multiple power settings, which lowers their consumption when less power is available.

After a phone reboots, the switch locks to one protocol (CDP or LLDP) for power negotiation. It locks to the first protocol (containing a power Threshold Limit Value (TLV)) that the phone transmits. If the system administrator disables that protocol on the phone, it cannot power up any accessories because the switch does not respond to power requests in the other protocol.

Cisco recommends that Power Negotiation always be enabled (default) when connecting to a switch that supports power negotiation.

If disabled, the switch may disconnect power to the phone. If the switch does not support power negotiation, then disable the Power Negotiation feature before you power up accessories over PoE. When the Power Negotiation feature is disabled, the phone can power the accessories up to 12.9W.

Note   When CDP and Power Negotiation are disabled, the phone can power the accessories up to 15.4W.

To enable or disable power negotiation, see Table 8-1, "Telephony Features for the Cisco Unified IP Phone".

Obtaining Additional Information About Power

For related information about power, refer to the documents shown in Table 2-2. These documents provide information about the following topics:

- Cisco switches that work with Cisco Unified IP Phones

- The Cisco IOS releases that support bidirectional power negotiation

- Other requirements and restrictions regarding power

Table 2-2   Related Documentation for Power

Document Topics	URL
Cisco Unified IP Phone Power Injector	http://www.cisco.com/en/US/products/ps6951/index.html
PoE Solutions	http://www.cisco.com/en/US/netsol/ns340/ns394/ns147/ns412/networking_solutions_package.html
Cisco Catalyst Switches	http://cisco.com/en/US/products/hw/switches/index.html
Integrated Service Routers	http://www.cisco.com/en/US/products/hw/routers/index.html
Cisco IOS Software	http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.html

Understanding Phone Configuration Files

Configuration files for a phone are stored on the TFTP server and define parameters for connecting to Cisco Unified Communications Manager. In general, any time you make a change in Cisco Unified Communications Manager that requires the phone to be reset, a change is automatically made to the phone's configuration file.

Configuration files also contain information about which image load the phone should be running. If this image load differs from the one currently loaded on a phone, the phone contacts the TFTP server to request the required load files.

A phone accesses a default configuration file named XmlDefault.cnf.xml from the TFTP server when the following conditions exist:

- You have enabled auto-registration in Cisco Unified Communications Manager
- The phone has not been added to the Cisco Unified Communications Manager database
- The phone is registering for the first time

Note If the device security mode in the configuration file is set to Authenticated or Encrypted, but the phone has not received a CTL or ITL file, the phone tries four times to obtain the file so it can register securely.

If auto registration is not enabled and the phone has not been added to the Cisco Unified Communications Manager database, the phone registration request will be rejected and display a blank screen.

If the phone has registered before, the phone will access the configuration file named SEPmac_address.cnf.xml, where mac_address is the MAC address of the phone.

The filenames are derived from the MAC address and description fields in the Phone Configuration window of Cisco Unified Communications Manager Administration. The MAC address uniquely identifies the phone.

Understanding the Phone Startup Process

When connecting to the VoIP network, the Cisco Unified IP Phone 8961, 9951, and 9971 go through a standard startup process that is described in Table 2-3. Depending on your specific network configuration, not all of these steps may occur on your Cisco Unified IP Phone.

Table 2-3   Cisco Unified IP Phone Startup Process

Task	Purpose	Related Topics
1.	Obtain power from the switch. If a phone is not using external power, the switch provides in-line power through the Ethernet cable attached to the phone.	• Adding Phones to the Cisco Unified Communications Manager Database, page 2-9. • Resolving Startup Problems, page 12-1.
2.	(For a Cisco Unified IP Phone 9971 in a wireless LAN only) Scanning for an access point. The Cisco Unified IP Phone scans the RF coverage area with its radio. The phone searches its network profiles and scans for access points that have a matching SSID and authentication type. The phone associates with the access point with the highest RSSI that matches with its network profile.	• Interacting with Cisco Unified Wireless APs, page 6-8.

3.	(For a Cisco Unified IP Phone 9971 in a wireless LAN only) Authenticating with the access point.
	
	The Cisco Unified IP Phone begins the authentication process:
	
	• If set for **Open**, then any device can authenticate to the access point. For added security, static WEP encryption might optionally be used.
	
	• If set to **Shared Key**, the phone encrypts the challenge text using the WEP key and the access point must verify that the WEP key was used to encrypt the challenge text before network access is available.
	
	• If set for **LEAP** or **EAP-FAST**, then the user name and password are authenticated by the RADIUS server before network access is available. For more information about the name and password authentication, see "WLAN Setup Menu" section on page 7-7.
	
	• If set for **Auto** (**AKM**), the phone looks for an access point with one of the following key management options enabled:
	  – WPA, WPA2, or CCKM—The username and password are authenticated by the RADIUS server before network access is available.
	  – WPA-Pre-shared key, WPA2-Pre-shared key—The phone authenticates with the access point using the pre-shared key.
		• Authentication Methods, page 6-11.

Table 2-3 **Cisco Unified IP Phone Startup Process (continued)**

Task	Purpose	Related Topics
4.	Load the stored phone image. The Cisco Unified IP Phone has non-volatile Flash memory in which it stores firmware images and user-defined preferences. At startup, the phone runs a bootstrap loader that loads a phone image stored in Flash memory. Using this image, the phone initializes its software and hardware.	• Resolving Startup Problems, page 12-1.
5.	Configure the VLAN. If the Cisco Unified IP Phone is connected to a Cisco Catalyst switch, the switch next informs the phone of the voice VLAN defined on the switch. The phone needs to know its VLAN membership before it can proceed with the Dynamic Host Configuration Protocol (DHCP) request for an IP address.	• Ethernet Setup Menu, page 7-4. • Resolving Startup Problems, page 12-1.
6.	Obtain an IP address. If the Cisco Unified IP Phone is using DHCP to obtain an IP address, the phone queries the DHCP server to obtain one. If you are not using DHCP in your network, you must assign static IP addresses to each phone locally.	• Ethernet Setup Menu, page 7-4. • Resolving Startup Problems, page 12-1.
7.	Requesting the CTL file. The TFTP server stores the CTL file. This file contains the certificates necessary for establishing a secure connection between the phone and Cisco Unified CM.	Refer to *Cisco Unified Communications Manager Security Guide*, Configuring the Cisco CTL Client.
8.	Requesting the ITL file. The phone requests the ITL file after it requests the CTL file. The ITL file contains the certificates of the entities that the phone can trust. The certificates are used for authenticating a secure connection with the servers or authenticating a digital signature signed by the servers. The ITL file is supported on the Cisco Unified CM 8.5 and later.	See the "Preparing to Install the Cisco Unified IP Phone on Your Network" chapter. See the "Troubleshooting and Maintenance" chapter.
9.	Access a TFTP server. In addition to assigning an IP address, the DHCP server directs the Cisco Unified IP Phone to a TFTP Server. If the phone has a statically defined IP address, you must configure the TFTP server locally on the phone; the phone then contacts the TFTP server directly. **Note** You can also assign an alternative TFTP server to use instead of the one assigned by DHCP.	• Ethernet Setup Menu, page 7-4. • Resolving Startup Problems, page 12-1.

Table 2-3   Cisco Unified IP Phone Startup Process (continued)

Task	Purpose	Related Topics
10.	Request the configuration file. The TFTP server has configuration files, which define parameters for connecting to Cisco Unified Communications Manager and other information for the phone.	• Adding Phones to the Cisco Unified Communications Manager Database, page 2-9. • Resolving Startup Problems, page 12-1.
11.	Contact Cisco Unified CM The configuration file defines how the Cisco Unified IP Phone communicates with Cisco Unified CM and provides a phone with its load ID. After obtaining the file from the TFTP server, the phone attempts to make a connection to the highest priority Cisco Unified CM on the list. If the security profile of the phone is configured for secure signaling (encrypted or authenticated), and the Cisco Unified CM is set to secure mode, the phone makes a TLS connection. Otherwise, it makes a nonsecure TCP connection. If the phone was manually added to the database, Cisco Unified Communications Manager identifies the phone. If the phone was not manually added to the database and auto-registration is enabled in Cisco Unified Communications Manager, the phone attempts to auto-register itself in the Cisco Unified Communications Manager database. **Note** Autoregistration is disabled when you configure the CTL client. In this case, the phone must be manually added to the Cisco Unified CM database.	See the "Preparing to Install the Cisco Unified IP Phone on Your Network" chapter. See the "Troubleshooting and Maintenance" chapter.

Adding Phones to the Cisco Unified Communications Manager Database

Before installing the Cisco Unified IP phone, you must choose a method for adding phones to the Cisco Unified Communications Manager database. These sections describe the methods:

- Adding Phones with Auto-Registration, page 2-10
- Adding Phones with Auto-Registration and TAPS, page 2-11
- Adding Phones with Cisco Unified Communications Manager Administration, page 2-12
- Adding Phones Using BAT Phone Template, page 2-12

Table 2-4 provides an overview of these methods for adding phones to the Cisco Unified Communications Manager database.

Table 2-4   Methods for Adding Phones to the Cisco Unified Communications Manager Database

Method	Requires MAC Address?	Notes
Auto-registration	No	Results in automatic assignment of directory numbers
Auto-registration with TAPS	No	Requires auto-registration and the Bulk Administration Tool (BAT); updates information in the Cisco Unified IP Phone and in Cisco Unified Communications Manager Administration
Using the Cisco Unified Communications Manager Administration	Yes	Requires phones to be added individually
Using BAT	Yes	Allows for simultaneous registration of multiple phones

Adding Phones with Auto-Registration

By enabling auto-registration before you begin installing phones, you can:

- Add phones without first gathering MAC addresses from the phones.
- Automatically add a Cisco Unified IP Phone to the Cisco Unified Communications Manager database when you physically connect the phone to your IP telephony network. During auto-registration, Cisco Unified Communications Manager assigns the next available sequential directory number to the phone.
- Quickly enter phones into the Cisco Unified Communications Manager database and modify any settings, such as the directory numbers, from Cisco Unified Communications Manager.
- Move auto-registered phones to new locations and assign them to different device pools without affecting their directory numbers.

Note Cisco recommends you use auto-registration to add less than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT). See the "Adding Phones Using BAT Phone Template" section on page 2-12.

Auto-registration is disabled by default. In some cases, you might not want to use auto-registration; for example, if you want to assign a specific directory number to the phone, or use a secure connection with Cisco Unified CM as described in Cisco Unified CM Security Guide. For information about enabling auto-registration, go to the "Enabling Auto-Registration" section in the *Cisco Unified Communications Manager Administration Guide.*

Related Topics

- Adding Phones with Auto-Registration and TAPS, page 2-11
- Adding Phones with Cisco Unified Communications Manager Administration, page 2-12
- Adding Phones Using BAT Phone Template, page 2-12

Adding Phones with Auto-Registration and TAPS

You can add phones with auto-registration and TAPS, the Tool for Auto-Registered Phones Support, without first gathering MAC addresses from phones.

TAPS works with the Bulk Administration Tool (BAT) to update a batch of phones that were already added to the Cisco Unified Communications Manager database with dummy MAC addresses. Use TAPS to update MAC addresses and download pre-defined configurations for phones.

Note   Cisco recommends you use auto-registration and TAPS to add less than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT). See the "Adding Phones Using BAT Phone Template" section on page 2-12.

To implement TAPS, you or the end-user dial a TAPS directory number and follow voice prompts. When the process is complete, the phone will have downloaded its directory number and other settings, and the phone will be updated in Cisco Unified Communications Manager Administration with the correct MAC address.

Auto-registration must be enabled in Cisco Unified Communications Manager Administration (**System > Cisco Unified CM**) for TAPS to function.

Note   When you configure the cluster for mixed mode through the Cisco CTL client, auto-registration is automatically disabled. When you configure the cluster for non-secure mode through the Cisco CTL client, auto-registration is not enabled automatically.

For more information, refer to the *Cisco Unified Communications Manager Bulk Administration Guide*.

Related Topics

- Adding Phones with Auto-Registration, page 2-10
- Adding Phones with Cisco Unified Communications Manager Administration, page 2-12
- Adding Phones Using BAT Phone Template, page 2-12

Adding Phones with Cisco Unified Communications Manager Administration

You can add phones individually to the Cisco Unified Communications Manager database by using Cisco Unified Communications Manager Administration. To do so, you first need to obtain the MAC address for each phone.

For information about determining a MAC address, see the "Determining the MAC Address for a Cisco Unified IP Phone" section on page 2-13.

After you have collected MAC addresses, in Cisco Unified Communications Manager Administration, choose **Device > Phone** and click **Add New** to begin.

For complete instructions and conceptual information about Cisco Unified Communications Manager, go to the "Cisco Unified Communications Manager Overview" chapter in the *Cisco Unified Communications Manager System Guide*.

Related Topics

- Adding Phones with Auto-Registration, page 2-10
- Adding Phones with Auto-Registration and TAPS, page 2-11
- Adding Phones Using BAT Phone Template, page 2-12

Adding Phones Using BAT Phone Template

The Cisco Unified Communications Bulk Administration Tool (BAT) enables you to perform batch operations including registration on multiple phones.

To add phones using BAT only (not in conjunction with TAPS), you must obtain the appropriate MAC address for each phone.

For information about determining a MAC address, see the "Determining the MAC Address for a Cisco Unified IP Phone" section on page 2-13.

For detailed instructions about adding phones using Bulk Administration menu, refer to the *Cisco Unified Communications Manager Bulk Administration Guide*, chapter Inserting Phones.

To add a phone to the Cisco Unified Communications Manager, follow these steps:

Procedure

Step 1   From Cisco Unified Communications Manager, choose **Bulk Administration > Phones > Phone Template**.

Step 2   Click **Add New**.

Step 3   Choose a Phone Type and click **Next**.

Step 4   Enter the details of phone specific parameters like Device Pool, Phone Button Template, Device Security Profile and so on.

Step 5   Click **Save**.

Step 6   From Cisco Unified Communications Manager, choose **Device > Phone > Add New** to add a phone using an existing BAT phone template.

For more information about using BAT, refer to the *Cisco Unified Communications Manager Bulk Administration Guide*. For more information about creating of BAT Phone Templates, see the *Cisco Unified Communications Manager Bulk Administration Guide*, Phone Template.

Related Topics

- Adding Phones with Auto-Registration, page 2-10

- Adding Phones with Auto-Registration and TAPS, page 2-11

- Adding Phones with Cisco Unified Communications Manager Administration, page 2-12

Determining the MAC Address for a Cisco Unified IP Phone

Several procedures described in this manual require you to determine the MAC address of a Cisco Unified IP Phone. You can determine a phone's MAC address in these ways:

- From the phone, press the **Applications** button and choose **Phone Information** and look at the MAC Address field.

- Look at the MAC label on the back of the phone.

- Display the web page for the phone and click the **Device Information** hyperlink.

  For information about accessing the web page, see the "Accessing the Web Page for a Phone" section on page 11-2.

Setting Up the Cisco Unified IP Phone

This chapter includes the following topics, which help you install the Cisco Unified IP Phone on an IP telephony network:

- Before You Begin, page 3-1
- Understanding the Cisco Unified IP Phone Components, page 3-2
- Installing the Cisco Unified IP Phone, page 3-11
- Connecting the Footstand, page 3-19
- Phone Display Viewing Angle, page 3-20
- Verifying the Phone Startup Process, page 3-21
- Configuring Startup Network Settings, page 3-21
- Configuring Security on the Cisco Unified IP Phone, page 3-21

Note Before you install a Cisco Unified IP phone, you must decide how to configure the phone in your network. Then you can install the phone and verify its functionality. For more information, see Chapter 2, "Preparing to Install the Cisco Unified IP Phone on Your Network."

Before You Begin

Before installing the Cisco Unified IP Phone, review the requirements in these sections:

- Network Requirements, page 3-1
- Cisco Unified Communications Manager Configuration, page 3-2

Network Requirements

For the Cisco Unified IP Phone to successfully operate as a Cisco Unified IP Phone endpoint in your network, your network must meet the following requirements:

- Working Voice over IP (VoIP) Network:
    - VoIP configured on your Cisco routers and gateways
    - Cisco Unified Communications Manager installed in your network and configured to handle call processing

- IP network that supports DHCP or manual assignment of IP address, gateway, and subnet mask

> **Note** The Cisco Unified IP Phone displays the date and time from Cisco Unified Communications Manager.

- Voice over Wireless LAN (Optional for Cisco Unified IP Phone 9971)
  - Cisco Aironet Access Points (APs) configured to support Voice over WLAN (VoWLAN)
  - Controllers and switches configured to support VoWLAN
  - Security implemented for authenticating wireless voice devices and users

Cisco Unified Communications Manager Configuration

The Cisco Unified IP Phone requires Cisco Unified Communications Manager to handle call processing. Refer to *Cisco Unified Communications Manager Administration Guide* or to context-sensitive help in the Cisco Unified Communications Manager application to ensure that Cisco Unified Communications Manager is set up properly to manage the phone and to properly route and process calls.

If you plan to use auto-registration, verify that it is enabled and properly configured in Cisco Unified Communications Manager Administration before connecting any Cisco Unified IP Phone to the network. For information about enabling and configuring auto-registration, refer to *Cisco Unified Communications Manager Administration Guide*. Also, see the "Adding Phones to the Cisco Unified Communications Manager Database" section on page 2-9.

You must use Cisco Unified Communications Manager Administration to configure and assign telephony features to the Cisco Unified IP Phones. See the "Telephony Features Available for the Cisco Unified IP Phone" section on page 8-2 for details.

In Cisco Unified Communications Manager Administration, you can add users to the database and associate them with specific phones. In this way, users gain access their Cisco Unified CM User Option page to configure items such as call forwarding, speed dialing, and voice messaging system options. See the "Adding Users to Cisco Unified Communications Manager" section on page 8-33 for details.

Understanding the Cisco Unified IP Phone Components

The Cisco Unified IP Phone includes these components on the phone or as accessories for the phone:

- Network and Computer Ports, page 3-3
- Handset Rest, page 3-3
- Speakerphone, page 3-4
- Accessory Support on the Cisco Unified IP Phone 8961, 9951, and 9971, page 3-4
- USB Port Data Information, page 3-5
- External Speakers and Microphone, page 3-5
- Headsets, page 3-5
- Using External Devices, page 3-11

Network and Computer Ports

The back of the Cisco Unified IP Phone includes these ports:

- Network port
- Computer port

Each port supports 10/100/1000 Mbps half- or full-duplex (except for full-duplex only for 1000 Mbps) connections to external devices. You can use either Category 3 or 5 cabling for 10-Mbps connections, but you must use Category 5/5e for 100 and 1000 Mbps connections.

Use the SW network port to connect the phone to the network. You must use a straight-through cable on this port. The phone can also obtain inline power from a switch over this connection. See the "Adding Phones to the Cisco Unified Communications Manager Database" section on page 2-9 for details.

Use the Computer port to connect a network device, such as a computer, to the phone. You must use a straight-through cable on this port.

Handset Rest

The wideband-capable handset is designed especially for use with a Cisco Unified IP Phone. It includes a light strip that indicates incoming calls and voice messages waiting.

To connect a handset to the Cisco Unified IP Phone, plug the cable into the handset and the Handset port on the back of the phone.

With a wall-mounted phone, you might need to adjust the handset rest to ensure that the receiver will not slip out of the cradle, as shown in Figure 3-1.

Figure 3-1   Removing the Hookswitch Clip
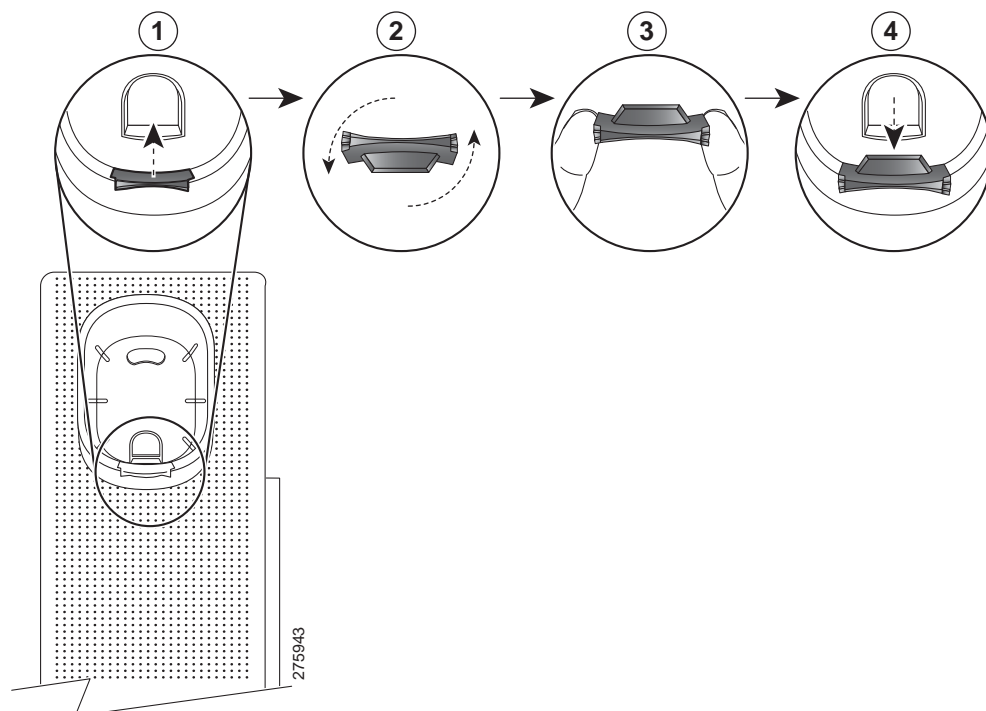
1	Remove handset from the cradle and pull the plastic tab from the handset rest.
2	Rotate the tab 180 degrees.
3	Hold the tab between two fingers, with the corner notches facing you.
4	Line up the tab with the slot in the cradle, and press the tab evenly into the slot. An extension protrudes from the top of the rotated tab. Return the handset to the handset rest.

Speakerphone

By default, the wideband-capable speakerphone is enabled on the Cisco Unified IP Phone.

You can disable the speakerphone by using Cisco Unified Communications Manager Administration. To do so, choose **Device > Phone** and locate the phone you want to modify. In the Phone Configuration window for the phone, check the **Disable Speakerphone** check box.

Accessory Support on the Cisco Unified IP Phone 8961, 9951, and 9971

Table 3-1 indicates the accessories that the Cisco Unified IP Phones 8961, 9951, and 9971 support; an "X" indicates support for a particular phone model and a dash (—) indicates non-support:

Table 3-1   Accessory support for the Cisco Unified IP Phone 8961, 9951, and 9971

Accessory	Type	Cisco Unified IP Phone		
		8961	9951	9971
Cisco Accessory				
Cisco Unified IP Color Key Expansion Module—See Chapter 4, "Setting Up the Cisco Unified IP Color Key Expansion Module."	Add-on module	1	up to 2	up to 3
Cisco Unified Video Camera—See Chapter 5, "Setting Up the Cisco Unified Video Camera."	Add-on module	—	X	X
Third-Party Accessories				
Headsets—See the "Headsets" section on page 3-5. This section includes information on each headset type.	Analog	X	X	X
	Analog Wideband	X	X	X
	Bluetooth	—	X	X
	USB(wired or wireless)	X	X	X
Microphone—See "External Speakers and Microphone" section on page 3-5.	External PC	—	X	X
Speakers—See "External Speakers and Microphone" section on page 3-5.	External PC	—	X	X

USB Port Data Information

The Cisco Unified IP Phone supports a maximum of five devices connected to each USB port. Each device connected to the phone is included in the maximum device count. For example, your phone can support five USB devices (such as three Cisco Unified IP Color Key Expansion modules, one hub, and one other standard USB device) on the side port and five additional standard USB devices on the back port (the Cisco Unified IP Phone 8961 does not have a back USB port). (Many third-party USB products count as several USB devices, so refer to documentation that came with a third-party product.)

> **Note**   Unpowered hubs are not supported, and powered hubs with more than four ports are not supported.

> **Note**   USB headsets connected to the phone through a USB hub are not supported.
> The Cisco Unified Video Camera connected to the phone through a USB hub is not supported.

External Speakers and Microphone

External speakers and microphones are plug-and-play accessories. You can connect an external PC-type microphone and powered speakers (with amplifier) on the Cisco Unified IP Phone 9951 or 9971 using the line in/out jacks. Connecting an external microphone disables the internal microphone and connecting an external speaker will disable the phone's internal speaker.

> **Note**   Using poor quality external audio devices, playing loudspeakers at very loud volumes or placing the microphone very close to the loudspeaker may result in undesirable echo heard by other parties on your speakerphone calls.

Headsets

Although Cisco Systems performs internal testing of third-party headsets for use with the Cisco Unified IP Phones, Cisco does not certify or support products from headset or handset vendors.

The phone reduces some background noise that is detected by a headset microphone, but if you want to further reduce the background noise and improve the overall audio quality, use a noise cancelling headset.

Cisco recommends the use of good quality external devices, for example, headsets that are screened against unwanted radio frequency (RF) and audio frequency (AF) signals. Depending on the quality of headsets and their proximity to other devices such as mobile (cell) phones and two-way radios, some audio noise or echo may still occur. An audible hum or buzz may be heard by either the remote party or by both the remote party and the Cisco Unified IP Phone user. Humming or buzzing sounds can be caused by a range of outside sources; for example, electric lights, electric motors, or large PC monitors. See , for more information.

> **Note**   In some cases, hum may be reduced or eliminated by using a local power cube or power injector.

These environmental and hardware inconsistencies in the locations where Cisco Unified IP Phones are deployed means that there is not a single headset solution that is optimal for all environments.

Cisco recommends that customers test headsets in their intended environment to determine performance before making a purchasing decision and deploying en masse.

Audio Quality Subjective to the User

Beyond the physical, mechanical and technical performance, the audio portion of a headset must sound good to the user and to the party on the far end. Sound quality is subjective and Cisco cannot guarantee the performance of any headsets. However, a variety of headsets from leading headset manufacturers have been reported to perform well with Cisco Unified IP Phones. See manufacturer's sites for details.

Wired Headsets

To connect a wired headset to the Cisco Unified IP Phone, plug it into the Headset port on the back of the phone. Press the **Headset** button on the phone to place and answer calls using the headset.

You can use the wired headset with all of the features on the Cisco Unified IP Phone, including the Volume and Mute buttons. Use these buttons to adjust the ear piece volume and to mute the speech path from the headset microphone.

If the headset is analog, see the "Analog Headsets" section on page 3-7 for the procedure on configuring the wideband codec.

Disabling a Wired Headset

You can disable the headset by using Cisco Unified Communications Manager Administration. If you do so, you also will disable the speakerphone.

To disable the headset from Cisco Unified Communications Manager Administration, choose **Device > Phone** and locate the phone that you want to modify. In the Phone Configuration window (Product Specific Configuration layout portion), select the **Disable Speakerphone and Headset** check box.

USB Headsets

Wired and wireless USB headsets are also supported. You can connect a USB headset (or the base station for a wireless headset) to either the Back USB port (if your phone has this port) or the Side USB port. (The Cisco Unified IP Phone 9951 and 9971 contain both a back USB port and a side USB port, while the Cisco Unified IP Phone 8961 contains only a side USB port). For more information about wireless headsets, see the "Wireless Headsets" section on page 3-8.

You must enable the applicable USB Port (either the Back USB Port parameter or the Side USB Port parameter) in Cisco Unified Communications Manager Administration (in the Product Specific Configuration layout portion on the window). Also, for the Enable/Disable USB Classes parameter in Cisco Unified Communications Manager Administration, make sure that "Audio Class" is selected.

These parameters can be enabled on either the Phone Configuration window (**Device > Phone**), the Enterprise Phone Configuration window (**System > Enterprise Phone Configuration**), or the Common Phone Profile window (**Device > Device Settings > Common Phone Profile**). Also check the corresponding Override Common Settings parameter in the configuration window.

For more information about parameters that can be configured in any of these three configuration windows, see the "Configuring Product Specific Configuration Parameters" section on page 8-26.

Disabling the USB Headset

To disable the USB headset, disable the USB port (or disable the Audio Class parameter) that you enabled in Cisco Unified Communications Manager Administration. Also, you can select another type of headset in the Accessories window on the phone, thus disabling the previously enabled headset.

Analog Headsets

Analog headsets are supported on the Cisco Unified IP Phone 8961, 9951, and 9971. However, the Cisco Unified IP Phone 8961, 9951, and 9971 cannot detect when there is an analog headset plugged in. For this reason, the analog headset will appear by default in the Accessories page on the phone screen. (Press the **Applications** button 🔘 and select **Accessories**.)

The main reason for this is to allow users to enable wideband for the analog headset. The phone is unable to detect if the headset supports the wideband codec, but the user can enable wideband on analog headsets by following these steps:

Procedure

Step 1   On the Cisco Unified IP Phone, press the **Applications** button 🔘 .

Step 2   Select **Accessories**.

Step 3   Highlight the analog headset, then press the **Setup** softkey.

Step 4   Turn wideband on/off for the selected headset by using the on/off toggle.

If the wideband on/off toggle is not enabled, follow the steps below to make sure the user can enable wideband codec on an analog headset:

Procedure

Step 1   In Cisco Unified Communications Manager Administration, go to **Device > Phone.**

Step 2   In the Find and List Phones window, enter the search criteria for the phone to which you want to add the analog headset, then click **Find**.

Step 3   Click on the Device Name you want; the Phone Configuration window displays.

Step 4   On the Product Specific Configuration Layout portion of the Phone Configuration window, be sure the option called Wideband Headset UI Control is enabled (enabled by default).

Step 5   (Optional) Also on the Product Specific Configuration Layout portion of the Phone Configuration window, you can set the Wideband Headset option (also enabled by default) in that window.

Wireless Headsets

The Cisco website provides information about wireless headsets that work with your IP phone. Go to the following URL:

http://www.cisco.com/en/US/partner/prod/voicesw/ucphone_headsets.html

1. Choose **IP Communications** from the Enter Solution drop-down list box. The Select a Solution Category drop-down list box displays.

2. Choose **IP Phone Headsets** to see a list of Technology Development Program partners.

Refer to the wireless headset documentation for information about connecting the headset and using the features.

Using Bluetooth Wireless Headsets

The Cisco Unified IP Phone 9951 and 9971 support Bluetooth Class 2 technology when the headsets support Bluetooth. Bluetooth enables low-bandwidth wireless connections within a range of 30 feet (10 meters). The best performance is in the 3- to 6-foot range (1 to 2 meters). You can pair up to 5 headsets, but only the last one connected is used as the default.

There can be a potential interference issues. Cisco recommends that you reduce the proximity of other 802.11b/g devices, Bluetooth devices, microwave ovens, and large metal objects. If possible, configure other 802.11 devices to use the 802.11a channels.

For a Bluetooth wireless headset to work, it does not need to be within direct line-of-sight of the phone, but some barriers, such as walls or doors, and interference from other electronic devices, could affect the connection.

Handsfree Profile

Your phone supports various Handsfree Profile features that enable you to use handsfree devices (such as Bluetooth wireless headsets) to perform certain tasks without having to handle the phone. For example, instead of pressing Redial on the phone, users can redial a number from their Bluetooth wireless headset according to instructions from the headset manufacturer.

These handsfree features apply to Bluetooth wireless headsets used with the Cisco Unified IP Phone 9951 and 9971:

- Answer a call
- End a call
- Change the headset volume for a call
- Redial
- Caller ID
- Reject
- Divert
- Hold and Accept
- Release and Accept

Handsfree devices may differ in how features are activated. Device manufacturers may also use different terms when referring to the same feature.

For more information, see the manufacturer's documentation.

Adding a Bluetooth Wireless Headset to the Phone

The Cisco Unified IP Phones 9951 and 9971 support Bluetooth wireless headsets.

You can enable your bluetooth wireless headset by following these steps:

Procedure

Step 1   In Cisco Unified Communications Manager administration, choose **Device > Phone,** locate the phone you want to modify, and go to the Phone Configuration window for that phone.

Step 2   In the Phone Configuration window, select **Enable** for the Bluetooth setting and **Handsfree** for the Bluetooth Profiles settings.

Step 3   Save your changes.

After the bluetooth wireless headset is enabled through Cisco Unified Communications Manager Administration, you must add the headset as an accessory to the phone by using following these steps:

Procedure

Step 1   On the Cisco Unified IP Phones 9951 or 9971, press the **Applications** button and select **Accessories**.

Step 2   Select **Add Bluetooth Accessory**.

The Adding Bluetooth Accessory window appears. A message tells you to make sure your accessory is "discoverable," which means that the Bluetooth should be powered on and in "discoverable" or "pairing" mode.

Once the Bluetooth device is located, its name will appear in the window, and a message appears that asks for a PIN so that the Bluetooth device can be paired with the Cisco Unified IP Phone.

Step 3   The Cisco Unified IP Phone automatically tries to pair with the headset by using a PIN of "0000." If the headset uses a different PIN, enter the correct PIN by referring to the user guide that came with the headset.

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

Once the phone has the correct pin, the phone will try to connect to the accessory. The phone will provide feedback to the user while it is trying to connect the accessory. If unable to connect, an error alert will be shown to let the user know the reason for the failure. There will be a timeout of 10 seconds for the phone to try to connect the accessory. If the timer expires without a successful connection, an error alert will be displayed.

The Cisco Unified IP Phone connects with headsets using a shared key authentication and encryption method. The Cisco Unified IP Phone can be connected with up to five headsets at a time. The last one connected is used as the default. Pairing is typically performed once for each headset.

Once a device has been paired, its Bluetooth connection is maintained as long as both devices (phone and headset) are enabled and within range of each other. The connection typically re-establishes itself automatically if either of the devices powers down then powers up. However, some headsets require user action to re-establish the connection.

The Bluetooth icon indicates whether or not a device is connected.

When headsets are more than 30 feet (10 meters) away from the Cisco Unified IP Phone, Bluetooth drops the connection after a 15- to 20-second timeout. If the paired headset comes back into range of the Cisco Unified IP Phone and the phone is not connected to another Bluetooth headset, the in-range Bluetooth headset automatically reconnects. For certain phone types that operate in power-save modes, the user may have to "wake-up" the headset by tapping on its operational button to initiate the reconnect.

Removing a Bluetooth Device From the Phone

To remove a Bluetooth device from the Cisco Unified IP Phone 9951 or 9971, follow these steps:

Procedure

Step 1   Press the **Applications** button .

Step 2   Select **Accessories**.

Step 3   Highlight the device you want to remove and press the **Delete** softkey.

Related Documentation About Bluetooth Wireless Headsets

For information about how to use your Bluetooth wireless headset, see:

* *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager*
* User guides that were provided with your headset

Important Note about Headset Types

Only one headset type will work at any given time, so if you have both a Bluetooth headset and an analog headset attached to the phone, enabling the Bluetooth headset disables the analog headset. To enable the analog headset, disable the Bluetooth headset. Plugging a USB headset into a phone that has Bluetooth headset enabled disables both the Bluetooth and analog headset. If you unplug the USB headset, then you can either enable the Bluetooth headset or disable the Bluetooth headset to use the analog headset.

Using External Devices

Cisco recommends the use of good quality external devices (such as speakers, microphones, and headsets) that are shielded (screened) against unwanted radio frequency (RF) and audio frequency (AF) signals.

Depending on the quality of these devices and their proximity to other devices such as mobile phones or two-way radios, some audio noise may still occur. In these cases, Cisco recommends that you take one or more of the following actions:

- Move the external device away from the source of the RF or AF signals.
- Route the external device cables away from the source of the RF or AF signals.
- Use shielded cables for the external device, or use cables with a better shield and connector.
- Shorten the length of the external device cable.
- Apply ferrites or other such devices on the cables for the external device.

Cisco cannot guarantee the performance of the system because Cisco has no control over the quality of external devices, cables, and connectors. The system will perform adequately when suitable devices are attached using good quality cables and connectors.

⚠️

Caution   In European Union countries, use only external headsets that are fully compliant with the EMC Directive [89/336/EC].

Installing the Cisco Unified IP Phone

You must connect the Cisco Unified IP Phone to the network and to a power source before using it. See Figure 3-2, Figure 3-4 and Figure 3-6 for graphical representations of the back connections for Cisco Unified IP Phones 8961, 9951, and 9971, respectively. See Figure 3-3, Figure 3-5, and Figure 3-7 for graphical representations of the side connections for Cisco Unified IP Phones 8961, 9951, and 9971, respectively.

Note   Before you install a phone, even if it is new, upgrade the phone to the current firmware image.

Before using external devices, read the "Using External Devices" section on page 3-11 for safety and performance information.

Note   Firmware upgrades over the WLAN interface may take longer than upgrading over the wired interface, depending on the quality and bandwidth of the wireless connection. Some upgrades may take more than hour.

To install a Cisco Unified IP Phone, you must perform the task described in Table 3-2.

Table 3-2   Installing the Cisco Unified IP Phone

Task	Purpose	Related Topics
1.	Connect the handset to the handset port.	—
2.	Connect a headset to the headset port. Optional. You can add a headset later if you do not connect one now.	See the "Headsets" section on page 3-5 for more information.
3.	(Optional) Connect a wireless headset (for the Cisco Unified IP Phone 9951 and 9971 only). You can add a wireless headset later if you do not want to connect one now.	Refer to your wireless headset documentation for information.
4.	Connect a straight-through Ethernet cable from the switch to the network port labeled 10/100/1000 SW on the Cisco Unified IP Phone. Each Cisco Unified IP Phone ships with one Ethernet cable in the box. Use either Category 3/5/5e cabling for 10-Mbps connections, use Category 5/5e for 100 Mbps connections, and use Category 5e for 1000Mbps connections.	See the "Network and Computer Ports" section on page 3-3 for guidelines.
5.	Connect a straight-through Ethernet cable from another network device, such as a desktop computer, to the Computer port on the Cisco Unified IP Phone. Optional. You can connect another network device later if you do not connect one now. You can use either Category 3/5/5e cabling for 10-Mbps connections, use Category 5/5e for 100 Mbps connections, and use Category 5e for 1000Mbps connections.	See the "Network and Computer Ports" section on page 3-3 for guidelines.
6.	(Optional) Enable the phone to use the wireless local area network (WLAN). **Note** You must disconnect all ethernet connections if you deploy the Cisco Unified IP Phone 9971 on a wireless LAN.	

Figure 3-2   *Cisco Unified IP Phone 8961 Connections (Back)*
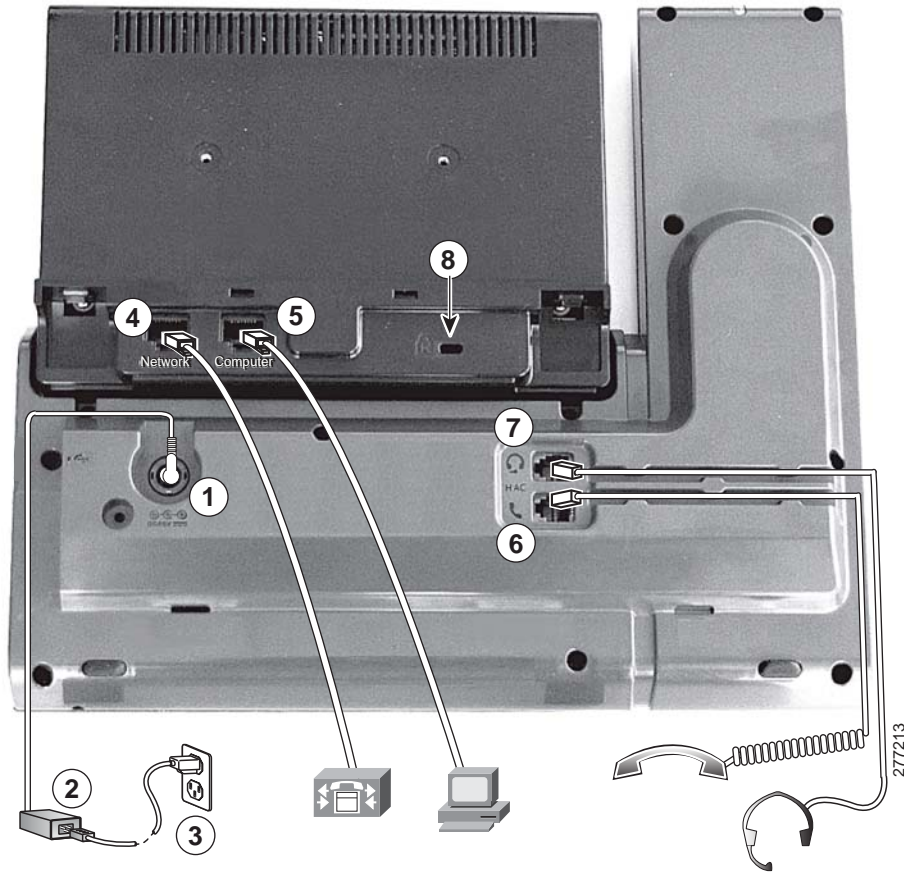
1	DC adaptor port (DC48V)	**5**	Computer port (10/100/1000 PC) connection
2	AC-to-DC power supply (optional)	**6**	Handset Connection
3	AC power wall plug (optional)	**7**	Analog Headset Connection (optional)
4	Network port (10/100/1000 SW) with IEEE 802.3af and 802.3at power enabled	**8**	Anti-theft security lock connector (lock optional)

Figure 3-3   *Cisco Unified IP Phone 8961 Cable Connections (Side)*

1	USB port	2	Accessory connector (such as for the Cisco Unified IP Color Key Expansion Module)

Figure 3-4   *Cisco Unified IP Phone 9951 Cable Connections (Back)*
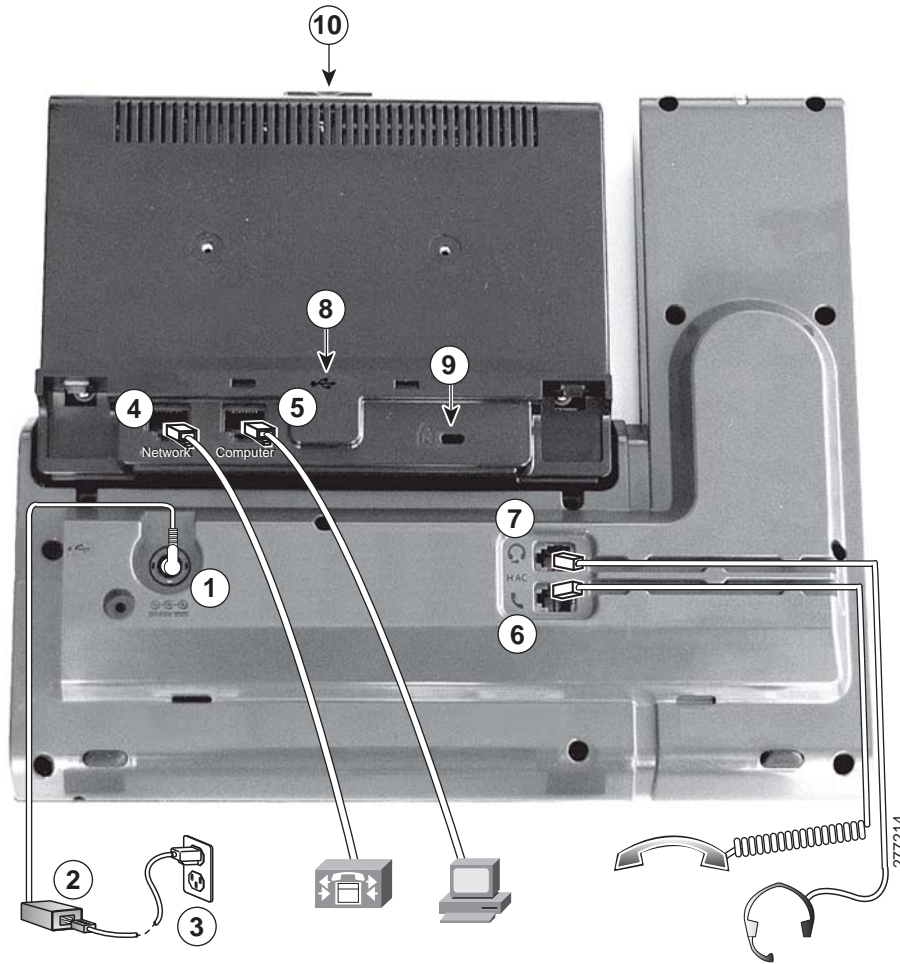
1	DC adaptor port (DC48V)	6	Handset Connection
2	AC-to-DC power supply (optional)	7	Analog Headset Connection (optional)
3	AC power wall plug (optional)	8	USB Port
4	Network port (10/100/1000 SW) with IEEE 802.3af power enabled	9	Anti-theft Security lock connector (lock optional)
5	Computer port (10/100/1000 PC) Connection	10	Camera pin holes (for Cisco Unified Video Camera)

Figure 3-5   *Cisco Unified IP Phone 9951 Cable Connections (Side)*

1	Side USB port	**3**	General purpose output port (speakers)
2	Accessory connector (such as for the Cisco Unified IP Color Key Expansion Module)	**4**	General purpose input port (microphone)

Figure 3-6   *Cisco Unified IP Phone 9971 Cable Connections (Back)*
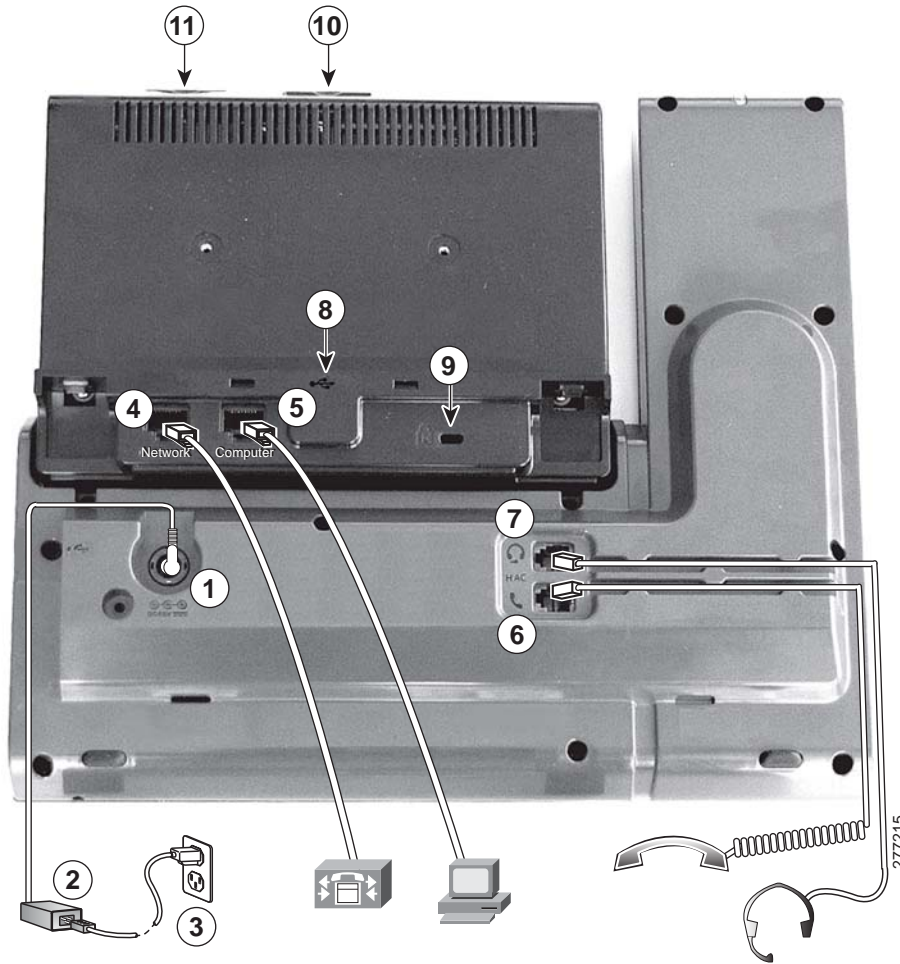
1	DC adaptor port (DC48V)	7	Analog Headset Connection (optional)
2	AC-to-DC power supply (optional)	8	USB Port
3	AC power wall plug (optional)	9	Anti-theft Security lock connector (lock optional)
4	Network port (10/100/1000 SW) with IEEE 802.3af and IEEE 802.3at power enabled	10	Camera pin holes (for Cisco Unified Video Camera)
5	Computer port (10/100/1000 PC) Connection	11	SDIO slot (not used for this release)
6	Handset Connection		

Figure 3-7   *Cisco Unified IP Phone 9971 Cable Connections (Side)*

1	Side USB port	**3**	General purpose output port (speakers)
2	Accessory connector (such as for the Cisco Unified IP Color Key Expansion Module)	**4**	General purpose input port (microphone)

Related Topics

- Connecting the Footstand, page 3-19
- Verifying the Phone Startup Process, page 3-21
- Configuring Startup Network Settings, page 3-21

Connecting the Footstand

If your phone is placed on a table or desk, connect the footstand to the back of the phone.

Figure 3-8 illustrates the footstand on the Cisco Unified IP Phone 8961, 9951, and 9971. To attach the footstand to the phone, align the tabs to the appropriate set of holes on the phone and snap into place.

Figure 3-8   *Cisco Unified IP Phone 8961, 9951, and 9971*

1	Insert the curved connectors into the lower slots.	2	Lift the footstand until the connectors snap into the upper slots.
			Note Connecting and disconnecting the footstand requires a little extra force than you might expect.

Phone Display Viewing Angle

The phone display viewing angle can be adjusted according to your preference. Hold the handset and cradle with your left hand, hold the right side of the bezel (to the right of the display) with your right hand, then move your hands back and forth in opposite directions to adjust the angle.

Securing the Phone with a Cable Lock

You can secure the Cisco Unified IP Phone 8961, 9951, and 9971 to a desktop by using a laptop cable lock. The lock connects to the anti-theft security connector on the back of the phone, and the cable can be secured to a desktop.

The security slot can accommodate a lock up to 20 mm. Compatible laptop cable locks include the Kensington laptop cable lock and laptop cable locks from other manufacturers that can fit into the security slot on the back of the phone.

Mounting the Phone to the Wall

You can mount the Cisco Unified IP Phone on the wall by using special brackets available in a Cisco Unified IP Phone wall mount kit. (Wall mount kits must be ordered separately from the phone.) For detailed information, see Appendix E, "Installing the Wall Mount for the Cisco Unified IP Phone" or Appendix F, "Cisco Unified IP Phone Non-Lockable Wall Mount."

Verifying the Phone Startup Process

After the Cisco Unified IP Phone has power connected to it, the phone begins its startup diagnostic process. by cycling through the following steps.

1. The buttons on the Feature and Session buttons flash amber and then green in sequence during the various stages of bootup as the phone checks its hardware.

2. The main screen displays a "Registering to Cisco Unified Communications Manager" message.

If the phone successfully passes through these stages, it has started up properly and the Select button stays lit until it is selected. If the phone does not start up properly, see the "Resolving Startup Problems" section on page 12-1.

Configuring Startup Network Settings

If you are not using DHCP in your network, you must configure these network settings on the Cisco Unified IP Phone after installing the phone on the network:

- IP address

- IP subnet information

- TFTP server IP address

- You also may configure the domain name and the DNS server settings, if necessary.

Collect this information and see the instructions in Chapter 7, "Configuring Settings on the Cisco Unified IP Phone."

Configuring Security on the Cisco Unified IP Phone

The security features protect against several threats, including threats to the identity of the phone and to data. These features establish and maintain authenticated communication streams between the phone and the Cisco Unified Communications Manager server, and ensure that the phone uses only digitally signed files.

Cisco Unified Communications Manager (beginning with Release 8.5(1)) includes Security by Default, which provides the following security features for Cisco Unified IP phones without running the CTL client:

- Signing of the phone configuration files.

- Phone configuration file encryption.

- https with Tomcat and other Web services.

Note   Secure signaling and media features still require you to run the CTL client and use hardware eTokens.

For more information about the security features, see the "Understanding Security Features for Cisco Unified IP Phones" section on page 1-15. Also, refer to the *Cisco Unified Communications Manager Security Guide*.

A Locally Significant Certificate (LSC) installs on phones after you perform the necessary tasks that are associated with the Certificate Authority Proxy Function (CAPF). You can use Cisco Unified Communications Manager Administration to configure an LSC, as described in the *Cisco Unified Communications Manager Security Guide*.

Alternatively, you can initiate the installation of an LSC from the Security Setup menu on the phone. This menu also lets you update or remove an LSC.

Before You Begin

Make sure that the appropriate Cisco Unified Communications Manager and the Certificate Authority Proxy Function (CAPF) security configurations are complete:

- The CTL or ITL file should have a CAPF certificate.
- On Cisco Unified Communications Operating System Administration, verify that the CAPF certificate has been installed
- The CAPF is running and configured.

Refer to the *Cisco Unified Communications Manager Security Guide* for more information.

To configure an LSC on the phone, perform these steps:

Procedure

Step 1   Obtain the CAPF authentication code that was set when the CAPF was configured.

Step 2   From the phone, press **Applications** and choose **Administrator Settings > Security Setup**.

> **Note**   You can control access to the Settings Menu by using the Settings Access field in the Cisco Unified Communications Manager Administration Phone Configuration window. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

Step 3   Choose LSC and press the **Select** button or **Update** softkey.

The phone prompts for an authentication string.

Step 4   Enter the authentication code and press the **Submit** softkey.

The phone begins to install, update, or remove the LSC, depending on how the CAPF was configured. During the procedure, a series of messages appears in the LSC option field in the Security Configuration menu, so you can monitor progress. When the procedure completes successfully, the phone will display Installed or Not Installed.

The LSC install, update, or removal process can take a long time to complete. You can stop the process at any time by pressing the **Stop** softkey from the Security Setup menu.

When the phone successfully completes the installation procedure, it displays "Installed." If the phone displays, "Not Installed," the authorization string may be incorrect or the phone may not enabled for upgrading. If the CAPF operation was to delete the LSC, the phone will display "Not Installed" to indicate that the operation was successful. Refer to error messages generated on the CAPF server and take appropriate actions.

C H A P T E R 4

Setting Up the Cisco Unified IP Color Key Expansion Module

The Cisco Unified IP Color Key Expansion Module (KEM) attaches to your Cisco Unified IP Phone 8961, Cisco Unified IP Phone 9951, and Cisco Unified IP Phone 9971 to add additional line appearances, speed dials, or programmable buttons to your phone.

You can add one Key Expansion Module (KEM) to the Cisco Unified IP Phone 8961 to add up to 36 extra lines or buttons, two Expansion Modules to the Cisco Unified Phone 9951 to add up to 72 extra lines or buttons, and three Expansion Modules to the Cisco Unified IP Phone 9971 to add up to 108 extra lines or buttons.

The programmable buttons can be set up as phone line buttons, speed-dial buttons, or phone feature buttons.

Most call functions, such as answering a call, placing a call on hold, and transferring a call, can be performed with the Cisco Unified IP Color Key Expansion Module.

Table 4-1 lists the Cisco Unified IP Phones and the number of Key Expansion Modules supported by each model.

Note For information on installing a wall mount kit for a phone that includes a Cisco Unified IP Color Key Expansion Module, see the "Installing a Wall Mount for a Phone with a Key Expansion Module" section on page E-8.

Table 4-1   Cisco Unified IP Phones and Supported KEMs

Cisco Unified IP Phone Model	KEMs Supported
9971	3 KEMs with 108 lines or buttons
9951	2 KEMs with 72 lines or buttons
8961	1 KEM with 36 lines or buttons

This chapter includes the following topics:

- Installing a Key Expansion Module on the Cisco Unified IP Phone, page 4-2
- Configuring the Key Expansion Module in Cisco Unified Communications Manager Administration, page 4-4
- Key Expansion Module Settings on the Phone, page 4-5
- Upgrading the Key Expansion Module, page 4-5

Installing a Key Expansion Module on the Cisco Unified IP Phone

This section contains the following topics:

Power Information

The Cisco Unified IP Color Key Expansion Module for the Cisco Unified IP Phone 8961, 9951, and 9971 have the following power consumption and power scheme.

Power Consumption

48V DC, 5W per KEM

Power Scheme

- At least one KEM can be powered up if the Cisco Unified IP Phone 8961, 9951, and 9971 uses AT PoE.
- If the phone uses a power adapter, three KEMs can be powered up for the Cisco Unified IP Phone 9971, two KEMs can be powered up for the Cisco Unified IP Phone 9951, and one KEM can be powered up for the Cisco Unified IP Phone 8961.
- A KEM cannot be powered up if the Cisco Unified IP Phone 8961, 9951, and 9971 uses AF PoE.
- With AT power, the Cisco Unified IP Phones 9951 and 9971 can support two KEMs plus a USB headset or another USB device that is independently powered and only uses USB for signaling.
- The Cisco Unified IP Phone 9971 needs a power cube to support three KEMs.
- With AF power, the Cisco Unified IP Phones 9951 and 9971 need power cubes for any KEMS. The Cisco Unified IP Phone 8961 can support one KEM with CDP, AF power, and no power cube.

Connecting a Single KEM to the Cisco Unified IP Phone

To connect a single KEM to the Cisco Unified IP Phone, follow these steps:

Procedure

Step 1   Position the phone so that the front of the phone is facing up.

Step 2   Connect one end of the KEM spine connector to the Accessory Connector on the Cisco Unified IP Phone.

Step 3   Connect the other end of the KEM spine connector to the KEM as shown in Figure 4-1.

Figure 4-1   Connecting the KEM Spine Connector to the Cisco Unified IP Phone and KEM
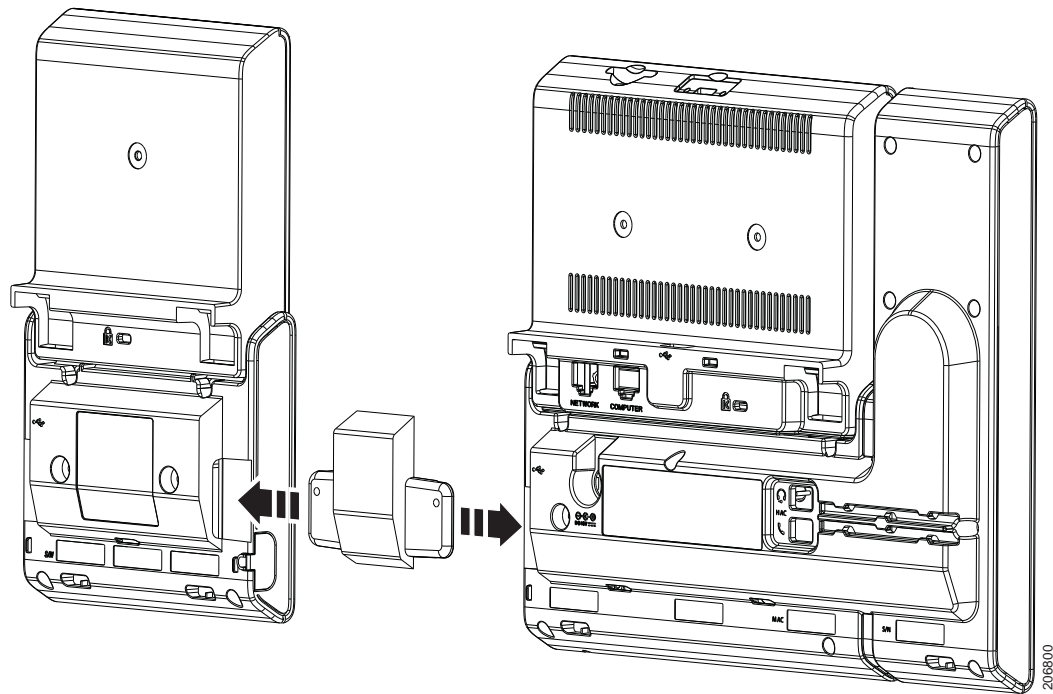
Step 4 Fasten the screws on the spine connector after connecting both the ends.

Note You can use a coin or screwdriver to fasten the screws. Make sure that the sides of the screw heads are fully inserted into the spine connector cavity and tightened.

Connecting Two or More KEMs to the Phone Using the KEM Spine Connector

To connect two or more KEMs to the Cisco Unified IP Phone, follow these steps:

Procedure

Step 1 Position the phone so that the front of the phone is facing up.

Step 2 Connect one end of the KEM spine connector to the Accessory Connector on the Cisco Unified IP Phone and the other end of the spine connector to a KEM, as shown in the (Figure 4-1 on page 4-3). The first KEM is now connected to the Cisco Unified IP Phone.

Step 3 Using a second KEM spine connector, connect the second KEM to the first KEM.

Step 4 (Optional) Using a third KEM spine connector, connect the third KEM to the second (middle) KEM. Figure 4-2 shows a Cisco Unified IP Phone with three KEMs attached.

Step 5 Fasten the screws on the spine connectors after connecting both the ends.

Figure 4-2   *Cisco Unified IP Phone with Three KEMs Attached*

Note   Cisco offers two other methods of connecting KEMs to your phone in case you either have a shortage of desk space that prevents you from using the spine connectors as shown in Figure 4-2, or in case you need access to the speaker and microphone ports (on the Cisco Unified IP Phone 9951 and 9971) that the KEM spine connector covers up.

Configuring the Key Expansion Module in Cisco Unified Communications Manager Administration

To configure the Cisco Unified IP Color Key Expansion Module on the Cisco Unified IP Phone, perform the following:

Procedure

Step 1   In Cisco Unified Communications Manager Administration, choose **Device > Phone.**

The Find and List Phones page appears. You can search for one or more phones that you want to configure for the Cisco Unified IP Color Key Expansion Module.

Step 2   Select and enter your search criteria and click **Find.**

The Find and List Phones window appears with a list of phones that match your search criteria.

Step 3   Click the IP Phone that you want to configure for the Cisco Unified IP Color Key Expansion Module. The Phone Configuration window appears.

Scroll down to the Expansion Module Information section on the right pane of the Phone Configuration window, and choose the appropriate expansion module (or "none) for the Module 1, Module 2 and Module 3 fields, in this order.

For the Module Load Name, enter the custom software for the appropriate expansion module, if applicable. The value that you enter overrides the default value for the current model. Ensure the firmware load matches the module load. If the Module Load Name is left blank, the default load (the load bundled with the phone load) is installed.

For the number of supported KEMs per phone model, refer to Table 4-1 on page 4-1.

Step 4   Make sure the Side USB Port parameter is enabled.

> **Note**   If the Side USB Port is disabled, the KEM will not work.

Step 5   Be sure to select the phone button template (in the Device Information portion of the Phone Configuration window) that has been configured to make full use of the KEM(s) attached to the phone.

Step 6   Click **Save**.

Key Expansion Module Settings on the Phone

Once you have installed one or more KEMs on the phone and have configured them in Cisco Unified Communications Manager Administration, the KEMs are automatically recognized by the Cisco Unified IP Phone 8961, 9951, and 9971.

On the phone, press the **Applications** button ⚙ and then press **Accessories**. All KEMs that have been properly installed and configured should appear in the list of accessories.

When multiple KEMs are attached, they will be numbered according to the order in which they are connected with respect to the phone. For example (refer to Figure 4-2):

- Key Expansion Module 1 is the KEM closest to the phone.
- Key Expansion Module 2 is the KEM in the middle.
- Key Expansion Module 3 is the KEM farthest to the right.

You can select a KEM, and then choose one of the following softkeys:

- Exit—Returns to the Applications menu.
- Details—Provides details about the selected KEM.
- Setup—Allows you to configure the brightness of the selected KEM. This can also be done by means of the Preferences menu. For details, refer to the *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager*, "Accessories" chapter, "Adjust the Brightness on the Cisco Unified IP Color Key Expansion Module" section.

Upgrading the Key Expansion Module

To automatically upgrade KEMs to the latest load, follow these steps:

Procedure

Step 1   Power on the KEM, press **Page 1**, and do not release. When the LCD turns white, continue pressing **Page 1** for at least one second.

Step 2   Release **Page 1**; LEDs should turn red. Immediately press **Page 2** and continue pressing **Page 2** for at least one second.

Step 3   Release **Page 2**; all LEDs should turn amber.

Step 4   Press Lines **5**, **14**, **1**, **18**, **10**, and **9** in sequence.

The LCD should turn blue, and the spinning loader is displayed in the center.

The KEM starts to upgrade.

Removing a Key Expansion Module

If you need to remove all existing KEMs from the phone, detach them from the phone, then go to Cisco Unified Communications Manager administration and update the phone configuration file accordingly.

If you are removing one or more KEMs but still leaving one or more KEMs attached to the phone, refer to the for instructions on how the KEMs and phone should be connected based on how many KEMs will remain. Also, go to Cisco Unified Communications Manager Administration and update the phone configuration file accordingly.

Troubleshooting

To obtain KEM troubleshooting information, follow these steps:

Procedure

Step 1   Open a command line interface.

Step 2   Enter the following command to enter debug mode:

`debugsh`

Step 3   Enter **?** to see all available commands and options.

Step 4   Use the applicable commands and options to find the KEM information desired.

To exit debug mode, either perform a Ctrl-C.

Setting Up the Cisco Unified Video Camera

The Cisco Unified IP Phone 9951 and 9971 supports the add-on accessory Cisco Unified Video Camera.

The Cisco Unified Video Camera connects to your Cisco Unified IP Phone and allows you to make a point-to-point video call with another Cisco Unified IP Phone with a Cisco Unified Video Camera attached. If a phone does not have a Cisco Unified Video Camera attached, it can only receive one-way video.

This chapter contains the following information:

- Configuring the Cisco Unified Video Camera, page 5-1
- Attaching the Cisco Unified Video Camera, page 5-2
- Adjusting the Camera Settings, page 5-2
- Post-Installation Steps, page 5-4
- Using the Cisco Unified Video Camera, page 5-4

Configuring the Cisco Unified Video Camera

To configure the Cisco Unified Video Camera, you must perform the following configuration steps in Cisco Unified Communications Manager administration:

Note The parameters described in the following procedure can be enabled on either the Phone Configuration window (**Device > Phone**), the Enterprise Phone Configuration window (**System > Enterprise Phone Configuration**), or the Common Phone Profile window (**Device > Device Settings > Common Phone Profile**). Be sure to also check the corresponding Override Common Settings parameter in the configuration window. The Phone Configuration window is referenced below for purposes of the procedure description.

For more information about parameters that can be configured in any of these three configuration windows, see the "Configuring Product Specific Configuration Parameters" section on page 8-26.

Procedure

Step 1 In the phone configuration window (**Device > Phone**) of the phone to which you are adding the Cisco Unified Video Camera, enable the Cisco Camera parameter. This field is located in the Product Specific Configuration layout portion of the window.

Step 2   On the same window, enable the Video Capabilities parameter.

Step 3   Click **Save**.

Attaching the Cisco Unified Video Camera

To install the Cisco Unified Video Camera, you can either:

- Attach the camera to your phone.
- Attach the camera to your computer monitor (or to another object in your work area).

The USB port connector on the bottom of the Cisco Unified Video Camera attaches to the back port (not the side port) on the Cisco Unified IP Phone 9951 or 9971. As you attach the USB connector to the back port on the phone, the camera should slide easily into the camera pin holes on the phone.

Figure 3-4 on page 3-15 shows the location of the back USB port and the camera pin holes for the Cisco Unified IP Phone 9951. Figure 3-6 on page 3-17 shows the location of the back USB port and the camera pin holes for the Cisco Unified IP Phone 9971.

Installation Procedure

For the complete installation procedure, see the *Cisco Unified Video Camera Quick Start Guide* at this location:

http://www.cisco.com/en/US/products/ps10655/products_user_guide_list.html

Adjusting the Camera Settings

Once you have attached the camera on your phone, you can control the features of the camera.

This section provides information on the features you can control from the phone:

- Adjusting the Camera View Area, page 5-2
- Adjusting the Brightness Setting, page 5-3
- Adjusting Auto Transmit Setting, page 5-3

Adjusting the Camera View Area

The View Area feature acts as a wide angle and zoom function for your camera and allows you to adjust the view area that is shared during video streaming. The View Area feature acts as a wide angle and zoom function for your camera.

To adjust the camera view area, follow these steps:

Procedure

Step 1   On the Cisco Unified IP Phone, press the **Applications** button ⚙.

Step 2   Select **Accessories**.

Step 3   Highlight **Cisco Unified Camera**.

Step 4   Press the **Set-up** softkey.

Step 5   Select **View Area**.

Step 6   Use the arrows on the Navigation pad to increase or decrease the view area.

Step 7   Press the **Save** softkey.

Adjusting the Brightness Setting

The Brightness setting affects the video that you transmit to others. However, it does not affect the video that you receive from other parties. You can adjust the brightness setting to improve the quality of the video during streaming.

Note   As the field of view can affect brightness, adjust the View Area feature for your camera before adjusting the Brightness setting.

To adjust the Brightness setting, follow these steps:

Procedure

Step 1   On the Cisco Unified IP Phone, press the **Applications** button .

Step 2   Select **Accessories**.

Step 3   Highlight **Cisco Unified Camera**.

Step 4   Press the **Set-up** softkey.

Step 5   Select **Brightness**.

Step 6   Use the arrows on the Navigation pad to increase or decrease brightness.

Step 7   Press the **Save** softkey.

Adjusting Auto Transmit Setting

The Auto Transmit feature allows you to control the streaming of videos for both inound and outbound calls.

When Auto Transmit is on (default setting), the camera streams video automatically during calls.

When Auto Transmit is off, video for each call is automatically muted (however, your phone still receives video). To resume video transmission in this case, press the Unmute Video softkey   .

To turn the Auto Transmit setting on or off, follow these steps:

Procedure

Step 1   On the Cisco Unified IP Phone, press the **Applications** button .

Step 2   Select **Accessories**.

Step 3   Highlight **Cisco Unified Camera**.

Step 4   Press the **Set-up** softkey.

Step 5   Press the **Turn On** or **Turn Off** softkey.

Post-Installation Steps

After installing the Cisco Unified Video Camera, perform the following checks:

1. Wait till the "camera ready" message appears.

    Note   The camera may need to upgrade after installation. This may take a few minutes before the camera is operational.

2. Press the **Video Preview** softkey to check the picture quality.

    –   If the video preview image looks too blue, try increasing the camera Brightness setting.

    –   If the background looks washed out, try decreasing the camera Brightness setting.

    Note   For information about adjusting camera settings on the phone, see the *Cisco Unified Video Camera Quick Start Guide* at this location:
    http://www.cisco.com/en/US/products/ps10655/products_user_guide_list.html

3. Move the phone/camera to a position where there are no bright lights in the field of view.

4. Move the phone/camera so that the user is illuminated by light coming from the front.

Using the Cisco Unified Video Camera

For information about placing and receiving video calls, setting up video conferences, and adjusting camera settings on the phone, see the *Cisco Unified Video Camera Quick Start Guide* at this location:

http://www.cisco.com/en/US/products/ps10655/products_user_guide_list.html

C H A P T E R 6

Understanding the VoIP Wireless Network

This chapter provides an overview of the interaction between a wireless-capable Cisco Unified IP Phone 9971 and other key components of a VoIP network in a wireless local area network (WLAN) environment. This chapter contains the following sections:

- Understanding the Wireless LAN, page 6-1
- Understanding WLAN Standards and Technologies, page 6-2
- Bluetooth Wireless Technology, page 6-7
- Components of the VoIP Wireless Network, page 6-8
- Security for Voice Communications in WLANs, page 6-11
- VoIP WLAN Configuration, page 6-15
- Configuring Wireless LAN, page 6-16

Note For instructions on deploying and configuring a wireless Cisco Unified IP Phone 9971, refer to the *Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide* at this location:

http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/9971_9951_8961/7_1_3/english/deployment/guide/9971dply.pdf

Understanding the Wireless LAN

With the introduction of wireless communication, Cisco Unified IP Phones with wireless capability, such as the Cisco Unified IP Phone 9971, can provide voice communication within the corporate WLAN. The Cisco Unified IP Phone depends upon and interacts with wireless access points (APs) and key Cisco IP telephony components, including Cisco Unified Communications Manager Administration, to provide wireless voice communication. Cisco Access Points can run in standalone or unified mode. Unified mode requires the Cisco Unified Wireless LAN Controller.

The Cisco Unified IP Phone 9971 exhibits Wi-fi capabilities which can be used 802.11a, 802.11b and 802.11g Wi-Fi.

Figure 6-1 shows a typical WLAN topology that enables the wireless transmission of voice for wireless IP telephony.

Figure 6-1   WLAN with Wireless IP Phones
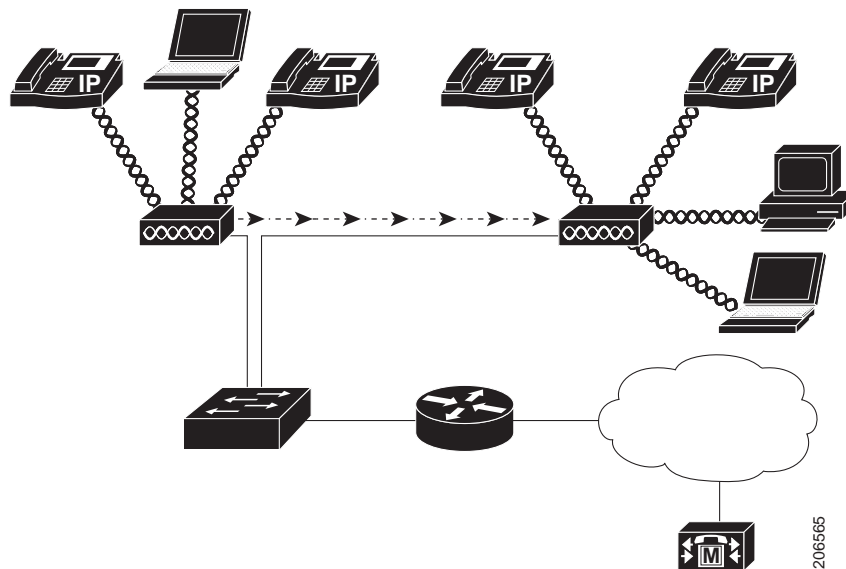
When a Cisco Unified IP Phone powers on, it searches for and becomes associated with an AP if the phone Wireless access is set to On.

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

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

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

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

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

Understanding WLAN Standards and Technologies

This section describes the following concepts:

802.11 Standards for WLAN Communications

Wireless LANs must follow the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards that define the protocols that govern all Ethernet-based wireless traffic. The Cisco Unified IP Phone supports 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 transmitting and receiving 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 which channels and powers to use. The Cisco Unified IP Phone 9971 requires world mode (802.11d) to determine which channels are legally allowed for any given country. For supported channels, see Table 6-1. Make sure that 802.11d is properly configured on the Cisco IOS Access Points or Cisco Unified Wireless LAN Controller; for more information, see the "World Mode (802.11d)" section on page 6-4.

- 802.11e—QoS

- 802.11g—Uses the same unlicensed 2.4 Ghz band as 802.11b, but extends the data rates to provide greater performance by using Orthogonal Frequency Division Multiplexing (OFDM) technology. OFDM is a physical-layer encoding technology for transmitting signals by using RF.

- 802.11h—5 GHz spectrum and transmit power management

- 802.11i—Security

Table 6-1   Supported Channels for the Cisco Unified IP Phone 9971

Part Number	Band Range	Available Channels	5 GHz Channel Set
CP-9971-K9	2.412 – 2.484 GHz	13 (14 in Japan)	
	5.180 – 5.240 GHz	4	UNII-2
	5.260 – 5.320 GHz	4	UNII-2
	5. 500 – 5.700 GHz	11	UNII-2 Extended
	5.745 – 5.805 GHz	4	UNII-3

Note   802.11j (channels 34, 38, 42, 46) and channel 165 are not supported.

World Mode (802.11d)

If you are using the Cisco Unified IP Phone 9971 in the World Mode, you must enable World mode (802.11d). The Cisco Unified IP Phone 9971 uses 802.11d to determine which channels and transmit powers to use and inherits its client configuration from the associated access point.

Note Enabling World Mode (802.11d) may not be necessary if the frequency is 2.4GHz and the current access point is transmitting on a channel 1-11.

As all countries support these frequencies, you can attempt to scan these channels regardless of supporting World Mode (802.11d). For the countries which support 2.4GHz, refer to Cisco Unified IP Phone 9971 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.

World Mode must be enabled manually for Cisco Autonomous Access Points using the following commands:

```
Interface dot11radio X
world-mode dot11d country US both
```

Supported Countries

The following countries are supported by the Cisco Unified IP Phone 9971:

Argentina (AR)	India (IN)	Poland (PL)
Australia (AU)	Indonesia (ID)	Portugal (PT)
Austria (AT)	Ireland (IE)	Puerto Rico (PR)
Belgium (BE)	Israel (IL)	Romania (RO)
Brazil (BR)	Italy (IT)	Russian Federation (RU)
Bulgaria (BG)	Japan (JP)	Saudi Arabia (SA)
Canada (CA)	Korea (KR / KP)	Singapore (SG)
Chile (CL)	Latvia (LV)	Slovakia (SK)
Colombia (CO)	Liechtenstein (LI)	Slovenia (SI)
Costa Rica (CR)	Lithuania (LT)	South Africa (ZA)
Cyprus (CY)	Luxembourg (LU)	Spain (ES)
Czech Republic (CZ)	Malaysia (MY)	Sweden (SE)
Denmark (DK)	Malta (MT)	Switzerland (CH)
Estonia (EE)	Mexico (MX)	Taiwan (TW)
Finland (FI)	Monaco (MC)	Thailand (TH)
France (FR)	Netherlands (NL)	Turkey (TR)
Germany (DE)	New Zealand (NZ)	Ukraine (UA)
Gibraltar (GI)	Norway (NO)	United Arab Emirates (AE)
Greece (GR)	Oman (OM)	United Kingdom (GB)
Hong Kong (HK)	Panama (PA)	United States (US)

Hungary (HU)	Peru (PE)	Venezuela (VE)
Iceland (IS)	Philippines (PH)	Vietnam (VN)

Radio Frequency Ranges

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

- 2.4 GHz—Many devices that utilize 2.4 GHz can potentially interfere with the 802.11b/g connection. An interferer can produce a Denial of Service (DoS) scenario, possibly preventing successful 802.11 transmissions.

- 5 GHz—Divided into several sections called Unlicensed National Information Infrastructure (UNII) bands and has four channels each. The channels are spaced at 20 MHz to provide non-overlapping channels and more channels than with 2.4 GHz.

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

Table 6-2 lists the Tx power capacities, data rates, ranges in feet and meters, and decibels tolerated by the receiver by 801.11 standard.

Table 6-2   Tx Power, Data Rates, Ranges, and Decibels by Standard

Standard	Maximum Tx Power[1]	Data Rate[2]	Range	Receiver Sensitivity
802.11a				
	16 dBm	6 Mbps	604 ft (184 m)	-91 dBm
		9 Mbps	604 ft (184 m)	-90 dBm
		12 Mbps	551 ft (168 m)	-88 dBm
		18 Mbps	545 ft (166 m)	-86 dBm
		24 Mbps	512 ft (156 m)	-82 dBm
		36 Mbps	420 ft (128 m)	-80 dBm
		48 Mbps	322 ft (98 m)	-77 dBm
		54 Mbps	289 ft (88 m)	-75 dBm
802.11g				
	16 dBm	6 Mbps	709 ft (216 m)	-91 dBm
		9 Mbps	650 ft (198 m)	-90 dBm
		12 Mbps	623 ft (190 m)	-87 dBm
		18 Mbps	623 ft (190 m)	-86 dBm
		24 Mbps	623 ft (190 m)	-82 dBm
		36 Mbps	495 ft (151 m)	-80 dBm
		48 Mbps	413 ft (126 m)	-77 dBm
		54 Mbps	394 ft (120 m)	-76 dBm

Table 6-2   Tx Power, Data Rates, Ranges, and Decibels by Standard (continued)

Standard	Maximum Tx Power[1]	Data Rate[2]	Range	Receiver Sensitivity
802.11b				
	17 dBm	1 Mbps	1,010 ft (308 m)	-96 dBm
		2 Mbps	951 ft (290 m)	-85 dBm
		5.5 Mbps	919 ft (280 m)	-90 dBm
		11 Mbps	902 ft (275 m)	-87 dBm

1. Adjusts dynamically when associating with an AP if the AP client setting is enabled.

2. Advertised rates by the APs are used. If the Restricted Data Rates functionality is enabled in the Cisco Unified Communications Manager Administration phone configuration, then the Traffic Stream Rate Set IE (CCX V4) is used.

For more information about supported data rates, tx power and rx sensitivity for WLANs, see Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide.

Wireless Modulation Technologies

Wireless communications uses the following modulation technologies for signaling:

- Direct-Sequence Spread Spectrum (DSSS)—Prevents interference by spreading the signal over the frequency range or bandwidth. DSSS technology multiplexes chunks of data over several frequencies so that multiple devices can communicate without interference. Each device has a special code that identifies its data packets and all others are ignored. Cisco wireless 802.11b/g products use DSSS technology to support multiple devices on the WLAN.

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

Table 6-3 provides a comparison of data rates, number of channels, and modulation technologies by standard.

Table 6-3   Data Rates, Number of Channels, and Modulation Technologies by IEEE Standard

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

AP, Channel, and Domain Relationships

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 non-overlapping channels for each AP. The recommended channels for 802.11b and 802.11g in North America are 1, 6, and 11.

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

For more information about APs, see the "VoIP WLAN Configuration" section on page 6-15.

For more information about AP, channel and domain relationships, see Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide.

WLANs and Roaming

The Cisco Unified IP Phone 9971 supports Cisco Centralized Key Management (CCKM), a centralized key management protocol, and provides a cache of session credentials on the wireless domain server (WDS). APs must register to the WDS for fast roaming to work. CCKM is also supported on the Cisco Unified Wireless LAN Controller alone.

The Cisco Unified IP Phone 9971 supports CCKM with 802.1x+WEP or WPA(TKIP) only. CCKM is not supported with WPA2 or WPA(AES). For details about CCKM, refer to the "Cisco Fast Secure Roaming Application Note" at:

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

Related Topics

- Voice QoS in a Wireless Network, page 6-9
- VoIP WLAN Configuration, page 6-15

Bluetooth Wireless Technology

Bluetooth enables low bandwidth wireless connections within a range of 30 feet (10 meters). The best performance is in the 3-to 6-foot (1- to 2-meter) range. Bluetooth wireless technology operates in the 2.4 GHz band which is the same as the 802.11b/g band. There can be a potential interference issues. It is recommended that you:

- Use 802.11a that operates in the 5 GHz band.
- Reduce the proximity of other 802.11b/g devices, Bluetooth devices, microwave ovens, and large metal objects.

For more information about using Bluetooth headsets with your Cisco Unified IP Phone, see the "Using Bluetooth Wireless Headsets" section on page 3-8.

Components of the VoIP Wireless Network

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

Interacting with Cisco Unified Wireless APs

Cisco Unified IP Phones use the same APs as wireless data devices. However, voice traffic over a WLAN requires different equipment configurations and layouts than a WLAN that is used exclusively for data traffic. Data transmission can tolerate a higher level of RF noise, packet loss, and channel contention than voice transmission. Packet loss during voice transmission can cause choppy or broken audio and make the phone call inaudible. Packet errors can also cause blocky or frozen video.

Because the Cisco Unified IP Phone 9971 are desktop and not mobile phones, changes in the local environment can cause phones 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 passage ways.

To ensure good voice quality and optimal RF signal coverage, you must perform a site survey. The site survey determines settings 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 post installation site surveys. When you add a group of new users, install more equipment, or stack large amounts of inventory, you are changing the wireless environment. A post installation survey verifies that the AP coverage is still adequate for optimal voice communications.

Note There are packet loss during roaming; however, the security mode and the presence of fast roaming depicts how much packet is lost during transmission.

For more information on Voice QoS in a wireless network, see Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide.

Associating to APs

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

- Received Signal Strength Indicator (RSSI)—Signal strength of available APs within the RF coverage area. The phone attempts to associate with the AP with the highest RSSI value.

- Traffic Specification (TSpec)—Calculation of call limits and WLAN load balancing. The TSpec value of each voice stream allows the system to allocate bandwidth to voice devices on a first-come, first-served basis. For more information, see "Voice QoS in a Wireless Network" section on page 6-9.

The Cisco Unified IP Phone associates with the AP with the highest RSSI and lowest channel usage values (QBSS) that have matching SSID and encryption types. To ensure that voice traffic is handled properly, you must configure the correct QoS in the AP.

Related Topics

- Security for Voice Communications in WLANs, page 6-11
- VoIP WLAN Configuration, page 6-15

Voice QoS in a Wireless Network

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

You need the following VLANs on the network switches and the APs that support voice connections on the WLAN:

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

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

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

Unlike wired networks with dedicated bandwidths, wireless LANs consider traffic direction when implementing QoS. Traffic is classified as upstream or downstream from the point of view of the AP as shown in Figure 6-2.

Figure 6-2   Voice Traffic in a Wireless Network
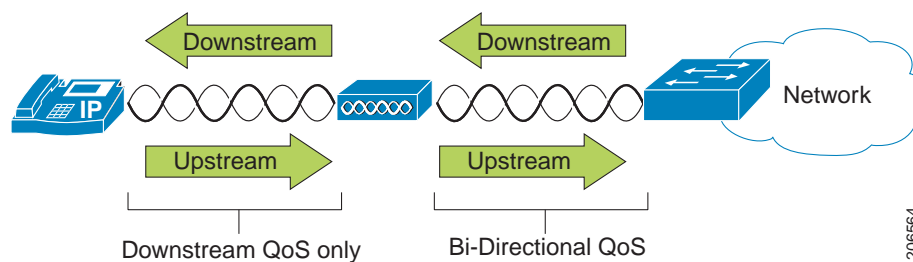
Beginning with Cisco IOS release 12.2(11)JA, Cisco Aironet APs support the contention-based channel access mechanism called Enhanced Distributed Coordination Function (EDCF). The EDCF-type of QoS has up to eight queues for downstream (toward the 802.11b/g clients) QoS. You can allocate the queues based on these options:

- QoS or Differentiated Services Code Point (DSCP) settings for the packets
- Layer 2 or Layer 3 access lists
- VLANs for specific traffic
- Dynamic registration of devices

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

Note   The Cisco Unified IP Phone marks the SCCP signaling packets with a DSCP value of 24 (CS3) and RTP packets with DSCP value of 46 (EF).

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

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

Implementing QoS in the connected Ethernet switch is highly desirable to maintain good voice quality. The COS and DSCP values that the Cisco Unified IP Phone sets do not need to be modified.

The DSCP, COS and UP (WMM) markings correctly for the optimum transmission of video frames.

Note   The Cisco Unified IP Phone 9971 does not support Video CAC; however, Voice CAC is supported for WLANs.

Related Topics

- Authentication Methods, page 6-11
- Interacting with Cisco Unified Communications Manager, page 6-11
- VoIP WLAN Configuration, page 6-15

Interacting with Cisco Unified Communications Manager

Cisco Unified Communications Manager is the call control component in the network that handles and routes calls for the wireless IP phones. Cisco Unified Communications Manager manages the components of the IP telephony system—the phones, access gateways, and the resources—for such features as call conferencing and route planning. When deploying a Cisco Unified IP Phone on a wireless LAN, you must use Cisco Unified Communications Manager Release 7.1(3) or later and the SIP protocol.

Before Cisco Unified Communications Manager can recognize a phone, the phone must register with Cisco Unified Communications Manager and be configured in the database. For information about setting up phones in Cisco Unified Communications Manager, see the "Configuring Cisco Unified IP Phones in Cisco Unified Communications Manager" section on page 1-24.

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

Related Topics

Security for Voice Communications in WLANs

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

This section contains the following items:

- Authentication Methods, page 6-11
- Authenticated Key Management, page 6-12
- Encryption Methods, page 6-13
- Choosing AP Authentication and Encryption Methods, page 6-13

Authentication Methods

The Cisco Wireless IP telephony solution provides wireless network security that prevents unauthorized logins and compromised communications by using the following authentication methods supported by the wireless Cisco Unified IP Phone 9971:

- Open Authentication—Any wireless device can request authentication in an open system. The AP that receives the request may grant authentication to any requestor or only to requestors on a list of users. Communication between the wireless device and AP could be non-encrypted or devices can use Wired Equivalent Privacy (WEP) keys to provide security. Devices that are using WEP only attempt to authenticate with an AP that is using WEP.

- Shared Key Authentication—The AP sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device that is requesting authentication uses a pre-configured WEP key to encrypt the challenge text and sends it back to the AP. If the challenge text is encrypted correctly, the AP allows the requesting device to authenticate. A device can authenticate only if its WEP key matches the WEP key on the APs.

  Shared key authentication can be less secure than open authentication with WEP because someone can monitor the challenges. An intruder can calculate the WEP key by comparing the unencrypted and encrypted challenge text strings.

- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) Authentication—This client server security architecture encrypts EAP transactions within a Transport Level Security (TLS) tunnel between the AP and the RADIUS server such as the Cisco Access Control Server (ACS).

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

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

- Light Extensible Authentication Protocol (LEAP)—Cisco proprietary password-based mutual authentication scheme between the client (phone) and a RADIUS server. Cisco Unified IP Phone can use LEAP for authentication with the wireless network.

- Auto (AKM)—Selects the 802.11 Authentication mechanism automatically from the configuration information exhibited by the AP. WPA-PSK or WPA.

Authenticated Key Management

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

- WPA/WPA2—Uses information on a RADIUS server 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 phone.

- Cisco Centralized Key Management (CCKM)—Uses information on a RADIUS server and a wireless domain server (WDS) to manage and authenticate keys. The WDS creates a cache of security credentials for CCKM-enabled client devices for fast and secure reauthentication.

With WPA/WPA2 and CCKM, encryption keys are not entered on the phone, but are automatically derived between the AP and phone. But the EAP username and password that are used for authentication must be entered on each phone.

Note CCKM is only supported with WPA(TKIP) and 802.1x(WEP).

Encryption Methods

To ensure that voice traffic is secure, the Cisco Unified IP Phone supports WEP, TKIP, and Advanced Encryption Standards (AES) for encryption. When using these mechanisms for encryption, both the signaling Skinny Client Control Protocol (SCCP) packets and voice Real-Time Transport Protocol (RTP) packets are encrypted between the AP and the Cisco Unified IP Phone.

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

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

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

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

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

Choosing AP Authentication and Encryption Methods

Authentication and encryption schemes are setup within the wireless LAN. VLANs are configured in the network and on the APs and specify different combinations of authentication and encryption. An SSID is associated with a VLAN and its particular authentication and encryption scheme. In order for wireless client devices to authenticate successfully, you must configure the same SSIDs with their authentication and encryption schemes on the APs and on the Cisco Unified IP Phone.

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

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

Note
- When using WPA Pre-shared key or WPA2 Pre-shared key, the pre-shared key must be statically set on the phone. These keys must match the keys configured on the AP.

- When using Auto (AKM), encryption options are automatically configured for WPA, WPA2, WPA Pre-shared key, WPA2 Pre-shared key, or CCKM.

- In AKM mode, the phone will authenticate with LEAP if it is configured with WPA, WPA2, or CCKM key management, or if 802.1x is used.

- The Cisco Unified IP Phone does not support auto EAP negotiation; to use EAP-FAST mode, you must specify it.

Table 6-4 provides a list of authentication and encryption schemes that are configured on the Cisco Aironet APs that the Cisco Unified IP Phone supports. The table shows the network configuration option for the phone that corresponds to the AP configuration.

Table 6-4   Authentication and Encryption Schemes

Cisco AP Configuration			Cisco Unified IP Phone Configuration
Authentication	Key Management	Common Encryption	Authentication
Open		None	Open
Open (Static WEP)		WEP	Open+WEP
Shared key (Static WEP)		WEP	Shared+WEP
LEAP 802.1x	Optional CCKM	WEP	LEAP or Auto (AKM)
LEAP WPA	WPA with Optional CCKM	TKIP	LEAP or Auto (AKM)
LEAP WPA2	WPA2	AES	LEAP or Auto (AKM)
EAP-FAST 802.1x	Optional CCKM	WEP	EAP-FAST
EAP-FAST with WPA	WPA Optional CCKM	TKIP	EAP-FAST
EAP-FAST with WPA2	WPA2	AES	EAP-FAST
WPA-PSK	WPA-PSK	TKIP	Auto (AKM)
WPA2-PSK	WAP2-PSK	AES	Auto (AKM)

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

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

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

Related Topics

- Interacting with Cisco Unified Wireless APs, page 6-8
- Authentication Methods, page 6-11
- Encryption Methods, page 6-13
- Interacting with Cisco Unified Communications Manager, page 6-11
- Components of the VoIP Wireless Network, page 6-8

VoIP WLAN Configuration

This section provides configuration guidelines for deploying Cisco Unified IP Phones in the WLAN and includes these topics:

Supported Access Points

The wireless Cisco Unified IP Phone 9971 is supported on both the Cisco autonomous and unified solutions. Minimum and recommended versions are:

- Cisco IOS Access Points (Autonomous)
  - Minimum = 12.3(8)JEA2 or later
  - Recommended = 12.4(10b)JA3 or later (does not apply to Cisco Aironet Series 1100, 1140, 1200, or 1230)
- Cisco Unified Wireless LAN Controller
  - Minimum = 5.1.163.0 or later
  - Recommended = 5.2.193.0 or later

Supported APs and Modes

Table 6-5 lists the modes that are supported by each Cisco Access Point.

Table 6-5   Supported APs and Modes

AP Models	802.11b	802.11g	802.11a	Autonomous Mode	Unified Mode
Cisco Aironet 500 Series	Yes	Yes	No	Yes	Yes
Cisco Aironet 1100 Series	Yes	Yes	No	Yes	Yes
Cisco Aironet 1130 AG Series	Yes	Yes	Yes	Yes	Yes
Cisco Aironet 1140 Series	Yes	Yes	Yes	Yes	Yes
Cisco Aironet 1200 Series	Yes	Yes	Optional	Yes	Yes
Cisco Aironet 1230 AG Series	Yes	Yes	Yes	Yes	Yes
Cisco Aironet 1240 AG Series	Yes	Yes	Yes	Yes	Yes
Cisco Aironet 1250 Series	Yes	Yes	Yes	Yes	Yes
Cisco Aironet 1300 Series	Yes	Yes	No	Yes	Yes

Note Voice over the Wireless LAN (VoWLAN) via Outdoor MESH technology (Cisco 1500 series) is not supported in the Cisco Unified IP Phone 9971.

Third-party access points are not supported since there is no interoperability testing with these access points. However, if the access point supports the key features and follows the standards, the Cisco Unified Wireless IP Phone will be compliant.

Wi-Fi compliant APs that are manufactured by third-party vendors will support the Cisco Unified Wireless IP Phone 9971, but might not support key features such as Wi-Fi MultiMedia (WMM), Unscheduled Auto Power Save Delivery (U-APSD), Traffic Specification (TSPEC), QoS Basic Service Set (QBSS), Dynamic Transmit Power Control (DTPC), or proxy ARP.

Supported Antennas

Some Cisco Access Points require or allow external antennas. Refer to the following URL for the list of supported antennas and how these external antennas should be mounted.

http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html

Note The Cisco Aironet Series 1130 and 1140 access points must be mounted on the ceiling because they have omni-directional antennas.

Configuring Wireless LAN

Ensure that the Wi-Fi coverage in the location where the wireless is deployed, is suitable for transmitting video and voice packets.

If the Wi-Fi connectivity for voice and video has been enabled for the Cisco Unified IP Phone 9971, you have to authenticate the Wi-Fi network using the WLAN Sign in application within your applications menu.

To enable, to go to **Applications > Administrator Settings > Network Setup > WLAN Setup > WLAN Sign in Access** and enable WLAN network.

To change the username/password must go to **Applications > Administrator Settings**.

For complete configuration information, see the *Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide*.

The *Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide* includes the following configuration information:

- Configuring the wireless network
- Configuring the wireless LAN in Cisco Unified Communications Manager administration
- Configuring the wireless LAN on the Cisco Unified IP Phone 9971

Summary of Configuring the Wireless LAN in Cisco Unified Communications Manager Administration

In Cisco Unified Communications Manager administration, you must enable a parameter called "Wi-Fi" for the wireless Cisco Unified IP Phone 9971. This can be done in one of the following locations in Cisco Unified Communications Manager administration:

- To enable wireless LAN on a specific phone, select the enable setting for the Wi-Fi parameter in the Product Specific Configuration Layout section (**Device > Phone**) for the specific phone, and check the Override Common Settings check box.

- To enable wireless LAN for a group of phones, select the enable setting for the Wi-Fi parameter on a Common Phone Profile Configuration window (**Device > Device Settings > Common Phone Profile**), check the Override Common Settings check box, then associate the phone (**Device > Phone** page) with that common phone profile.

- To enable wireless LAN for all WLAN-capable phones in your network, select the enable setting for the Wi-Fi parameter on the Enterprise Phone Configuration window (**System > Enterprise Phone Configuration**), and check the Override Common Settings check box.

Note On the Phone Configuration window in Cisco Unified Communications Manager administration (**Device > Phone**), when you configure the MAC address, use the wired-line MAC address. The wireless MAC address is not used for Cisco Unified Communications Manager registration.

Summary of Configuring the Wireless LAN on the Cisco Unified IP Phone

Before the phone can connect to the WLAN, you must configure the network profile for the phone with the appropriate WLAN settings. You can use the Network Setup menu on the phone to access the WLAN Setup submenu and set up the WLAN configuration. For instructions, see "WLAN Setup Menu" section on page 7-7.

Configuring Settings on the Cisco Unified IP Phone

The Cisco Unified IP Phone includes many configurable network settings that you may need to modify before the phone is functional for your users. You can access these settings, and change some of them, through menus on the phone. Settings that are display-only on the phone are configured in Cisco Unified Communications Manager Administration.

This chapter includes the following topics:

- Setup Menus on the Cisco Unified IP Phone, page 7-1
- Ethernet Setup Menu, page 7-4
- WLAN Setup Menu, page 7-7
- IPv4 Setup Menu Options, page 7-10
- Security Setup Menu, page 7-13

Setup Menus on the Cisco Unified IP Phone

The Cisco Unified IP Phone includes the following configuration menus:

- Network Setup—Provides options for viewing and configuring a variety of network settings. For more information, see the "Ethernet Setup Menu" section on page 7-4.

    - Ethernet Setup—A submenu of the Network Setup menu, the Ethernet Setup menu items provide configuration options to configure the Cisco Unified IP Phone over an ethernet network. For more information, see the "Ethernet Setup Menu" section on page 7-4.

    - WLAN Setup—A submenu of the Network Setup menu, the WLAN Setup menu items provide configuration options to configure the Cisco Unified IP Phone with the wireless local area network (WLAN). For more information, see the "WLAN Setup Menu" section on page 7-7.

    - IPv4 Setup—A submenu of the Ethernet Setup menu and of the WLAN Setup menu, the IPv4 menu items provide additional network options for viewing and setting. For more information, see the "IPv4 Setup Menu Options" section on page 7-10.

- Security Setup—Provides options for viewing and configuring a variety of security settings. For more information, see the "Security Setup Menu" section on page 7-13.

Before you can change option settings on the Network Setup menu, you must unlock options for editing. See the "Unlocking and Locking Options" section on page 7-3 for instructions.

For information about the keys you can use to edit or change option settings, see the "Editing Values" section on page 7-3.

You can control whether a phone user has access to phone settings by using the Settings Access field in the Cisco Unified Communications Manager Administration Phone Configuration window (in the Product Specific Information portion of the window).

Related Topics

- Displaying a Setup Menu, page 7-2
- Unlocking and Locking Options, page 7-3
- Editing Values, page 7-3
- Ethernet Setup Menu, page 7-4
- WLAN Setup Menu, page 7-7
- IPv4 Setup Menu Options, page 7-10
- Security Setup Menu, page 7-13

Displaying a Setup Menu

To display a configuration menu, perform the following steps.

Procedure

Step 1   Press the **Applications** button ⚙.

Step 2   Select **Administrator Settings**.

Step 3   Select **Network Setup** or **Security Setup**.

> **Note**   For information about the Status menu, see Chapter 10, "Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone." For information about the Reset Settings menu, see Chapter 12, "Troubleshooting and Maintenance."

Step 4   Enter your user ID and password, if required, then click **Sign-In**.

Step 5   Perform one of these actions to display the desired menu:

- Use the navigation arrows to select the desired menu and then press the **Select** button.
- Use the keypad on the phone to enter the number that corresponds to the menu.

Step 6   To display a submenu repeat Step 5.

Step 7   To exit a menu, press the **Exit** softkey or the back arrow softkey ↰ .

Related Topics

- Unlocking and Locking Options, page 7-3
- Editing Values, page 7-3
- Ethernet Setup Menu, page 7-4
- WLAN Setup Menu, page 7-7

- IPv4 Setup Menu Options, page 7-10
- Security Setup Menu, page 7-13

Unlocking and Locking Options

You can apply a password to the phone so that no changes can be made to the administrative options on the phone without the password being entered on the Administrator Settings phone screen.

To apply a password to the phone, in Cisco Unified Communications Manager administration, navigate to the Common Phone Profile Configuration window (**Device > Device Settings > Common Phone Profile**). Enter a password in the Local Phone Unlock Password option. Apply the password to the common phone profile that the phone uses.

Related Topics

- Displaying a Setup Menu, page 7-2
- Editing Values, page 7-3
- Ethernet Setup Menu, page 7-4
- WLAN Setup Menu, page 7-7
- IPv4 Setup Menu Options, page 7-10

Editing Values

When you edit the value of an option setting, follow these guidelines:

- Use the arrows on the navigation pad to highlight the field you wish to edit, then press the **Select** button of the navigation pad to activate that field. (You can also double-tap on an editable field to activate it for editing.) Once the field is activated, you can enter values.
- Use the keys on the keypad to enter numbers and letters.
- To enter letters by using the keypad, use a corresponding number key. Press the key one or more times to display a particular letter. For example, press the **2** key once for "a," twice quickly for "b," and three times quickly for "c." After you pause, the cursor automatically advances to allow you to enter the next letter.
- Press the arrow softkey ↰ if you make a mistake. This softkey deletes the character to the left of the cursor.
- Press the **Cancel** softkey before pressing the **Save** softkey to discard any changes that you have made.
- To enter an IP address, you enter values into four segments already divided for you. When you are done entering the leftmost digits before the first period, use the right arrow key to move to the next segment. The period that follows the leftmost digits is automatically inserted.

✎ **Note**   The Cisco Unified IP Phone provides several methods you can use to reset or restore option settings, if necessary. For more information, see the "Resetting the Cisco Unified IP Phone" section on page 12-15.

Related Topics

- Displaying a Setup Menu, page 7-2

- Unlocking and Locking Options, page 7-3

- Ethernet Setup Menu, page 7-4

- WLAN Setup Menu, page 7-7

- IPv4 Setup Menu Options, page 7-10

Ethernet Setup Menu

The Ethernet Setup menu provides options for viewing and making a variety of network settings. Table 7-1 describes these options and, where applicable, explains how to change them.

For information about how to access the Ethernet Setup menu, see the "Displaying a Setup Menu" section on page 7-2.

For information about the keys you can use to edit options, see the "Editing Values" section on page 7-3.

> **Note**   The Ethernet data fields are overwritten when a VPN connection is established.

Table 7-1   Ethernet Setup Menu Options

Option	Description	To Change
IPv4 Setup	In the IPv4 Setup configuration submenu, you can do the following: • Enable or disable the phone to use the IP address that is assign by the DHCP server. • Manually set the IP Address, Subnet Mask, Default Routers, DNS Server, and Alternate TFTP servers. For more information on the IPv4 address fields, refer to Table 7-3.	Scroll to IPv4 Setup and press the **Select** button.
MAC Address	Unique Media Access Control (MAC) address of the phone.	Display only—Cannot configure.
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.	1. Set the DHCP Enabled option to **No**. 2. Scroll to the Domain Name option, press the **Select** key, and then enter a new domain name. 3. Press the **Apply** softkey.

Table 7-1   Ethernet Setup Menu Options (continued)

Option	Description	To Change
Operational VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member. If the phone has not received an auxiliary VLAN, this option indicates the Administrative VLAN. If neither the auxiliary VLAN nor the Administrative VLAN are configured, this option is blank.	Display only—Cannot configure. The phone obtains its Operational VLAN ID via Cisco Discovery Protocol (CDP) or Link Level Discovery Protocol Media Endpoint Discovery (LLDP-MED). This information comes from the switch to which the phone is attached. To assign a VLAN ID manually, use the Admin VLAN ID option.
Admin. VLAN ID	Auxiliary VLAN in which the phone is a member. Used only if the phone does not receive an auxiliary VLAN from the switch; otherwise it is ignored.	1. Scroll to the Admin. VLAN ID option, press the **Select** softkey, and then enter a new Admin VLAN setting. 2. Press the **Apply** softkey.
PC VLAN	Allows the phone to interoperate with 3rd party switches that do not support a voice VLAN. The Admin VLAN ID option must be set before you can change this option.	1. Make sure the Admin VLAN ID option is set. 2. Scroll to the **PC VLAN** option, press the **Select** softkey, and then enter a new PC VLAN setting. 3. Press the **Apply** softkey.

Table 7-1 **Ethernet Setup Menu Options (continued)**

Option	Description	To Change
SW Port Setup	Speed and duplex of the Network port. Valid values: • Auto Negotiate • 1000 Full—1000-BaseT/full duplex • 100 Half—100-BaseT/half duplex • 100 Full—100-BaseT/full duplex • 10 Half—10-BaseT/half duplex • 10 Full—10-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to auto-negotiate. If you change the setting of this option, you must change the PC Port Configuration option to the same setting.	1. Unlock network configuration options. 2. Scroll to the SW Port Configuration option and then press the **Select** softkey. 3. Scroll to the setting that you want and then press the **Select** key.
PC Port Setup	Speed and duplex of the Computer (access) port. Valid values: • Auto Negotiate • 1000 Full—1000-BaseT/full duplex • 100 Half—100-BaseT/half duplex • 100 Full—100-BaseT/full duplex • 10 Half—10-BaseT/half duplex • 10 Full—10-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to auto-negotiate. If you change the setting of this option, you must change the SW Port Configuration option to the same setting.	1. Unlock network configuration options. 2. Scroll to the PC Port Configuration option and then press the **Select** softkey. 3. Scroll to the setting that you want and then press the **Select** key. To configure the setting on multiple phones simultaneously, enable the Remote Port Configuration in the Enterprise Phone Configuration (**System > Enterprise Phone Configuration**). **Note** If the ports are configured for Remote Port Configuration in Unified CM, the data cannot be changed on the phone.

Related Topics

WLAN Setup Menu

The WLAN Setup menu provides options for viewing and making a variety of network settings. Table 7-2 describes these options and, where applicable, explains how to change them.

> **Note** You can configure the WLAN settings only on the Cisco Unified IP Phone keypad. You must use the ac adapter when using the Cisco Unified IP Phone in WLAN mode. WLAN is disabled when Ethernet is connected.

For information about how to access the WLAN Setup menu, see the "Displaying a Setup Menu" section on page 7-2.

For information about the keys you can use to edit options, see the "Editing Values" section on page 7-3.

Table 7-2   WLAN Setup Menu Options

Option	Description	To Change
Wireless	Used to turn the wireless radio on Cisco Unified IP Phone on or off. Valid values: • On—Turns the wireless radio on the phone on. • Off—Turns the wireless radio on the phone off. Default: On	1. Scroll to the Wireless option, and use the toggle switch to change the setting between on and off. 2. Press the **Apply** softkey.
WLAN Sign in Access	Enables the display of the WLAN Sign in Access window in the main Applications menu: • On—The WLAN Sign In Access window displays. Turning this value on allows you to sign in or change your WLAN user ID and password on the main Applications menu. Otherwise, to change your login information, you would have to navigate down to the Security menu level and select either the LEAP or EAP-FAST methods, both of which require login credentials. • Off—The WLAN Sign In Access window does not display. Default: Off	1. Scroll to the Wireless Sign In option, and use the toggle switch to change the setting between on and off. 2. Press the **Apply** softkey.
IPv4 Setup	In the IPv4 Setup configuration submenu, you can do the following: • Enable or disable the phone to use the IP address that is assign by the DHCP server. • Manually set the IP Address, Subnet Mask, Default Routers, DNS Server, and Alternate TFTP servers. For more information on the IPv4 address fields, refer to Table 7-3.	Scroll to IPv4 Setup and press the **Select** button.
MAC Address	Unique Media Access Control (MAC) address of the phone.	Display only—Cannot configure.

Table 7-2   *WLAN Setup Menu Options (continued)*

Option	Description	To Change
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.	1. Set the DHCP Enabled option to **No**. 2. Scroll to the Domain Name option, press the **Select** key, and then enter a new domain name. 3. Press the **Apply** softkey.
SSID	Specifies the Service Set Identifier, a unique identifier for accessing wireless access points.	1. Scroll to the SSID option, press the **Select** softkey, and then enter a SSID. 2. Press the **Apply** softkey.

Table 7-2   WLAN Setup Menu Options (continued)

Option	Description	To Change
Security Mode	The type of authentication that the phone uses to access the WLAN. Valid values: • Open—Access to all access points (APs) without encryption. • Open with WEP—Open 802.11 authentication but uses Wired Equivalent Privacy (WEP) for encrypting the data. Specifies access to all APs and authentication through WEP keys at the local AP. • Shared Key—Shared key authentication using WEP. • LEAP—Lightweight Extensible Authentication Protocol authentication exchanges a username and cryptographically secure password with a RADIUS server in the network (Cisco proprietary version of EAP). LEAP supports WPA and WPA2. • EAP-FAST—Extensible Authentication Protocol Flexible Authentication via Secure Tunneling exchanges a username and cryptographically secure password with a RADIUS server in the network where a PAC (Protected Access Credential) is used to established a secure tunnel for authentication. EAP-FAST supports WPA and WPA2. • AKM—Selects the 802.11 authentication mechanism automatically from the configuration information exhibited by the access point. WPA-PSK or WPA versions 1 or 2 can be used when configured for this mode. **Note** Consider the following when you select AKM: 1) AKM uses LEAP for 802.1x when using WPA, WPA2 or CCKM, 2) AKM selects the encryption method by giving precedence to the strongest key management type and then the strongest cipher, and 3) CCKM is not supported with WPA2.	1. Scroll to the Security Mode option, then highlight the desired value. 2. Click **Apply**.
802.11 Mode	Specifies the wireless signal standard that is used in the WLAN. Valid values: • Auto—Default value. Gives precedence to 5.0 Ghz if available. • 802.11a • 802.11b/g	1. Scroll to the 802.11 Mode option, then highlight the desired value. 2. Click **Apply**.

IPv4 Setup Menu Options

The IPv4 Setup menu is a submenu of the Ethernet Setup menu and of the WLAN Setup menu. To reach the IPv4 menu, select the IPv4 option on the Ethernet Setup menu or on the WLAN Setup menu.

Table 7-3 describes the IPv4 Setup menu options.

For information about the keys you can use to edit options, see the "Editing Values" section on page 7-3.

Table 7-3   IPv4 Setup Menu Options

Option	Description	To Change
DHCP Enabled	Indicates whether the phone has DHCP enabled or disabled. When DHCP is enabled, the DHCP server assigns the phone an IP address. When DHCP is disabled, the administrator must manually assign an IP address to the phone.	Scroll to the DHCP Enabled option and press the **No** softkey to disable DHCP, or press the **Yes** softkey to enable DHCP.
IP Address	Internet Protocol (IP) address of the phone. If you assign an IP address with this option, you must also assign a subnet mask and default router. See the Subnet Mask and Default Router options in this table.	1. Set the DHCP Enabled option to **No**. 2. Scroll to the IP Address option, press the **Select** softkey, and then enter a new IP Address. 3. Press the **Apply** softkey
Subnet Mask	Subnet mask used by the phone.	1. Set the DHCP Enabled option to No. 2. Scroll to the Subnet Mask option, press the **Select** softkey, and then enter a new subnet mask. 3. Press the **Apply** softkey.
Default Router	Default router used by the phone.	1. Set the DHCP Enabled option to No. 2. Scroll to the appropriate Default Router option, press the **Select** softkey, and then enter a new router IP address. 3. Press the **Apply** softkey.
DNS Server 1 DNS Server 2 DNS Server 3	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–3) used by the phone.	1. Set the DHCP Enabled option to No. 2. Scroll to the appropriate DNS Server option, press the **Select** softkey, and then enter a new DNS server IP address. 3. Press the **Apply** softkey. 4. Repeat Steps 2 and 3 as needed to assign backup DNS servers.

Table 7-3   IPv4 Setup Menu Options (continued)

Option	Description	To Change
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.	Scroll to the Alternate TFTP option and press the **Yes** softkey if the phone should use an alternative TFTP server; press the **No** softkey if the phone should not use an alternative TFTP server.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone. If you are not using DHCP in your network and you want to change this server, you must use the TFTP Server 1 option. If you set the Alternate TFTP option to yes, you must enter a non-zero value for the TFTP Server 1 option. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL or ITL file on the phone, you must unlock the file before you can save changes to the TFTP Server 1 option. In this case, the phone will delete the file when you save changes to the TFTP Server 1 option. A new CTL or ITL file will be downloaded from the new TFTP Server 1 address. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in this order: 1. Any manually assigned IPv6 TFTP servers 2. Any manually assigned IPv4 TFTP servers 3. DHCPv6 assigned TFTP servers 4. DHCP assigned TFTP servers **Note** For information about the CTL and ITL files, refer to *Cisco Unified Communications Manager Security Guide*.	1. Unlock the CTL or ITL file if necessary (for example, if you are changing the administrative domain of the phone). If the CTL and ITL files both exist, unlock either file. 2. If DHCP is enabled, set the Alternate TFTP option to **Yes**. 3. Scroll to the TFTP Server 1 option, press the **Select** softkey, and then enter a new TFTP server IP address. 4. Press the **Apply** softkey then press Save.

Table 7-3   IPv4 Setup Menu Options (continued)

Option	Description	To Change
TFTP Server 2	Optional backup TFTP server that the phone uses if the primary TFTP server is unavailable. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL or ITL file on the phone, you must unlock either of the files before you can save changes to the TFTP Server 2 option. In this case, the phone will delete either of the files when you save changes to the TFTP Server 2 option. A new CTL or ITL file will be downloaded from the new TFTP Server 2 address. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: 1. Manually assigned IPv6 TFTP servers 2. Manually assigned IPv4 TFTP servers 3. DHCPv6 assigned TFTP servers 4. DHCP assigned TFTP servers **Note** For information about the CTL or ITL file, see *Cisco Unified Communications Manager Security Guide*.	1. Unlock the CTL or ITL file if necessary (for example, if you are changing the administrative domain of the phone). If both the CTL and ITL files exist, unlock either of the files. 2. Unlock network configuration options. 3. Enter an IP address for the TFTP Server 1 option. 4. Scroll to the TFTP Server 2 option, press the **Select** softkey, and then enter a new backup TFTP server IP address. If there is no secondary TFTP Server, you can use the **Delete** softkey to clear the field of a previous value. 5. Press the **Apply** softkey and then press Save. If you forgot to unlock the CTL or ITL file, you can change the TFTP Server 2 address in either file, then erase them by pressing the Erase softkey from the Security Configuration menu. A new CTL or ITL file will be downloaded from the new TFTP Server 2 address.
BOOTP Server	Indicates whether the phone received its IP address from a BOOTP server rather than from a DHCP server.	Display-only field.
DHCP Address Released	Releases the IP address assigned by DHCP.	This field is editable if DHCP is enabled. If you wish to remove the phone from the VLAN and release the IP address for reassignment, set this option to "Yes" and press the **Apply** softkey.

Related Topics

- Displaying a Setup Menu, page 7-2
- Unlocking and Locking Options, page 7-3
- Editing Values, page 7-3

Security Setup Menu

The Security Setup menu that you access directly from the Administrator Settings menu provides information about various security settings. It also provides access to the Trust List menu and indicates if the CTL or ITL file is installed on the phone.

For information about how to access the Security Setup menu and its submenus, see the "Displaying a Setup Menu" section on page 7-2.

Table 7-4 describes the options in the security setup menu.

Table 7-4   Security Menu Settings

Option	Description	To Change
Security Mode	Displays the security mode that is set for the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**. The setting appears in the Protocol Specific Information portion of the window.
LSC	Indicates whether a locally significant certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).	For information about how to manage the LSC for your phone, refer to the "Using the Certificate Authority Proxy Function" chapter in *Cisco Unified Communications Manager Security Guide*.
Trust List	The Trust List provides submenus for the CTL, ITL, and Signed Configuration files. The CTL File submenu displays the contents of the CTL file. The ITL File submenu displays contents of the ITL file.	For more information, see the "Trust List Menu" section on page 7-14.
802.1X Authentication	Allows you to enable 802.1X authentication for this phone.	See the "802.1X Authentication and Transaction Status" section on page 7-15.

Trust List Menu

The Trust List menu provides a top-level menu containing CTL, ITL, and the Signed Configuration submenus. The content of the Signed Configuration file is SRST.

The Trust List menu only display components that have certificates associated with them. Table 7-5 describes trust list menu options.

Table 7-5   *Trust List Menu Settings*

Option	Description	To Change
CTL Signature	MD5 hash of the CTL file.	For more information about these settings, refer to the "Configuring the Cisco CTL Client" section in *Cisco Unified Communications Manager Security Guide*.
Unified CM/TFTP Server	Common name of a Cisco Unified Communications Manager and TFTP server used by the phone. Also displays a certificate icon if a certificate is installed for this server.	For more information about these settings, refer to the "Configuring the Cisco CTL Client" section in *Cisco Unified Communications Manager Security Guide*.
CAPF Server	Common name of the CAPF used by the phone. Also displays a certificate icon if a certificate is installed for this server.	For more information about these settings, refer to the "Configuring the Cisco CTL Client" section in *Cisco Unified Communications Manager Security Guide*.
SRST Router	IP address of the trusted SRST router that is available to the phone, if such a device has been configured in Cisco Unified Communications Manager Administration. Also displays a certificate icon if a certificate is installed for this server.	For more information about these settings, refer to the "Configuring the Cisco CTL Client" section in *Cisco Unified Communications Manager Security Guide*.

802.1X Authentication and Transaction Status

The 802.1X Authentication Settings menu allows you to enable 802.1X authentication and view transaction status. These options are described in Table 7-6.

You can access the 802.1X Authentication settings by pressing the **Applications** button ⚙ and choosing **Administrator Settings** > **Security Setup > 802.1X Authentication**. To exit this menu, press the **Exit** softkey

Table 7-6   802.1X Authentication Settings

Option	Description	To Change
Device Authentication	Determines whether 802.1X authentication is enabled: • **Enabled**—Phone uses 802.1X authentication to request network access. • **Disabled**—Default setting in which the phone uses CDP to acquire VLAN and network access.	1. After pressing the **Applications** button ⚙, choose **Administrator Settings > Security Setup > 802.1X Authentication > Device Authentication**. 2. Set the Device Authentication option to Enabled or Disabled. 3. Press the **Apply** softkey.
EAP-MD5	Specifies a password for use with 802.1X authentication using the following menu options (described in the following rows): • Device ID • Shared Secret • Realm	After pressing the **Applications** button ⚙, choose **Administrator Settings > Security Setup > 802.1X Authentication > EAP-MD5**.
	Device ID—Derivative of the phone's model number and unique MAC address displayed in this format: CP-<model>-SEP-<MAC>	Display only—Cannot configure.
	Shared Secret—Choose a password to use on the phone and on the authentication server. The password must be between 6 and 32 characters, consisting of any combination of numbers or letters. **Note** If you disable 802.1X authentication or perform a factory reset (reset all settings) of the phone, the shared secret is deleted.	1. Choose **EAP-MD5 > Shared Secret**. 2. Enter the shared secret. 3. Press the **Apply** softkey. See the "Troubleshooting Cisco Unified IP Phone Security" section on page 12-9 for assistance in recovering from a deleted shared secret.
	Realm—Indicates the user network domain, always set as *Network*.	Display only—Cannot configure.

Table 7-6   802.1X Authentication Settings (continued)

Option	Description	To Change

Transaction Status	• State—Displays the state of 802.1x authentication:
	
	  – Disconnected—Indicates that 802.1x authentication is not configured on the phone.
	
	  – Authenticated—Indicates that the phone has been authenticated.
	
	  – Held—Indicates that the authentication process is in progress.
	
	• Protocol—Displays the EAP method used for 802.1x authentication (can be EAP-MD5, EAP-FAST or EAP-TLS).
		Display only—Cannot configure.

VPN Configuration Menu

The VPN Configuration menu allows you to enable the VPN Client connection using the Secure Sockets Layer (SSL). The VPN connection is used when a phone is located outside a trusted network or when network traffic between the phone and Unified CM must cross untrusted networks.

Your system administrator determines if your phone should be configured with the VPN functionality and enables the VPN feature.

If your phone is configured for VPN, the status of Auto-Detect Network Connection, which is configured on the UCM server, determines if a VPN connection is possible:

- If Auto-Detect Network Connection is disabled, a VPN connection is possible. The Sign In screen appears, and you are prompted for credentials based on the authentication method that your system administrator configured on your phone. (On the phone in the Applications > VPN window, you can toggle the VPN Enabled field to On or Off to turn on or off the phone's ability to attempt a VPN connection.)

- If Auto-Detect Network Connection is enabled, you cannot connect through VPN, so the Sign In screen does not appear, and you are not prompted for credentials.

Connecting to VPN

Use this procedure to connect through VPN.

Procedure Steps

Step 1   After you turn on your phone and the Sign In screen for VPN Client appears (except with certificate authentication mode), enter your credentials based on the configured authentication method:

- Username and password—Enter the username and the password that your system administrator gave you.

- Certificate and password—Enter the password that your system administrator gave you. Your username is derived from the certificate.

- Certificate—If the phone uses only a certificate for authentication, the Sign In screen does not appear, and phone displays the status of the phone attempting the VPN connection.

(When the power is lost or reset under some circumstances, the stored credentials are cleared.)

When a phone is at the Sign In screen, the screen stays lit and does not enter a power-save mode. This alerts the user that the phone is unregistered. If the phone remains in this state for a long time, the image may persist in the display for a short time after the user logs back in and then the image fades.

Step 2   Select the **Sign In** softkey to connect.

(If you press **Cancel** while the phone is attempting the connection, the connection attempt stops, and the Sign In screen appears again. Then if you press Cancel, the VPN menu appears and shows the VPN field as Off. The phone will not attempt a connection again until you set the VPN Enabled field to On.)

VPN Configuration Settings

Table 7-7 describes the VPN configuration options on the Cisco Unified IP Phone.

Table 7-7   *VPN Configuration Settings*

Option	Description	To Change
VPN Enabled	If Auto-Detect Network Connection is disabled, toggle the VPN Enabled field to On or Off to turn on or off the phone's ability to attempt a VPN connection.	Choose **Applications** > **VPN**. Set the VPN option to On or Off. If the feature is disabled on the Cisco Unified Communications Manager, this option is disabled.
Change Credentials	Changes the user ID and password. If authentication is certificate-only or VPN Enabled is off, the option will be grayed out.	—
VPN Status	Shows if option is enabled or disabled.	Display only—Configured on Unified CM.

<CHAPTER 8

Configuring Features, Templates, Services, and Users

After you install Cisco Unified IP Phones in your network, configure their network settings, and add them to Cisco Unified Communications Manager, you must use the Cisco Unified Communications Manager Administration application to configure telephony features, optionally modify phone templates, set up services, and assign users.

This chapter provides an overview of these configuration and setup procedures. Cisco Unified Communications Manager documentation provides detailed instructions for these procedures.

For suggestions about how to provide users with information about features, and what information to provide, see Appendix A, "Providing Information to Users Via a Website."

For information about setting up phones in non-English environments, see Appendix B, "Supporting International Users."

This chapter includes following topics:

- Telephony Features Available for the Cisco Unified IP Phone, page 8-2
- Configuring Product Specific Configuration Parameters, page 8-26
- Configuring Corporate and Personal Directories, page 8-27
- Feature Buttons and Softkeys, page 8-28
- Park Monitoring, page 8-23
- Modifying Phone Button Templates, page 8-29
- Configuring Feature Control Policies, page 8-31
- Setting Up Services, page 8-32
- Adding Users to Cisco Unified Communications Manager, page 8-33
- Managing the User Options Web Pages, page 8-34

Telephony Features Available for the Cisco Unified IP Phone

After you add Cisco Unified IP Phones to Cisco Unified Communications Manager, you can add functionality to the phones. Table 8-1 includes a list of supported telephony features, many of which you can configure using Cisco Unified Communications Manager Administration. The Reference column lists Cisco Unified Communications Manager and other documentation that contains configuration procedures and related information.

For information about using most of these features on the phone, refer to *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager.* Also, see Table 8-4 for a list of features that can be configured as programmable buttons; Table 8-4 also lists whether a feature is a softkey or a dedicated feature button.

Note   Cisco Unified Communications Manager Administration also provides several service parameters that you can use to configure various telephony functions. For more information on accessing and configuring service parameters, refer to *Cisco Unified Communications Manager Administration Guide.* For more information on the functions of a service, click on the name of the parameter or the question mark help button in the Service Parameter Configuration window.

Table 8-1   Telephony Features for the Cisco Unified IP Phone

Feature	Description	Configuration Reference
Agent Greeting	Allows an agent to create and update a prerecorded greeting that plays at the beginning of a call, such as a customer call, before the agent begins the conversation with the caller. The Agent can prerecord a single greeting or multiple ones as needed and create and update them. When a customer calls, both callers hear the prerecorded greeting. The agent can remain on mute until the greeting ends or answer the call over the greeting. All codecs supported for the phone are supported for Agent Greeting calls. To enable Agent Greeting in the Cisco Unified CM Administration application, choose Device > Phone, locate IP Phone that you want to configure. Scroll to the Device Information Layout pane and set Built In Bridge to On or Default. If Built In Bridge is set to Default, in the Cisco Unified CM Administration application, choose **System** > **Service Parameter** and select the appropriate Server and Service. Scroll to the Clusterwide Parameters (Device - Phone) pane and set Builtin Bridge Enable to On.	For more information, see: • *Cisco Unified Communications Manager Features and Services Guide*, Barge and Privacy. • *Cisco Unified Communications Manager System Guide*, *Cisco Unified IP Phones*.
All Calls	Allows a user to view a list, sorted in chronological order (oldest first), of all active calls on all of their phone lines.	For more information, see the "Modifying a Phone Button Template for All Calls" section on page 8-29.

Table 8-1   Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Anonymous Call Block	Allows a user to reject calls from anonymous callers.	For more information, go to the "SIP Profile Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.
Any Call Pickup	Allows users to pick up a redirected call via the CTI application, on any line in their call pickup group, regardless of how the call was routed to the phone.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" chapter.
Answer (oldest call)	Allows a user to answer the oldest call that is available on all line appearances on the user's phone, including Hold Reversion and Park Reversion calls that are in an altering state.	No configuration required other than to make this a programmable feature button.
Assisted Directed Call Park	Lets the end user press only one button to direct-park a call. This requires you to configure a BLF Directed Call Park button. Then, when the user presses an idle BLF Directed Call Park feature button for an active call, the active call will be immediately parked at the Dpark slot associated with the Directed Call Park feature button.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide,* "Configuring Directed Call Park" section.
Auto Answer	Connects incoming calls automatically after a ring or two. Auto Answer works with either the speakerphone, or the headset.	For more information, go to the "Directory Number Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.
Auto dial	Allows the phone user to choose from matching numbers in the Placed Calls log while dialing. To place the call, the user can choose a number from the Auto Dial list or continue to enter digits manually.	Requires no configuration.

Table 8-1   ***Telephony Features for the Cisco Unified IP Phone (continued)***

Feature	Description	Configuration Reference
Automatic Port Synchronization	When the Cisco Unified CM administrator uses the Remote Port Configuration feature to set the speed and duplex function of an IP phone remotely, loss of packets can occur if one port is slower than the other. The Automatic Port Synchronization feature synchronizes the ports to the lowest speed among the two ports, which eliminates packet loss. When automatic port synchronization is enabled, it is recommended that both ports be configured for autonegotiate. If one port is enabled for autonegotiate and the other is at a fixed speed, the phone synchronizes to the fixed port speed. **Note** If both the ports are configured for fixed speed, the Automatic Port Synchronization feature is ineffective. **Note** The Remote Port Configuration and Automatic Port Synchronization features are compatible only with IEEE 802.3AF Power of Ethernet (PoE) switches. Switches that support only Cisco Inline Power are not compatible. Enabling this feature on phones that are connected to these types of switches could result in loss of connectivity to Cisco Unified CM, if the phone is powered by PoE.	To configure the parameter in the Cisco Unified CM Administration application, choose **Device > Phone**, select the appropriate IP phones, and scroll to the Product Specific Configuration Layout pane. To configure the setting on multiple phones simultaneously, enable Automatic Port Synchronization in the Enterprise Phone Configuration (**System > Enterprise Phone Configuration**).
Barge	Allows a user to join a non-private call on a shared phone line. Barge features adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features. **Note** The Cisco Unified IP Phone can still use barge when the Built in Bridge Enable service parameter is set to off. To prevent a user from using the barge feature on the The Cisco Unified IP Phone, you must disable Barge in Feature Control Policy for the phone.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide,* "Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone" chapter. • *Cisco Unified Communications Manager Features and Services Guide,* "Barge and Privacy" chapter. • *Cisco Unified Communications Manager Administration Guide,* "Feature Control Policy Configuration."

Table 8-1   ***Telephony Features for the Cisco Unified IP Phone (continued)***

Feature	Description	Configuration Reference
Bluetooth Profiles	Allows you to select the bluetooth profiles for Cisco Unified Phone 9951 and 9971. The two profiles are: • Handsfree • Human Interface Device	1. Go to Cisco Unified CM Administration > **Device > Phone**. 2. Find your phone from the list of phones associated with the Cisco Unified CM. 3. Click on the **Device Name** of the phone. 4. The Phone Configuration window appears. 5. Go to Product Specific Configuration Layout area and from the Bluetooth Profiles drop-down list box, choose the applicable profile. The Handsfree profile is selected by default. Check the "Override Common Settings" check box for any setting in Product Specific Configuration area that you wish to update. • If you do not check this check box, the corresponding parameter setting does not take effect. • Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window. If you set these same parameters in these other windows too, the setting that takes precedence is determined in the following order: 1. Device Configuration window settings, 2. Common Phone Profile window settings 3. Enterprise Phone Configuration window settings. For more information, see *Cisco Unified Communications Manager Administration Guide*.
Block external to external transfer	Prevents users from transferring an external call to another external number.	For more information, go to the "External Call Transfer Restrictions" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Busy Lamp Field (BLF)	Allows a user to monitor the call state of a directory number associated with a speed-dial button, call log, or directory listing on the phone.	For more information, go to the "Presence" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 8-1   Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Busy Lamp Field (BLF) Pickup	Provides enhancements to BLF speed dial. Allows you to configure a Directory Number (DN) that a user can monitor for incoming calls. When the DN receives an incoming call, the system alerts the monitoring user, who can then pick up the call.	For more information, go to the "Call Pickup" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available.	For more information, refer to: • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone" chapter. • *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Call Back" chapter.
Call Chaperone	Allows an authorized Call Chaperone user to supervise and record a call. **Note** This feature will work only if the External Call Control feature, described later in this table, is also configured. The Call Chaperone user intercepts and answers the call from calling party, manually creates a conference to the called party and remains on the conference to supervise and record the call. Cisco Unified IP Phones that have the Call Chaperone feature configured on them have a Record softkey. The Call Chaperone user presses the Record softkey to record a call. For chaperoned calls, an announcement is played or spoken by one of the participants at the start of the call. An announcement will alert later participants in the call that the call is being recorded.	For more information, refer to the Cisco Unified Communications Manager Features and Services Guide, "External Call Control" chapter.
Call display restrictions	Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide,* "Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager Features and Services Guide,* "Call Display Restrictions" chapter.

Table 8-1   Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Call Forward	Allows users to redirect incoming calls to another number. Call forward options include Call Forward All, Call Forward Busy, Call Forward No Answer, and Call Forward No Coverage. Call forward options can be assigned on a per-line basis.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide,* "Directory Number Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone" chapter. • "Specifying Options that Appear on the User Options Web Pages" section on page 8-36
Call Forward All loop breakout	Detects and prevents Call Forward All loops. When a Call Forward All loop is detected, the Call Forward All configuration is ignored and the call rings through.	For more information, go to the "Cisco Unified IP Phone" chapter in the *Cisco Unified Communications Manager System Guide*.
Call Forward All loop prevention	Prevents a user from configuring a Call Forward All destination directly on the phone that creates a Call Forward All loop or that creates a Call Forward All chain with more hops than the existing *Forward Maximum Hop Count* service parameter allows.	For more information, go to the "Cisco Unified IP Phone" chapter in the *Cisco Unified Communications Manager System Guide*.
Call Forward destination override	Allows you to override Call Forward All (CFA) in cases where the CFA target places a call to the CFA initiator. This feature allows the CFA target to reach the CFA initiator for important calls. The override works whether the CFA target phone number is internal or external.	For more information, go to the "Understanding Directory Numbers" chapter in the *Cisco Unified Communications Manager System Guide*.
Call Park	Allows users to park (temporarily store) a call and then retrieve the call by using another phone in the Cisco Unified Communications Manager system.	For more information, go to the "Call Park and Directed Call Park" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 8-1   Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Call Pickup	Allows a user to answer a call that is ringing on a co-worker's phone by redirecting the call. You can configure the call pickup feature to support the following: • Allows users to redirect a call that is ringing on another phone within their pickup group to their phone. • Allows a user to answer a call that is ringing on a particular directory number. • Allows a user to answer a call that is ringing on a directory number in another group. • Allows a user to answer a call ringing on a phone in another group that is associated with their own group. You can configure the phone to allows a user to use one-touch pickup functionality for call pickup features. You can configure an audio and/or visual alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group.	For more information, go to the "Call Pickup" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Call recording	Allows a supervisor to record an active call. The user might hear a recording audible alert tone during a call when it is being recorded. When a call is secured, the security status of the call is displayed as a lock icon on Cisco Unified IP Phones. The connected parties might also hear an audible alert tone that indicates the call is secured and is being recorded. The intercom feature is disabled when a call is being monitored or recorded. When an active call is being monitored or recorded, you can receive or place intercom calls; however, if you place an intercom call, the active call will be put on hold, which causes the recording session to terminate and the monitoring session to suspend. To resume the monitoring session, the party whose call is being monitored must resume the call.	For more information, refer to *Cisco Unified Communications Manager Features and Services Guide*, "Monitoring and Recording" chapter.
Call Waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. Displays incoming call information on the phone screen.	For more information, go to the "Understanding Directory Numbers" chapter in the *Cisco Unified Communications Manager System Guide*.

Table 8-1   Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Caller ID	Displays caller identification such as a phone number, name, or other descriptive text on the phone screen.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide,* "Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Understanding Route Plans" chapter. • *Cisco Unified Communications Manager Features and Services Guide,* "Call Display Restrictions" chapter. • *Cisco Unified Communications Manager Administration Guide,* "Directory Number Configuration" chapter.
Caller ID Blocking	Allows a user to block their phone number or e-mail address from phones that have caller identification enabled.	For more information, refer to: • *Cisco Unified Communications Manager System Guide,* "Understanding Route Plans" chapter. • *Cisco Unified Communications Manager Administration Guide,* "Directory Number Configuration" chapter.
Calling Party Normalization	Globalizes or localizes the incoming calling party number so that the appropriate calling number presentation displays on the phone. Supports the international escape character +.	For more information, go to the "Calling Party Normalization" chapter in the *Cisco Unified Communications Features and Services Guide.*
CAST for SIP	Establishes communication between the Cisco Unified Video Advantage (CUVA) and the Cisco Unified IP phones to support video on the PC even if the IP phone does not have video capability.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide.*
Cisco Extension Mobility	Allows users to temporarily access their Cisco Unified IP Phone configuration such as line appearances, services, and speed dials from shared Cisco Unified IP Phone by logging into the Cisco Extension Mobility service on that phone. Cisco Extension Mobility can be useful if users work from a variety of locations within your company or if they share a workspace with coworkers.	For more information, go to the "Cisco Extention Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide.*

Table 8-1 *Telephony Features for the Cisco Unified IP Phone (continued)*

Feature	Description	Configuration Reference
Cisco Extension Mobility Change PIN	Enables a user to change the PIN from a Cisco Unified IP Phone. The PIN can be changed by: • Using the ChangePIN softkey on the Extension Mobility logout screen. • Configuring the Change Credential IP Phone Service on the phone.	• For more information, go to the "Cisco Extension Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. • For changing the PIN by change credential service, see Configuring the Change Credential IP Phone Service section in the *Cisco Unified Communications Manager Administration*.
Cisco Extension Mobility Cross Cluster	Enables a user configured in one cluster to log into a Cisco Unified IP Phone in another cluster. Users from a home cluster log into a Cisco Unified IP Phone at a visiting cluster. Configure Cisco Extension Mobility on Cisco Unified IP Phones before you configure EMCC.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Extension Mobility Cross Cluster" chapter.
Cisco Web Dialer	Allows users to make calls from web and desktop applications.	For more information go to the "Cisco Web Dialer" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Conference	• Allows a user to talk simultaneously with multiple parties by calling each participant individually. • Allows a non-initiator in a standard (ad hoc) conference to add or remove participants. • Allows users to join two or more calls that are on one line to create a conference call and remain on the call.	The service parameter, Advance Adhoc Conference, (disabled by default in Cisco Unified Communications Manager Administration) allows you to enable these features. For information on conferences, go to the "Conference Bridges" chapter in the *Cisco Unified Communications Manager System Guide*. For more information, go to the "Cisco Unified IP Phone" chapter in the *Cisco Unified Communications Manager System Guide*. **Note** Be sure to inform your users whether these features are activated.
CTI Applications	A computer telephony integration (CTI) route point can designate a virtual device to receive multiple, simultaneous calls for application-controlled redirection.	For more information, go to the "CTI Route Point Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.
Directed Call Park	Allows a user to transfer an active call to an available directed call park number that the user dials or speed dials. A Call Park BLF button indicates whether a directed call park number is occupied and provides speed-dial access to the directed call park number.	For more information, go to the "Call Park and Directed Call Park" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 8-1   *Telephony Features for the Cisco Unified IP Phone (continued)*

Feature	Description	Configuration Reference
Divert	Allows a user to transfer a ringing, connected, or held call directly to a voice-messaging system or to the busy target. Divert acts on the highlighted call only. Incoming calls are not automatically highlighted. If a second call rings while the user is on the first call, Divert will act on the first call unless the user actively highlights the second call. When a call is diverted, the line becomes available to make or receive new calls. When Enhanced Immediate Divert is enabled, it allows users to transfer incoming calls directly to their voice messaging system or to the voice messaging system of the original called party.	For more information on diverting calls to voicemail, go to the "Immediate Divert" chapter in the *Cisco Unified Communications Manager Features and Services Guide.* For more information on Enhanced Immediate Divert, go to the "Cisco Unified IP Phone" chapter in the *Cisco Unified Communications Manager System Guide*.
Dual Bank Information	Allows the Cisco Unified CM administrator to upgrade phone firmware with a new load before resetting the previous load to an Inactive load status. The Cisco Unified CM administrator can verify whether the active and inactive loads were swapped correctly.	1. In Cisco Unified CM Administration, choose **Device > Device Defaults**. 2. Check the load information in the **Inactive Load Information** field. 3. From the **Bulk Administration > Import/Export > Export > Device Defaults** window, schedule an export job. 4. Download the exported tar file and untar it. 5. Check the file format in the exported CSV file and verify that the CSV file has a column for "Inactive Load Information" with correct value. The CSV file value must match the Device Default value in the Cisco Unified CM Administration window.

Table 8-1   Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Do Not Disturb (DND)	When DND is turned on, either no audible rings occur during the ringing-in state of a call, or no audible or visual notifications of any type occur. You can configure the phone to have a phone-button template with DND as one of the selected features. The following DND-related parameters are configurable in Cisco Unified Communications Manager Administration: • Do Not Disturb—This check box allows you to enable DND on a per-phone basis. Use **Cisco Unified Communications Manager Administration > Device > Phone > Phone Configuration**. • DND Incoming Call Alert—Choose the type of alert to play, if any, on a phone for incoming calls when DND is active. This parameter is located on both the Common Phone Profile page and the Phone configuration page (Phone Configuration window value takes precedence). • BLF Status Depicts DND—Enables DND status to override busy/idle state.	For more information, go to the "Do Not Disturb" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
External Call Control	Allows Cisco Unified Communications Manager to route audio and video calls to a route server that hosts routing rules. The route server receives routing requests from Cisco Unified Communications Manager and in turn returns routing directives to Cisco Unified Communications Manager.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide, "External Call Control"* chapter.
Fast Dial Service	Allows a user to enter a Fast Dial code to place a call. Fast Dial codes can be assigned to phone numbers or Personal Address Book entries. (See "Services" in this table.)	For more information, refer to Modifying a Phone Button Template for Personal Address Book or Speed Dials, page 8-30.

Table 8-1   Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Hold Reversion	Limits the amount of time that a call can be on hold before reverting back to the phone that put the call on hold and alerting the user. Reverting calls are distinguished from incoming calls by a single ring (or beep, depending on the new call indicator setting for the line). This notification repeats at intervals if not resumed. A call that triggers Hold Reversion also displays an animated icon in the call bubble and a brief message on the status line. You can configure call focus priority to favor incoming or reverting calls.	For more information about configuring this feature, go to the "Hold Reversion" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Hold Status	Enables phones with a shared line to distinguish between the local and remote lines that placed a call on hold.	No configuration is required.
Hold/Resume	Allows the user to move a connected call from an active state to a held state. To place a call on hold, select the Hold button. To resume a call, choose the line with the held call and select the **Resume** softkey**.**	• Requires no configuration, unless you want to use music on hold. See "Music-on-Hold" in this table for information. • See "Hold Reversion" in this table.
Hunt Group Display	Provides load sharing for calls to a main directory number. A hunt group contains a series of directory numbers that can answer the incoming calls. When an incoming call is offered to a directory number that is part of the hunt group, this feature displays the main directory number in addition to the calling party.	For more information, refer to: • Cisco Unified Communications Manager *Administration Guide,* "Hunt Group Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Understanding Route Plans" chapter. • Cisco Unified Communications Manager Administration Guide, "CTI Route Point Configuration" chapter.

Table 8-1   Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Intercom	Allows users to place and receive intercom calls using programmable phone buttons. You can configure intercom line buttons to: • Directly dial a specific intercom extension. • Initiate an intercom call and then prompt the user to enter a valid intercom number. **Note** If your user logs into the same phone on a daily basis using their Cisco Extension Mobility profile, assign the phone button template that contains intercom information to their profile, and assign the phone as the default intercom device for the intercom line. **Note** Intercom feature does not support Extension Mobility Cross Cluster.	For more information, go to the "Intercom chapter" chapter in the *Cisco Unified Communications Manager Feature and Services Guide*.
Intelligent Session Control	Reroutes a enterprise originated call to a users' mobile phone to the enterprise number. The call only rings the user's mobile but not his/her desk phone. When the call is answered on the mobile phone, the desk phone displays a Remote in Use message. During these calls, a user can use the various features of the mobile phone.	For more information, go to the "Cisco Unified Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Line select	If this feature is disabled (default), then the ringing line is selected. When enabled, the primary line is picked up even if a call is ringing on another line. The User must manually select the other line. **Note** This feature can also be enabled or disabled for Extension Mobility.	For more information, refer to the option "Always use prime line" in the following chapters of *Cisco Unified Communications Manager Administration Guide*: • "Device Profile Configuration" • "Common Phone Profile Configuration" • "Cisco Unified IP Phone Services Configuration"
Line select for voice messages	When disabled (default), pressing the Messages button selects the line that has a voice message. If more than one line has voice mail, then the first available line is selected. When enabled, the primary line is always used to retrieve voice messages. **Note** This feature can also be enabled or disabled for Extension Mobility.	For more information, refer to the option "Always use prime line for voice message" in the following chapters of *Cisco Unified Communications Manager Administration Guide*: • "Device Profile Configuration" • "Common Phone Profile Configuration" • "Cisco Unified IP Phone Services Configuration"

Table 8-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Log out of Hunt Groups	Allows users to log out of a hunt group and temporarily block calls from ringing their phone when they are not available to take calls. Logging out of hunt groups does not prevent non-hunt group calls from ringing their phone.	For more information • See the "Setting Up Services" section on page 8-32. • *Cisco Unified Communications Manager System Guide,* "Understanding Route Plans" chapter.
Malicious Caller Identification (MCID)	Allows users to notify the system administrator about suspicious calls that are received.	For more information refer to: • *Cisco Unified Communications Manager System Guide,* ""Cisco Unified IP Phone" • *Cisco Unified Communications Manager Features and Services Guide,* "Malicious Call Identification" chapter.
Meet-Me conference	Allows a user to host a Meet-Me conference in which other participants call a predetermined number at a scheduled time.	For more information go to the "Meet-Me Number/Pattern Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide.*
Message Waiting	Defines directory numbers for message-waiting on and message-waiting off indicator. A directly connected voice-messaging system uses the specified directory number to set or to clear a message-waiting indication for a particular Cisco Unified IP Phone.	For more information, refer to: • *Cisco Unified Communications Manager Administration Guide,* "Message Waiting Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter.
Message waiting Indicator	A light on the handset that indicates that a user has one or more new voice messages.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Message Waiting Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter.
Message Waiting Indicator (MWI)	The MWI is both a visual indicator, viewable from 360 degrees and an audible message waiting indicator. Users change the voice message light on their handset and the audible voice message indicator on their phone by logging in to their User Options web pages and accessing the message indicator settings. Users change the setting to on or off.	For more information, go to the "Cisco Unified IP Phone" chapter in the *Cisco Unified Communications Manager System Guide.*
Missed Call History	Allows a user to specify whether missed calls will be logged in the missed calls history for a given line appearance.	For more information refer to the Cisco Unified Communications Manager Administration Guide, "Directory Number Configuration" chapter.

Table 8-1 **Telephony Features for the Cisco Unified IP Phone (continued)**

Feature	Description	Configuration Reference
Mobile Connect	Enables users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and a remote device such as a mobile phone. Users can restrict the group of callers according to phone number and time of day. Also see the "Session Handoff" entry in this table.	For more information, go to the "Cisco Unified Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Mobile Voice Access	Extends Mobile Connect capabilities by allowing users to access an interactive voice response (IVR) system to originate a call from a remote device such as a cellular phone.	For more information, go to the "Cisco Unified Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Multiple calls per line appearance	Each line can support multiple calls. Only one call can be active at any time; other calls are automatically placed on hold.	For more information, go to the "Understanding Directory Numbers" chapter in the *Cisco Unified Communications Manager System Guide*.
Music on hold	Plays music while callers are on hold.	For more information go to the "Music On Hold" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Mute	Mutes the microphone from the handset or headset.	Requires no configuration.
On-hook Dialing	Allows a user to dial a number without going off hook. The user can then either pick up the handset, press the Call softkey, or press either the headset or speaker buttons to initiate the call.	For more information, refer to the *Cisco Unified IP Phone 9971 User Guide for Cisco Unified Communications Manager (SIP)*, "Calling Features" chapter.
Park Monitoring	Monitors the status of a parked call. The park monitoring call bubble is not cleared until the parked call gets retrieved or is abandoned by the parkee. This parked call can be retrieved using the same call bubble on the parker's phone.	For more information, see the "Park Monitoring" section on page 8-23. For information on call park, see the *Cisco Unified Communications Manager Features and Services Guide*, "Call Park and Directed Call Park" chapter.

Table 8-1   *Telephony Features for the Cisco Unified IP Phone (continued)*

Feature	Description	Configuration Reference
Peer Firmware Sharing	The Peer Firmware Sharing feature provides these advantages in high speed campus LAN settings: • Limits congestion on TFTP transfers to centralized remote TFTP servers • Eliminates the need to manually control firmware upgrades • Reduces phone downtime during upgrades when large numbers of devices are reset simultaneously Peer Firmware Sharing may also aid in firmware upgrades in branch/remote office deployment scenarios running over bandwidth-limited WAN links. When enabled, it allows the phone to discover like phones on the subnet that are requesting the files that make up the firmware image, and to automatically assemble transfer hierarchies on a per-file basis. The individual files making up the firmware image are retrieved from the TFTP server by only the root phone in the hierarchy, and are then rapidly transferred down the transfer hierarchy to the other phones on the subnet using TCP connections. This menu option indicates whether the phone supports peer firmware sharing. Settings include: • Enabled—default • Disabled **Note** Phone firmware release 9.1(1) supports HTTP and TFTP firmware downloads methods.	1. Go to Cisco Unified CM Administration > **Device** > **Phone**. 2. Find your phone from the list of phones associated with the Cisco Unified CM. 3. Click on the **Device Name** of the phone. The Phone Configuration window appears. 4. Go to **Product Specific Configuration Layout** area and select **Enable** from the Peer Firmware Sharing drop-down list box. The Peer Firmware Sharing is enabled by default. Check the "Override Common Settings" check box for any setting in Product Specific Configuration area that you wish to update. • If you do not check this check box, the corresponding parameter setting does not take effect. • Parameters that you set in the Product Specific Configuration area may also appear in the Phone Configuration window for various devices and in the Enterprise Phone Configuration window. If you set these same parameters in these other windows too, the setting that takes precedence is determined in the following order: 1. Device Configuration window settings, 2. Common Phone Profile window settings 3. Enterprise Phone Configuration window settings.
Phone secure web access	Cisco Unified IP Phones can now securely access the web with the use of a phone trust store called "phone-trust."	*Cisco Unified Communications Manager Security Guide*, "Security Overview" chapter.
Plus Dialing	Allows the user to dial E.164 numbers prefixed with a "+" sign. To dial the + sign, the user needs to press and hold the "*" key for at least 1 second. This applies to dialing the first digit for an on-hook or off-hook call only.	Requires no configuration.

Table 8-1   ***Telephony Features for the Cisco Unified IP Phone (continued)***

Feature	Description	Configuration Reference
Power Negotiation over LLDP	Allows the phone to negotiate the power using LLDP and CDP protocols. Power Negotiation should not be disabled when connected to a switch that supports power negotiation. If disabled, it could cause the switch to shut off power to the phone.	The Power Negotiation is enabled by default. To change the setting of Power Negotiation to Disabled, select Disabled in the Power Negotiation drop-down list box in the Phone Configuration window, Product Specific Configuration. For more information, see *Cisco Unified Communications Manager Administration Guide*.
Presence-enabled directories	Allows a user to monitor the call state of another directory number (DN) listed in call logs, speed-dials, and corporate directories. The Busy Lamp Field (BLF) for the DN displays the call state.	For more information, go to the "Presence" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.
Privacy	Prevents users who share a line from adding themselves to a call and from viewing information on their phone screens about the call of the other user.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone" chapter. • *Cisco Unified Communications Manager Features and Services Guide* "Barge and Privacy" chapter.
Private Line Automated Ringdown (PLAR)	The Cisco Unified Communications Manager administrator can configure a phone number that the Cisco Unified IP Phone dials as soon as the handset goes off hook. This can be useful for phones that are designated for calling emergency or "hotline" numbers.	For more information, go to the "Directory Number Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.
Programmable Feature Button	The administrator can assign features to programmable keys. When the administrator configures features on the feature button, they always remain visible and accessible to the user; for example the administrator can assign a dedicated Pickup button on the phone.	For more information, refer to: • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone" chapter. • *Cisco Unified Communications Manager Administration Guide*, "Phone Button Template Configuration" chapter
Protected calling	Provides a secure (encrypted) connection between two phones. A security tone is played at the beginning of the call to indicate that both phones are protected. Some features, such as conference calling, shared lines, Extension Mobility, and Join Across Lines are not available when protected calling is configured. Protected calls are not authenticated.	For more information about security, see the "Overview of Supported Security Features" section on page 1-16. For additional information, refer to the *Cisco Unified Communications Manager Security Guide*.

Table 8-1   Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Quality Reporting Tool (QRT)	Allows users to use the **QRT** feature button on a phone to submit information about problem phone calls. QRT can be configured for either of two user modes, depending upon the amount of user interaction desired with QRT.	For more information refer to: • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone" chapter. • *Cisco Unified Communications Manager Features and Services Guide,* "Quality Report Tool" chapter.
Redial	Allows users to call the most recently dialed phone number by pressing the Redial softkey.	Requires no configuration.
Remote Port Configuration	Allows the administrator to configure the speed and duplex function of the phone Ethernet ports remotely by using Cisco Unified CM Administration. This enhances the performance for large deployments with specific port settings. **Note** If the ports are configured for Remote Port Configuration in Cisco Unified CM, the data cannot be changed on the phone.	To configure the parameter in the Cisco Unified CM Administration application, choose **Device > Phone**, select the appropriate IP phones, and scroll to the Product Specific Configuration Layout pane (Switch Port Remote Configuration or PC Port Remote Configuration). To configure the setting on multiple phones simultaneously, configure the Remote Port Configuration in the Enterprise Phone Configuration (**System** > **Enterprise Phone Configuration**).
Ring Tone Setting	Identifies ring type used for a line when a phone has another active call.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Directory Number Configuration" chapter. • "Creating Custom Phone Rings" section on page 9-2.
Ringtone	Users can customize how their phone indicates an incoming call and a new voice mail message.	For more information, go to the "Custom Phone Rings" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Table 8-1   Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference

Secure and Nonsecure Indication Tone	When a phone is configured as secure (encrypted and trusted) in Unified CM, it can be given a "protected" status. After that if desired, the protected phone can be configured to play an indication tone at the beginning of a call:
	
	• Protected Device—To change the status of a secure phone to protected, check the "Protected Device" check box in Cisco Unified Communications Manager Administration > Device > Phone > Phone Configuration.
	
	• Play Secure Indication Tone—To enable the protected phone to play a secure or nonsecure indication tone, set the "Play Secure Indication Tone" to True. (The default is False.) You set this option in Cisco Unified Communications Manager Administration > System > Service Parameters. Select the server and then the Unified CM service. In the Service Parameter Configuration window, select the option in the Feature - Secure Tone area. (The default is False.)
	
	Only protected phones hear these secure or nonsecure indication tones. (Nonprotected phones never hear tones.) If the overall call status changes during the call, the indication tone changes accordingly. At that time, the protected phone plays the appropriate tone.
	
	A protected phone plays a tone or not under these circumstances:
	
	• When the option to play the tone is enabled Play Secure Indication Tone option is enabled (True):
	
	   – W1hen end-to-end secure media is established and the call status is secure, the phone plays the secure indication tone (three long beeps with pauses).
	
	   – When end-to-end nonsecure media is established and the call status is nonsecure, the phone plays the nonsecure indication tone (six short beeps with brief pauses).
	
	If the Play Secure Indication Tone option is disabled, no tone is played.
		Requires no configuration.

Table 8-1   Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Secure Conference	• Allows secure phones to place conference calls using a secured conference bridge. • As new participants are added by using Confrn, Barge softkeys or MeetMe conferencing, the secure call icon displays as long as all participants use secure phones. • The Conference List displays the security level of each conference participant. Initiators can remove non-secure participants from the Conference List. (Non-initiators can add or remove conference participants if the Advanced Adhoc Conference Enabled parameter is set.)	For more information about security, see the "Overview of Supported Security Features" section on page 1-16. For additional information, refer to: • *Cisco Unified Communications Manager System Guide,* "Conference Bridges" chapter • *Cisco Unified Communications Manager Administration Guide,* "Conference Bridge Configuration" chapter • *Cisco Unified Communications Manager Security Guide.*
Services	Allows you to use the Cisco Unified IP Phone Services Configuration menu in Cisco Unified Communications Manager Administration to define and maintain the list of phone services to which users can subscribe. **Note** Some services appear on the phone by default, or you can disable them so that they do not display on the phone.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone Services" chapter.
Services URL button	Allows users to access services from a programmable button rather than by using the Services menu on a phone.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone Services" chapter.
Session Handoff	Allows users to switch calls from a mobile phone to Cisco Unified devices that share the same line. Handsets on all the devices on the shared line then flash simultaneously. After a user answers the call from one of the Cisco Unified devices, the other Cisco Unified devices that share the same line display a Remote in Use message. However, if the call fails to switch from the mobile phone, the mobile phone might display a Cannot Move Conversation message.	For more information, refer to the *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Unified Mobility" chapter. *Cisco Unified Communications Manager Features and Services Guide,* "Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator Integration" chapter.
Shared line	Allows a user to have multiple phones that share the same phone number or allows a user to share a phone number with a coworker.	For more information, go to the "Understanding Directory Numbers" chapter in the *Cisco Unified Communications Manager System Guide*.

Table 8-1   Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Monitoring and Recording	Allows a supervisor to monitor an active call silently. The supervisor cannot be heard by either party on the call. The user may receive an audible alert during a call when it is being monitored. When a call is secure, a lock icon is displayed. Callers may also receive an audible alert to indicate that the call is being monitored. The connected parties may also receive an audible alert that indicates the call is secure and is being monitored. When an active call is being monitored or recorded, you can receive or place intercom calls; however, if you place an intercom call, the active call is put on hold. This causes the recording session to terminate and the monitoring session to suspend. To resume the monitoring session, the person being monitored must resume the call.	For more information, go to the *"Monitoring and Recording"* chapter in the *Cisco Unified Communications Manager Features and Services Guide.*
Speed Dial	Allows users to speed dial a phone number by entering an assigned index code (1-99) on the phone keypad. **Note** You can use Speed Dialing while on-hook or off-hook. Users assign index codes from the User Options web pages.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Cisco Unified IP Phone Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone" chapter.
Time-of-Day Routing	Restricts access to specified telephony features by time period.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Time Period Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Time-of-Day Routing" chapter.
Time Zone Update	Updates the Cisco Unified IP Phone with time zone changes.	For more information, refer to the *Cisco Unified Communications Manager Administration Guide*, "Date/Time Group Configuration" chapter.
Transfer	Allows users to redirect connected calls from their phones to another number. The user can connect two calls to each other. The user can remain on the line or transfer the call without staying on line.	Requires no configuration.

Table 8-1   Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Video mode	Allows a user to select the video display mode for viewing a video conference, depending on the modes configured in the system.	For more information: • Refer to *Cisco Unified Communications Manager Administration Guide,* "Conference Bridge Configuration" chapter. • Refer to *Cisco Unified Communications Manager System Guide,* "Understanding Video Telephony" chapter.
Video Support	Enables video support on the phone.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Conference Bridge Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Understanding Video Telephony" chapter. • *Cisco VT Advantage Administration Guide*, "Overview of Cisco VT Advantage" chapter.
VPN	Using SSL, provides a virtual private network (VPN) connection on the Cisco Unified IP Phone when it is located outside a trusted network or when network traffic between the phone and Unified CM must cross untrusted networks.	For more information, see *Cisco Unified Communications Manager Security Guide*, Configuring Virtual Private Networks.
Voice messaging system	Enables callers to leave messages if calls are unanswered.	For more information refer to: • *Cisco Unified Communications Manager Administration Guide,* "Cisco Voice-Mail Port Configuration" chapter. • *Cisco Unified Communications Manager System Guide,* "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter.

Park Monitoring

Park monitoring is supported only when a Cisco Unified IP Phone 8961, 9951, or 9971 parks a call. Park monitoring then monitors the status of a parked call. The park monitoring call bubble is not cleared until the parked call gets retrieved or is abandoned by the parkee. This parked call can be retrieved using the same call bubble on the parker's phone.

The following sections describe the options for configuring park monitoring:

Setting the Service Parameters for Park Monitoring

Cisco Unified Communications Manager administration provides three clusterwide service timer parameters for park monitoring: Park Monitoring Reversion Timer, Park Monitoring Periodic Reversion Timer, and Park Monitoring Forward No Retrieve Timer. Each service parameter includes a default and requires no special configuration. These timer parameters are for park monitoring only; the Call Park Display Timer and Call Park Reversion Timer are not used for park monitoring. See Table 8-2 for descriptions of these parameters.

Table 8-2   Service Parameters for Park Monitoring

Field	Description
Park Monitoring Reversion Timer	Default is 60 seconds. This parameter determines the number of seconds that Cisco Unified Communications Manager waits before prompting the user to retrieve a call that the user parked. This timer starts when the user presses the Park softkey on the phone, and a reminder is issued when the timer expires.
	You can override the value specified in this service parameter on a per-line basis in the Directory Number Configuration window (in Cisco Unified Communications Manager administration, choose **Call Routing > Directory Number**), in the Park Monitoring section. Specify a value of 0 to immediately utilize the periodic reversion interval specified in the Park Monitoring Periodic Reversion Timer service parameter (see below). For example, if this parameter is set to zero and the Park Monitoring Periodic Reversion Timer is set to 15, the user will be immediately prompted about the parked call and every 15 seconds thereafter until the Park Monitoring Forward No Retrieve Timer (see below) expires.
Park Monitoring Periodic Reversion Timer	Default is 30 seconds.This parameter determines the interval (in seconds) that Cisco Unified Communications Manager waits before prompting the user again that a call has been parked. To be connected to the parked call, the user can simply go off-hook during one of these prompts. Cisco Unified Communications Manager continues to prompt the user about the parked call as long as the call remains parked and until the time specified in the Park Monitoring Forward No Retrieve Timer (see below) expires. Specify a value of 0 to disable periodic prompts about the parked call.
Park Monitoring Forward No Retrieve Timer	Default is 300 seconds. This parameter determines the number of seconds that park reminder notifications occur before the parked call is forwarded to the Park Monitoring Forward No Retrieve destination specified in the parker Directory Number Configuration window. (If no forward destination is provided in Cisco Unified Communications Manager Administration, the call is returned to the line that parked the call.) This parameter starts when the time specified in the Park Monitoring Reversion Timer service parameter has expired. When the Park Monitoring Forward No Retrieve Timer expires, the call is removed from park and forwarded to the specified destination or returned to the parker line.

Note   To set the timers, in Cisco Unified Communications Manager administration, choose **System > Service Parameters** and update the Park Monitoring Reversion Timer, Park Monitoring Periodic Reversion Timer, and Park Monitoring Forward No Retrieve Timer fields in the **Clusterwide Parameters (Feature-General)** pane.

Setting Park Monitoring Parameters in Directory Number Configuration Window

The Directory Number Configuration window (in Cisco Unified Communications Manager administration, choose **Call Routing > Directory Number**) contains an area called "Park Monitoring," where you can configure the three parameters shown in Table 8-3.

Table 8-3   Park Monitoring Parameters in Directory Number Configuration Window

Field	Description
Park Monitoring Forward No Retrieve Destination External	When the parkee is an external party, then the call will be forwarded to the specified destination in the parker's Park Monitoring Forward No Retrieve Destination External parameter. If the Forward No Retrieve Destination External field value is empty, the parkee will be redirected to the parker's line.
Park Monitoring Forward No Retrieve Destination Internal	When the parkee is an internal party, then the call will be forwarded to the specified destination in the parker's Park Monitoring Forward No Retrieve Destination Internal parameter. If the Forward No Retrieve Destination Internal is empty, the parkee will be redirected to the parker's line.
Park Monitoring Reversion Timer	This parameter determines the number of seconds that Cisco Unified Communications Manager waits before prompting the user to retrieve a call that the user parked. This timer starts when the user presses the Park softkey on the phone, and a reminder is issued when the timer expires. Default: 60 seconds **Note** If you configure a non-zero value, this value overrides the value of this parameter set in the Service Parameters window. However, if you configure a value of 0 here, then the value in the Service Parameters window will be used.

Setting Park Monitoring Parameter in Hunt Pilot Configuration Window

When a call that was routed via the hunt list is parked, the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter value is used (unless it is blank) when the Park Monitoring Forward No Retrieve Timer expires. This value is configured in the Hunt Pilot Configuration window (in Cisco Unified Communications Manager administration, choose **Call Routing > Route/Hunt > Hunt Pilot**). If the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter value is blank, then the call will be forwarded to the destination configured in the Directory Number Configuration window when the Park Monitoring Forward No Retrieve Timer expires.

Configuring Product Specific Configuration Parameters

Cisco Unified Communications Manager Administration allows you to set some product-specific configuration parameters for Cisco Unified IP Phones in any of the following windows:

- Phone Configuration window (**Device** > **Phone)**; Product Specific Configuration portion of window
- Common Phone Profile window (**Device** > **Device Settings** > **Common Phone Profile)**
- Enterprise Phone Configuration window (**System** > **Enterprise Phone Configuration)**

List of Parameters

You can set the following parameters in any of the three configuration windows listed above:

- Back USB Port (for Cisco Unified IP Phones 9951 and 9971)
- Side USB Port
- Enable/Disable USB Classes
- Bluetooth (for Cisco Unified IP Phones 9951 and 9971)
- Bluetooth Profiles (only for Cisco Unified IP Phones 9951 and 9971)
- WLAN (for Cisco Unified IP Phone 9971 only)
- Settings Access
- Web Access
- Days Display Not Active
- Display on Time
- Display on Duration
- Display Idle Timeout
- Load Server
- RTCP
- Peer Firmware Sharing
- Cisco Discovery Protocol (CDP): Switch Port
- Cisco Discovery Protocol (CDP): PC Port
- Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port
- Link Layer Discovery Protocol (LLDP): PC Port
- 802.1x Authentication
- Switch Port Remote Configuration
- PC Port Remote Configuration
- Automatic Port Synchronization

Note   Descriptions of these parameters can be found by clicking the "?" button in Cisco Unified Communications Manager administration.

Override Common Settings Check Box

When you set the parameters, select the Override Common Settings check box for each setting you wish to update. If you do not check this box, the corresponding parameter setting does not take effect. If you set the parameters at the three configuration windows, the setting takes precedence in the following order:

- Phone Configuration window
- Common Phone Profile window
- Enterprise Phone Configuration window

Configuring Corporate and Personal Directories

The **Contact** button on the Cisco Unified IP Phone gives users access to several directories. These directories can include:

- Corporate Directory—Allows a user to look up phone numbers for co-workers.

  To support this feature, you must configure corporate directories. See the "Configuring Corporate Directories" section on page 8-27 for more information.

- Personal Directory—Allows a user to store a set of personal numbers.

  To support this feature, you must provide the user with software to configure the personal directory. See the "Configuring Personal Directory" section on page 8-27 for more information.

Configuring Corporate Directories

Cisco Unified Communications Manager uses a Lightweight Directory Access Protocol (LDAP) directory to store authentication and authorization information about users of Cisco Unified Communications Manager applications that interface with Cisco Unified Communications Manager. Authentication establishes the users' rights to access the system. Authorization identifies the telephony resources that a user is permitted to use, such as a specific phone extension.

After completing the LDAP directory configuration, users can use the Corporate Directory service on their phone to look up users in the corporate directory.

Configuring Personal Directory

Personal Directory consists of the following features:

- Personal Address Book (PAB)
- Speed Dials
- Address Book Synchronization Tool (TABSynch)

Users can access Personal Directory features by these methods:

- From a web browser—Users can access the PAB and Speed Dials features from the Cisco Unified Communications Manager User Options web pages
- From the Cisco Unified IP Phone—Choose **Contacts** to search the corporate directory or the user's personal directory.

- From a Microsoft Windows application—Users can use the TABSynch tool to synchronize their PABs with Microsoft Windows Address Book (WAB). Customers who want to use the Microsoft Outlook Address Book (OAB) should begin by importing the data from the OAB into the Windows Address Book (WAB). TabSync can then be used to synchronize the WAB with Personal Directory.

To ensure that Cisco IP Phone Address Book Synchronizer users have access only to end-user data that pertains to them, activate the Cisco UXL Web Service in Cisco Unified Serviceability.

To configure Personal Directory from a web browser, users must access their User Options web pages. You must provide users with a URL and login information.

To synchronize with Microsoft Outlook, users must install the TABSynch utility, provided by you. To obtain the TABSynch software to distribute to users, choose **Application > Plugins** from Cisco Unified Communications Manager Administration, then locate and click **Cisco IP Phone Address Book Synchronizer**.

Feature Buttons and Softkeys

Table 8-4 provides information about some of the features that are available on softkeys, some that are available on dedicated feature buttons, and some that you need to configure as programmable feature buttons. An "X" in the table indicates that the feature is supported for the corresponding button type or softkey. Of the two button types and softkeys, only programmable feature buttons require configuration in Cisco Unified IP Phone administration.

Note   The Cisco Unified IP Phone 8961, 9951, and 9971 does not use softkey templates in Cisco Unified Communications Manager administration.

For information on configuring programmable feature buttons, see the "Modifying Phone Button Templates" section on page 8-29.

Table 8-4   Features and Corresponding Buttons and Softkeys

Feature Name	Dedicated Feature Button	Programmable Feature Button	Softkey
All Calls		X	
Answer		X	X
Call Back		X	X
Call Forward All		X	X
Call Park		X	X
Call Park Line Status		X	
Call Pickup		X	
Call Pickup Line Status		X	
Conference	X		X (available while on a conference only)
Divert			X

Table 8-4   Features and Corresponding Buttons and Softkeys

Do Not Disturb		X	
Group Pickup		X	
Hold	X		
Hunt Groups		X	
Intercom		X	
Malicious Call Identification (MCID)		X	
Meet Me		X	
Mobile Connect		X	
Mute	X		
Other Pickup		X	
Privacy		X	
Redial		X	X
Speed Dial		X	X
Speed Dial Line Status		X	
Transfer	X		X (available during a transfer only)
Quality Reporting Tool (QRT)		X	

Modifying Phone Button Templates

Phone button templates let you assign speed dials and call-handling features to programmable buttons. Call-handling features that can be assigned to buttons include Answer, Mobility, and All Calls.

Ideally, you modify templates before registering phones on the network. In this way, you can access customized phone button template options from Cisco Unified Communications Manager during registration.

To modify a phone button template, choose **Device > Device Settings > Phone Button Template** in Cisco Unified Communications Manager Administration. To assign a phone button template to a phone, use the Phone Button Template field in the Cisco Unified Communications Manager Administration Phone Configuration page. Refer to *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide* for more information.

- The default Cisco Unified IP Phone 9971 template that ships with the phone uses buttons 1 and 2 for lines.

Modifying a Phone Button Template for All Calls

It is recommended that you provision an All Calls button for users with multiple shared lines. When you configure an All Call button on the phone, you enable the users to do the following:

- Press the All Calls button to displays a consolidated list of current calls from all lines on the phone.

- Press the All Calls button under Call History to displays a list of all missed calls from all lines on the phone.

- Place a call on the users primary line when the user goes off-hook. All Calls automatically defaults to the users primary line for any outgoing call.

To add the All Calls button, you must modify the phone button template and then assign the template to the phone.

Modifying a Phone Button Template for Personal Address Book or Speed Dials

You can modify a phone button template to associate a service URL with a programmable button. Doing so enables users to have single-button access to the PAB and Speed Dials. Before you modify the phone button template, you must configure PAB or Speed Dials as an IP phone service.

To configure PAB or Speed Dial as an IP phone service (if it is not already a service), follow these steps:

Procedure

Step 1   From Cisco Unified Communications Manager Administration, choose **Device >Device Settings > Phone Services**.

The Find and List IP Phone Services window displays.

Step 2   Click **Add New**.

The IP Phone Services Configuration window displays.

Step 3   Enter the following settings:

- Service Name and ASCII Service Name—Enter **Personal Address Book**.

- Service Description—Enter an optional description of the service.

- Service URL

    For PAB, enter the following URL:

    http://<*Unified CM-server-name*>**:8080/ccmpd/login.do?name=#DEVICENAME#&service=pab**

    For Fast Dial, enter the following URL:

    http://<*Unified-CM-server-name*>**:8080/ccmpd/login.do?name=#DEVICENAME#&service=fd**

- Secure Service URL

    For PAB, enter the following URL:

    https://<Unified CM-server-name>:8443/ccmpd/login.do?name=#DEVICENAME#&service=pab

    For Fast Dial, enter the following URL:

    https://<Unified-CM-server-name>:8443/ccmpd/login.do?name=#DEVICENAME#&service=fd

- Service Category—Select **XML Service**.

- Service Type—Select **Directories**.

- Enable—Select the check box.

    http://<IP_address> or https://<IP_address> (depending on the protocol supported by the Cisco Unified IP Phone)

Step 4   Click **Save**.

You can add, update, or delete service parameters as needed as described in the "Cisco Unified IP Phone Services Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide.*

> **Note**   If you change the service URL, remove an IP phone service parameter, or change the name of a phone service parameter for a phone service to which users are subscribed, you must click **Update Subscriptions** to update all currently subscribed users with the changes, or users must resubscribe to the service to rebuild the correct URL.

To modify a phone button template for PAB or Fast Dial, follow these steps:

Procedure

Step 1   From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Phone Button Template**.

Step 2   Click **Find**.

Step 3   Select the phone model.

Step 4   Click **Copy**, enter a name for the new template, and then click **Save**.

The Phone Button Template Configuration window opens.

Step 5   Identify the button you would like to assign, and select **Service URL** from the Features drop-down list box associated with the line.

Step 6   Click **Save** to create a new phone button template using the service URL.

Step 7   Choose **Device > Phone** and open the Phone Configuration window for the phone.

Step 8   Select the new phone button template from the Phone Button Template drop-down list box.

Step 9   Click **Save** to store the change and then click **Reset** to implement the change.

The phone user can now access the User Options pages and associate the service with a button on the phone.

For additional information on IP phone services, go to the "Cisco Unified IP Phone Services Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide,* For additional information on configuring line buttons, go to the "Cisco Unified IP Phone Configuration" chapter and "Configuring Speed-Dial Buttons" section in the *Cisco Unified Communications Manager Administration Guide*.

Configuring Feature Control Policies

You can limit the appearance of some telephony features on the Cisco Unified IP Phone 8961, 9951, and 9971 by enabling or disabling these features in the feature control policy configuration. When you disable a feature in the feature control policy configuration for a phone, you restrict the user's access to the feature and the softkeys associated with the feature does not display on the phone.

To create a Feature Control Policy, follow these steps:

Procedure

Step 1   From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Feature Control Policy**.

The Find and List Feature Control Policy window displays.

Step 2   Click **Add New** to define a set of policies.

Step 3   Enter the following settings.

- Name—Enter a name for a new Feature Control Policy
- Description—(Optional) Enter a description.
- Feature Control Section—Check the check box for the features that you want to change the default setting. Table 8-5 displays the list of features that can be configured and the default value.

Step 4   Click **Save.**

Step 5   Apply the policy to the phone by including it in the following settings.

- Enterprise Parameters Configuration—Applies to all phones in the system.
- Common Phone Profile Configuration—Applies to all phones in a group.
- Phone Configuration—Applies to an individual phone

Table 8-5   Feature Control Policy Default Values

Feature	Default Value
Forward All	Enabled
Park	Disabled
To Voicemail	Disabled
Conference List	Enabled
Speed Dial	Enabled
Call Back	Enabled
Redial	Enabled
Barge	Enabled

For more information, refer to the "Feature Control Policy" chapter in the *Cisco Unified Communications Manager Administration Guide.*

Setting Up Services

You can give users access to Cisco Unified IP Phone Services on the Cisco Unified IP Phone 8961, 9951, and 9971. You can also assign a button to different phone services. These services comprise XML applications and Cisco-signed Java midlets that enable the display of interactive content with text and graphics on the phone. The Cisco Unified IP Phone manages each service as a separate application. Examples of services include local movie times, stock quotes, and weather reports.

Before a user can access any service:

- You must use Cisco Unified Communications Manager Administration to configure services that are not present by default.

- The user must subscribe to services using the Cisco Unified Communications Manager User Options application. This web-based application provides a graphical user interface (GUI) for limited, end-user configuration of IP Phone applications. However, a user cannot subscribe to any service that you configure as an enterprise subscription.

Before you set up services, gather the URLs for the sites you want to set up and verify that users can access those sites from your corporate IP telephony network. (This is not applicable for the default services provided by Cisco.)

To set up these services, choose **Device > Device Settings > Phone Services** from Cisco Unified Communications Manager Administration. Refer to "Cisco Unified IP Phone Services Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* and to the "Cisco Unified IP Phone Services" chapter in the *Cisco Unified Communications Manager System Guide* for more information.

After you configure these services, verify that your users have access to the Cisco Unified Communications Manager User Options web-based application, from which they can select and subscribe to configured services. See the "How Users Subscribe to Services and Configure Phone Features" section on page A-2 for a summary of the information that you must provide to end users.

> **Note** To configure Cisco Extension Mobility services for users, go to the "Cisco Extension Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Adding Users to Cisco Unified Communications Manager

Adding users to Cisco Unified Communications Manager allows you to display and maintain information about users and allows each user to perform these tasks:

- Access the corporate directory and other customized directories from a Cisco Unified IP Phone.

- Create a personal directory.

- Set up speed dial and call forwarding numbers.

- Subscribe to services that are accessible from a Cisco Unified IP Phone.

You can add users to Cisco Unified Communications Manager using one of these following methods:

- To add users individually, choose **User Management > End User** from Cisco Unified Communications Manager Administration.

  For more information, go to the End User Configuration chapter in the *Cisco Unified Communications Manager Administration Guide*.

- To add users in batches, use the Bulk Administration Tool. This method also enables you to set an identical default password for all users.

  For more information, go to the "Bulk Administration" chapter in *Cisco Unified Communications Manager Administration Guide*.

Managing the User Options Web Pages

From the User Options web page, users can customize and control several phone features and settings. For detailed information about the User Options web pages, refer to *Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager.*

Giving Users Access to the User Options Web Pages

Before a user can access the User Options web pages, you must add the user to the standard Cisco Unified Communications Manager end user group and associate the appropriate phone with the user.

To add the user to the stand Cisco Unified Communications Manager end user group, follow these steps:

Procedure

Step 1   From Cisco Unified Communications Manager Administration, choose **User Management** > **User Groups**.

The Find and List Users window displays.

Step 2   Enter the appropriate search criteria and click **Find**.

Step 3   Click on the **Standard CCM End Users** link. The User Group Configuration page for the Standard CCM End Users displays.

Step 4   Click **Add End Users to Group**. The Find and List Users window displays.

Step 5   Use the Find User drop-down list boxes to find the end users that you want to add and click **Find**.

Step 6   A list of end users that matches your search criteria displays.

Step 7   In the list of records that display, click the check box next to the users that you want to add to this user group. If the list comprises multiple pages, use the links at the bottom to see more results.

Note   The list of search results does not display end users that already belong to the user group.

Step 8   Click **Add Selected**.

To associate appropriate phones with the user, follow these steps:

Procedure

Step 1   From Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.

The Find and List Users window displays.

Step 2   Enter the appropriate search criteria and click **Find**.

Step 3   In the list of records that display, click the link for the user.

Step 4   Click **Device Association.**

The User Device Association window displays.

Step 5   Enter the appropriate search criteria and click **Find**.

Step 6   Choose the device that you want to associate with the end user by checking the box to the left of the device.

Step 7   Click **Save Selected/Changes** to associate the device with the end user.

Make sure to provide end users with the following information about the User Options web pages:

- The URL required to access the application. This URL is:

  http://<*server_name:portnumber*>**/ccmuser/**, where *server_name* is the host on which the web server is installed.

- A user ID and default password are needed to access the application.

  These settings correspond to the values you entered when you added the user to Cisco Unified Communications Manager (see the "Adding Users to Cisco Unified Communications Manager" section on page 8-33).

For additional information, refer to:

- *Cisco Unified Communications Manager Administration Guide*, "User Group Configuration" chapter.
- *Cisco Unified Communications Manager Administration Guide*, "End User Configuration" chapter.
- *Cisco Unified Communications Manager Administrator Guide*, "Role Configuration" chapter.

Specifying Options that Appear on the User Options Web Pages

Most options that are on the User Options web pages appear by default. However, the following options must be set by the system administrator by using Enterprise Parameters Configuration settings in Cisco Unified Communications Manager Administration:

- Show Ring Settings
- Show Line Text Label Settings
- Show Call Forwarding

Note   The settings apply to all User Options web pages at your site.

To specify the options that appear on the User Options web pages, follow these steps:

Procedure

Step 1   From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.

The Enterprise Parameters Configuration window appears.

Step 2   In the CCMUser Parameters area, specify whether a parameter appears on the User Options web pages by choosing one of these values from the Parameter Value drop-down list box for the parameter:

- **True**—Option displays on the User Options web pages (default except for Show Ring Settings, Show Line Text Label, and Show Call Forwarding).
- **False**—Option does not display on the User Options web pages.
- **Show All Settings**—All call forward settings display on the User Options web pages (default).
- **Hide All Settings**—No call forward settings display on the User Options web pages.
- **Show Only Call Forward All**—Only call forward all calls displays on the User Options web pages.

C H A P T E R 9

Customizing the Cisco Unified IP Phone

This chapter explains how you customize configuration files, phone ring sounds, and background images, and how to disable the phone screen to conserve power.

This chapter includes these topics:

Customizing and Modifying Configuration Files

You can modify configuration files (for example, edit the xml files) and add customized files (for example, custom ring tones, call-back tones) to the TFTP directory. You can modify files and add customized files to the TFTP directory in Cisco Unified Communications Operating System Administration, from the TFTP Server File Upload window. Refer to *Cisco Unified Communications Operating System Administration Guide* for information about how to upload files to the TFTP folder on a Cisco Unified Communications Manager server.

You can obtain a copy of the Ringlist.xml and List.xml files from the system using the following admin command-line interface (CLI) "file" commands (for exact syntax, refer to the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*):

- admin:file
    - file list
    - file view
    - file search
    - file get
    - file dump
    - file tail
    - file delete

Creating Custom Phone Rings

The Cisco Unified IP Phone ships with two default ring types that are implemented in hardware: Chirp1 and Chirp2. Cisco Unified Communications Manager also provides a default set of additional phone ring sounds that are implemented in software as pulse code modulation (PCM) files. The PCM files, along with an XML file (named Ringlist.xml) that describes the ring list options that are available at your site, exist in the TFTP directory on each Cisco Unified Communications Manager server.

For more information, see the "Cisco TFTP" chapter in *Cisco Unified Communications Manager System Guide* and the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide.*

The following sections describe how you can customize the phone rings that are available at your site by creating PCM files and editing the Ringlist.xml file:

- Ringlist.xml File Format Requirements, page 9-2
- PCM File Requirements for Custom Ring Types, page 9-3
- Configuring a Custom Phone Ring, page 9-3

Ringlist.xml File Format Requirements

The Ringlist.xml file defines an XML object that contains a list of phone ring types. This file can include up to 50 ring types. Each ring type contains a pointer to the PCM file that is used for that ring type and the text that will appear on the Ring Type menu on a Cisco Unified IP Phone for that ring. The Cisco TFTP server for each Cisco Unified Communications Manager contains this file.

The CiscoIPPhoneRinglist XML object uses the following simple tag set to describe the information:

```
<CiscoIPPhoneRingList>
    <Ring>
        <DisplayName/>
        <FileName/>
    </Ring>
</CiscoIPPhoneRingList>
```

The following characteristics apply to the definition names. You must include the required DisplayName and FileName for each phone ring type.

- DisplayName defines the name of the custom ring for the associated PCM file that will display on the Ring Type menu of the Cisco Unified IP Phone.
- FileName specifies the name of the PCM file for the custom ring to associate with DisplayName.

Note   The DisplayName and FileName fields must not exceed 25 characters.

This example shows a Ringlist.xml file that defines two phone ring types:

```
<CiscoIPPhoneRingList>
    <Ring>
        <DisplayName>Analog Synth 1</DisplayName>
        <FileName>Analog1.raw</FileName>
    </Ring>
    <Ring>
        <DisplayName>Analog Synth 2</DisplayName>
        <FileName>Analog2.raw</FileName>
    </Ring>
</CiscoIPPhoneRingList>
```

PCM File Requirements for Custom Ring Types

The PCM files for the rings must meet the following requirements for proper playback on Cisco Unified IP Phones:

- Raw PCM (no header)
- 8000 samples per second
- 8 bits per sample
- uLaw compression
- Maximum ring size—16080 samples
- Minimum ring size—240 samples
- Number of samples in the ring is evenly divisible by 240.
- Ring starts and ends at the zero crossing.
- To create PCM files for custom phone rings, you can use any standard audio editing packages that support these file format requirements.

Configuring a Custom Phone Ring

To create custom phone rings for the Cisco Unified IP Phone, follow these steps:

Procedure

Step 1   Create a PCM file for each custom ring (one ring per file). Ensure the PCM files comply with the format guidelines that are listed in the "PCM File Requirements for Custom Ring Types" section on page 9-3.

Step 2   Upload the new PCM files that you created to the Cisco TFTP server for each Cisco Unified Communications Manager in your cluster. For more information, see the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide.*

Step 3   Use an text editor to edit the Ringlist.xml file. See the "Ringlist.xml File Format Requirements" section on page 9-2 for information about how to format this file and for a sample Ringlist.xml file.

Step 4   Save your modifications and close the Ringlist.xml file.

Step 5   To cache the new Ringlist.xml file, stop and start the TFTP service by using Cisco Unified Serviceability or disable and re-enable the "Enable Caching of Constant and Bin Files at Startup" TFTP service parameter (located in the Advanced Service Parameters).

Creating Custom Background Images

You can provide users with a choice of background images (or *wallpaper*) for the LCD screen on their phones. Users can select a background image by choosing **Applications > Preferences > Wallpaper** on the phone.

The image choices that users see come from PNG images and an XML file (called List.xml) that are stored on the TFTP server used by the phone. By storing your own PNG files and editing the XML file on the TFTP server, you can designate the background images from which users can choose. In this way, you can provide custom images, such as your company logo.

The following sections describe how you can customize the background images that are available at your site by creating your own PNG files and editing the List.xml file:

- List.xml File Format Requirements, page 9-4.
- PNG File Requirements for Custom Background Images, page 9-5.
- Configuring a Custom Background Image, page 9-5

List.xml File Format Requirements

The List.xml file defines an XML object that contains a list of background images. The List.xml file is stored in the following subdirectory on the TFTP server:

Desktops/640x480x24

Tip   If you are manually creating the directory structure and the List.xml file, you must ensure that the directories and files can be accessed by the user\CCMService, which is used by the TFTP service.

For more information, see the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide*.

The List.xml file can include up to 50 background images. The images are in the order that they appear in the Background Images menu on the phone. For each image, the List.xml file contains one element type, called ImageItem. The ImageItem element includes these two attributes:

- Image—Uniform resource identifier (URI) that specifies where the phone obtains the thumbnail image that will appear on the Background Images menu on a phone.
- URL—URI that specifies where the phone obtains the full size image.

The following example shows a List.xml file that defines two images. The required Image and URL attributes must be included for each image. The TFTP URI that is shown in the example is the only supported method for linking to full size and thumbnail images. HTTP URL support is not provided.

List.xml Example

```
<CiscoIPPhoneImageList>
<ImageItem Image="TFTP:Desktops/640x480x24/TN-Fountain.png"
URL="TFTP:Desktops/640x480x24/Fountain.png"/>
<ImageItem Image="TFTP:Desktops/640x480x24/TN-FullMoon.png"
URL="TFTP:Desktops/640x480x24/FullMoon.png"/>
</CiscoIPPhoneImageList>
```

The Cisco Unified IP Phone firmware includes a default background image. This image is not defined in the List.xml file. The default image is always the first image that appears in the Background Images menu on the phone.

PNG File Requirements for Custom Background Images

Each background image requires two PNG files:

- Full size image—Version that appears on the on the phone.
- Thumbnail image—Version that displays on the Background Images screen from which users can select an image. Must be 25% of the size of the full size image.

Tip   Many graphics programs provide a feature that will resize a graphic. An easy way to create a thumbnail image is to first create and save the full size image, then use the sizing feature in the graphics program to create a version of that image that is 25% of the original size. Save the thumbnail version by using a different name.

The PNG files for background images must meet the following requirements for proper display on the Cisco Unified IP Phone:

- Full size image—640 pixels (width) X 480 pixels (height).
- Thumbnail image—123 pixels (width) X 111 pixels (height).

Tip   If you are using a graphics program that supports a posterize feature for grayscale, set the number of tonal levels per channel to 16, and the image will posterize to 16 shades of grayscale.

Configuring a Custom Background Image

To create custom background images for the Cisco Unified IP Phone, follow these steps:

Procedure

Step 1   Create two PNG files for each image (a full size version and a thumbnail version). Ensure the PNG files comply with the format guidelines that are listed in the "PNG File Requirements for Custom Background Images" section on page 9-5.

Step 2   Upload the new PNG files that you created to the following subdirectory in the TFTP server for the Cisco Unified Communications Manager:

Desktops/640x480x24

Note   The file name and subdirectory parameters are case sensitive. Be sure to use the forward slash "/" when you specify the subdirectory path.

To upload the files, choose **Software Upgrades > Upload TFTP Server File** in Cisco Unified Communications Operating System Administration. For more information, see the "Software Upgrades" chapter in *Cisco Unified Communications Operating System Administration Guide*.

Note   If the folder does not exist, the folder gets created and the files get uploaded to the folder.

Step 3   You must also copy the customized images and files to the other TFTP servers that the phone may contact to obtain these files.

> ✎
> **Note**   Cisco recommends that you also store backup copies of custom image files in another location. You can use these backup copies if the customized files are overwritten when you upgrade Cisco Unified Communications Manager.

Step 4   Use a text editor to edit the List.xml file. See the for the location of this file, formatting requirements, and a sample file.

Step 5   Save your modifications and close the List.xml file.

> ✎
> **Note**   When you upgrade Cisco Unified Communications Manager, a default List.xml file will replace your customized List.xml file. After you customize the List.xml file, make a copy of the file and store it in another location. After upgrading Cisco Unified Communications Manager, replace the default List.xml file with your stored copy.

Step 6   To cache the new List.xml file, stop and start the TFTP service by using Cisco Unified Serviceability or disable and re-enable the Enable Caching of Constant and Bin Files at Startup TFTP service parameter (located in the Advanced Service Parameters).

Configuring Wideband Codec

If Cisco Unified Communications Manager has been configured to use G.722 (G.722 is enabled by default for the Cisco Unified IP Phone 8961, 9951, and 9971) and if the far endpoint supports G.722, the call connects by using the G.722 codec in place of G.711. This situation occurs regardless of whether the user has enabled a wideband headset or wideband handset, but if either the headset or handset is enabled, the user may notice greater audio sensitivity during the call. Greater sensitivity means improved audio clarity but also means that more background noise can be heard by the far endpoint—noise such as rustling papers or nearby conversations. Even without a wideband headset or handset, some users may prefer the additional sensitivity of G.722. Other users may be distracted by the additional sensitivity of G.722.

Two parameters in Cisco Unified Communications Manager Administration affect whether wideband is supported for this Cisco Unified Communications Manager server and/or a specific phone:

- Advertise G.722 Codec—From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**. The default value of this enterprise parameter is *True*, which means that all Cisco Unified IP Phone Models 9971 that are registered to this Cisco Unified Communications Manager will advertise G.722 to Cisco Unified Communications Manager. If each endpoint in the attempted call supports G.722 in its capabilities set, Cisco Unified Communications Manager will choose that codec for the call when possible.

- Advertise G.722 Codec—From Cisco Unified Communications Manager Administration, choose **Device > Phone**. The default value of this product-specific parameter is to use the value specified in the enterprise parameter. If you want to override this on a per-phone basis, choose *Enabled* or *Disabled* in the Advertise G.722 Codec parameter on the Product Specific Configuration area of the Phone Configuration window.

Configuring the Idle Display

You can specify an idle display (text only; text-file size should not exceed 1M bytes) that appears on the phone screen. The idle display is an XML service that the phone invokes when the phone has been idle (not in use) for a designated period and no feature menu is open.

For detailed instructions about creating and displaying the idle display, refer to *Creating Idle URL Graphics on Cisco Unified IP Phone* at this URL:

http://www.cisco.com/warp/public/788/AVVID/idle-url.html

In addition, you can refer to *Cisco Unified Communications Manager Administration Guide* or to *Cisco Unified Communications Manager Bulk Administration Guide* for the following information:

- Specifying the URL of the idle display XML service:
  - For a single phone—Idle field on the Cisco Unified Communications Manager Phone configuration window
  - For multiple phones simultaneously—URL Idle field on the Cisco Unified Communications Manager Enterprise Parameters configuration window, or the Idle field in the Bulk Administration Tool (BAT)

- Specifying the length of time that the phone is not used before the idle display XML service is invoked:
  - For a single phone—Idle Timer field on the Cisco Unified Communications Manager Phone configuration window
  - For multiple phones simultaneously—URL Idle Time field on the Cisco Unified Communications Manager Enterprise Parameters configuration window, or the Idle Timer field in the Bulk Administration Tool (BAT)

From a phone, you can see settings for the idle display XML service URL and the length of time that the phone is not used before this service is invoked. To see these settings, choose **Settings > Device Configuration** and scroll to the Idle URL and the Idle URL Time parameters.

Automatically Disabling the Cisco Unified IP Phone Display

To conserve power and ensure the longevity of the phone screen display, you can set the display to turn off when it is not needed.

You can configure settings in Cisco Unified Communications Manager Administration to turn off the display at a designated time on some days and all day on other days. For example, you may choose to turn off the display after business hours on weekdays and all day on Saturdays and Sundays.

To turn on the display any time it is off, press the **Select** button.

When you turn the display on, it remains on until the phone has remained idle for a designated length of time, then it turns off automatically.

Table 9-1 explains the Cisco Unified Communications Manager Administration fields that control when the display turns on and off. You configure these fields in Cisco Unified Communications Manager Administration in the Product Specific configuration window. (You access this window by choosing **Device > Phone** from Cisco Unified Communications Manager Administration.)

Table 9-1   *Display On and Off Configuration Fields*

Field	Description
Days Display Not Active	Days that the display does not turn on automatically at the time specified in the Display On Time field.
	Choose the day or days from the drop-down list. To choose more than one day, Ctrl-click each day that you want.
Display On Time	Time each day that the display turns on automatically (except on the days specified in the Days Display Not Active field).
	Enter the time in this field in 24 hour format, where 0:00 is midnight.
	For example, to automatically turn the display on at 7:00 a.m., (0700), enter **7:00**. To turn the display on at 2:00 p.m. (1400), enter **14:00**.
	If this field is blank, the display will automatically turn on at 0:00.
	The default value is 07:30.
Display On Duration	Length of time that the display remains on after turning on at the time specified in the Display On Time field.
	Enter the value in this field in the format *hours:minutes*.
	For example, to keep the display on for 4 hours and 30 minutes after it turns on automatically, enter **4:30**.
	If this field is blank, the phone will turn off at the end of the day (0:00).
	Note If Display On Time is 0:00 and the display on duration is blank (or 24:00), the display will remain on continuously.
	The default value is 10:30.
Display Idle Timeout	Length of time that the phone is idle before the display turns off. Applies only when the display was off as scheduled and was turned on by an end-user (by pressing the **Select** button on the phone).
	Enter the value in this field in the format *hours:minutes*.
	For example, to turn the display off when the phone is idle for 1 hour and 30 minutes after an end-user turns the display on, enter **1:30**.
	The default value is 1:00.

Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone

This chapter describes how to use the following menus on the Cisco Unified IP Phone 8961, 9951, and 9971 to view model information, status messages, and network statistics for the phone:

- Model Information screen—Displays hardware and software information about the phone. For more information, see the "Model Information Screen" section on page 10-1.

- Status menu—Provides access to screens that display the status messages, network statistics, and statistics for the current call. For more information, see the "Status Menu" section on page 10-2.

You can use the information on these screens to monitor the operation of a phone and to assist with troubleshooting.

You can also obtain much of this information, and obtain other related information, remotely through the phone's web page. For more information, see Chapter 11, "Monitoring the Cisco Unified IP Phone Remotely."

For more information about troubleshooting the Cisco Unified IP Phone 8961, 9951, and 9971, see Chapter 12, "Troubleshooting and Maintenance."

This chapter includes these topics:

Model Information Screen

To display the Model Information screen, press the **Applications** button and then select **Phone Information**.

If the user is connected to a secure or authenticated server, a corresponding icon (lock or certificate) will be displayed in the Phone Information Screen to the right of the server option. If the user is not connected to a secure or authenticated Server, no icon will appear.

The Model Information screen includes the options described in Table 10-1.

To exit the Model Information screen, press the **Exit** softkey.

Table 10-1   Model Information Settings for the Cisco Unified IP Phone

Option	Description	To Change
Model Number	Model number of the phone.	Display only—Cannot configure.
IP Address	IP address of the phone.	Display only—Cannot configure.
Host name	Host name of the phone.	Display only—Cannot configure.
Active Load	Version of firmware currently installed on the phone. The user can press the Details softkey for more information.	Display only—Cannot configure.
Inactive Load	Inactive Load appears only when a download is in progress, and a download icon and a status of "Upgrade in Progress" or "Upgrade Failed" also display. If a user presses the Details softkey during an upgrade, the download filename and components are listed. A new firmware image can be set to download in advance of a maintenance window. Then instead of waiting for all of the phones to download the firmware, the system switches more rapidly between resetting an existing load to Inactive status and installing the new load. When the download is complete, the icon changes to indicate the completed status, and a check mark displays for a successful download, and an "X" displays for a failed download. If possible, the rest of the loads continue to download.	Display only—Cannot configure.
Last Upgrade	Date of the most recent firmware upgrade.	Display only—Cannot configure.
Active Server	IP address of the server to which the phone is registered.	Display only—Cannot configure.
Stand-by Server	IP address of the standby server.	Display only—Cannot configure.

Status Menu

To display the Status menu, press **Applications** button and then select **Administrator Settings > Status**. To exit the Status menu, press the **Exit** softkey.

The Status menu includes theses options, which provide information about the phone and its operation:

- Status Messages—Displays the Status Messages screen, which shows a log of important system messages. For more information, see the "Status Messages Screen" section on page 10-3.

- Ethernet Statistics—Displays the Ethernet Statistics screen, which shows Ethernet traffic statistics. For more information, see the "Ethernet Statistics Screen" section on page 10-7.

- WLAN Statistics—Displays the WLAN Statistics screen if applicable. For more information, see the "WLAN Statistics Screen" section on page 10-9.

- Call Statistics—Displays counters and statistics for the current call. For more information, see the "Call Statistics Screen" section on page 10-11. For information about video statistics, see "Video Statistics Screen" section on page 10-13.

- Current Access Point—Displays the Current Access Point screen, if applicable. For more information, see the "Current Access Point Screen" section on page 10-15.

Status Messages Screen

The Status Messages screen displays the 30 most recent status messages that the phone has generated. You can access this screen at any time, even if the phone has not finished starting up. Table 10-2 describes the status messages that might appear. This table also includes actions you can take to address errors.

To display the Status Messages screen, follow these steps:

Procedure

Step 1   Press **Applications** button ⚙.

Step 2   Select **Administrator Settings**.

Step 3   Select **Status.**

Step 4   Select **Status Messages.**

To remove current status messages, press the **Clear List** softkey.

To exit the Status Messages screen, press the **Exit** softkey.

Table 10-2   Status Messages on the Cisco Unified IP Phone

Message	Description	Possible Explanation and Action
CFG TFTP Size Error	The configuration file is too large for file system on the phone.	Power cycle the phone.
Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firmware and place it in the TFTPPath directory. You should only copy files into this directory when the TFTP server software is shut down, otherwise the files may be corrupted.
CTL and ITL installed	The CTL and ITL files are installed on the phone.	None. This message is informational only. Neither the CTL file nor the ITL file was installed previously. For more information about the Trust List, refer to *Cisco Unified Communications Manager Security Guide*.
CTL Installed	A certificate trust list (CTL) file is installed in the phone.	None. This message is informational only. The CTL file was not installed previously. For more information about the CTL file, refer to the *Cisco Unified Communications Manager Security Guide*.
CTL update failed	The phone could not update its certificate trust list (CTL) file.	Problem with the CTL file on the TFTP server. For more information, refer to the *Cisco Unified Communications Manager Security Guide*.

Table 10-2   Status Messages on the Cisco Unified IP Phone (continued)

Message	Description	Possible Explanation and Action
DHCP timeout	DHCP server did not respond.	• Network is busy—The errors should resolve themselves when the network load reduces. • No network connectivity between the DHCP server and the phone—Verify the network connections. • DHCP server is down—Check configuration of DHCP server. • Errors persist—Consider assigning a static IP address. See the "Ethernet Setup Menu" section on page 7-4 for details on assigning a static IP address.
DNS timeout	DNS server did not respond.	• Network is busy—The errors should resolve themselves when the network load reduces. • No network connectivity between the DNS server and the phone—Verify the network connections. • DNS server is down—Check configuration of DNS server.
DNS unknown host	DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	• Verify that the host names of the TFTP server or Cisco Unified Communications Manager are configured properly in DNS. • Consider using IP addresses rather than host names.
Duplicate IP	Another device is using the IP address assigned to the phone.	• If the phone has a static IP address, verify that you have not assigned a duplicate IP address. See the "Ethernet Setup Menu" section on page 7-4 section for details. • If you are using DHCP, check the DHCP server configuration.
Erasing CTL and ITL files	Erasing CTL or ITL file.	None. This message is informational only. For more information about the CTL and ITL files, refer to *Cisco Unified Communications Manager Security Guide*.
Error update locale	One or more localization files could not be found in the TFTPPath directory or were not valid. The locale was not changed.	From Cisco Unified Operating System Administration, check that the following files are located within subdirectories in the TFTP File Management: • Located in subdirectory with same name as network locale: – tones.xml • Located in subdirectory with same name as user locale: – glyphs.xml – dictionary.xml – kate.xml

Table 10-2   Status Messages on the Cisco Unified IP Phone (continued)

Message	Description	Possible Explanation and Action
File not found <Cfg File>	The name-based and default configuration file was not found on the TFTP Server.	The configuration file for a phone is created when the phone is added to the Cisco Unified Communications Manager database. If the phone has not been added to the Cisco Unified Communications Manager database, the TFTP server generates a CFG File Not Found response. • Phone is not registered with Cisco Unified Communications Manager. You must manually add the phone to Cisco Unified Communications Manager if you are not allowing phones to auto-register. See the "Adding Phones with Cisco Unified Communications Manager Administration" section on page 2-12 for details. • If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. • If you are using static IP addresses, check configuration of the TFTP server. See the "Ethernet Setup Menu" section on page 7-4 for details on assigning a TFTP server.
File Not Found <CTLFile.tlv>	This message displays on the phone when the Cisco Unified Communications Manager cluster is not in secure mode.	No impact; the phone can still register to Cisco Unified Communications Manager.
IP address released	The phone has been configured to release its IP address.	The phone remains idle until it is power cycled or you reset the DHCP address. See the "Ethernet Setup Menu" section on page 7-4 for details.
ITL installed	The ITL file is installed in the phone.	None. This message is informational only. The ITL file was not installed previously. For more information about the ITL file, refer to *Cisco Unified Communications Manager Security Guide*.
Load rejected HC	The application that was downloaded is not compatible with the phone's hardware.	Occurs if you were attempting to install a version of software on this phone that did not support hardware changes on this newer phone. Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose **Device > Phone**). Re-enter the load displayed on the phone.
No default router	DHCP or static configuration did not specify a default router.	• If the phone has a static IP address, verify that the default router has been configured. See the "Ethernet Setup Menu" section on page 7-4 section for details. • If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.
No DNS server IP	A name was specified but DHCP or static IP configuration did not specify a DNS server address.	• If the phone has a static IP address, verify that the DNS server has been configured. See the "Ethernet Setup Menu" section on page 7-4 section for details. • If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.

Table 10-2   *Status Messages on the Cisco Unified IP Phone (continued)*

Message	Description	Possible Explanation and Action
No Trust List installed	The CTL file or the ITL file is not installed on the phone.	The Trust List is not configured on the Cisco Unified CM, which does not support security by default. For more information about the Trust List, refer to *Cisco Unified CM Security Guide*.
Restart requested by Cisco Unified Communications Manager	The phone is restarting based on a request from Cisco Unified Communications Manager.	Configuration changes have likely been made to the phone in Cisco Unified Communications Manager, and **Apply** has been pressed so that the changes take effect.
TFTP access error	TFTP server is pointing to a directory that does not exist.	• If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. • If you are using static IP addresses, check configuration of TFTP server. See the "Ethernet Setup Menu" section on page 7-4 for details on assigning a TFTP server.
TFTP error	The phone does not recognize an error code provided by the TFTP server.	Contact Cisco TAC.
TFTP timeout	TFTP server did not respond.	• Network is busy—The errors should resolve themselves when the network load reduces. • No network connectivity between the TFTP server and the phone—Verify the network connections. • TFTP server is down—Check configuration of TFTP server.
Timed Out	Supplicant attempted 802.1X transaction but timed out to due the absence of an authenticator.	Authentication typically times out if 802.1X is not configured on the switch.

Table 10-2   ***Status Messages on the Cisco Unified IP Phone (continued)***

Message	Description	Possible Explanation and Action
Trust List update failed	Updating CTL and ITL files failed.	Phone has CTL and ITL files installed and it failed to update the new CTL and ITL files.
		Possible reasons for failure:
		• Network failure.
		• TFTP server was down.
		• The new security token used to sign CTL file and the TFTP certificate used to sign ITL file are introduced, but are not available in the current CTL and ITL files in the phone.
		• Internal phone failure.
		Possible solutions:
		• Check the network connectivity.
		• Check if the TFTP server is active and functioning normally.
		• If the Transactional Vsam Services (TVS) server is supported on Cisco Unified CM, check if the TVS server is active and functioning normally.
		• Verify if the security token and the TFTP server are valid.
		Manually delete the CTL and ITL files if all the above solutions fail, and reset the phone.
Trust List updated	The CTL file, the ITL file, or both files are updated.	None. This message is informational only.
		For more information about the Trust List, refer to *Cisco Unified Communications Manager Security Guide*.
Version error	The name of the phone load file is incorrect.	Make sure that the phone load file has the correct name.
XmlDefault.cnf.xml, or .cnf.xml corresponding to the phone device name	Name of the configuration file.	None. This is an informational message indicating the name of the configuration file for the phone.

Ethernet Statistics Screen

The Ethernet Statistics screen displays information about the phone and network performance. Table 10-3 describes the information that appears in this screen.

To display the Ethernet Statistics screen, follow these steps:

Procedure

Step 1   Press the **Applications** button ⚙.

Step 2   Select **Administrator Settings.**

Step 3   Select **Status.**

Step 4   Select **Status > Ethernet Statistics.**

To reset the Rx Frames, Tx Frames, and Rx Broadcasts statistics to 0, press the **Clear** List softkey.

To exit the Ethernet Statistics screen, press the **Exit** softkey.

Table 10-3   Ethernet Statistics Message Information for the Cisco Unified IP Phone

Item	Description
Rx Frames	Number of packets received by the phone
Tx Frames	Number of packets sent by the phone
Rx Broadcasts	Number of broadcast packets received by the phone
Restart Cause—One of the following values: Initialized TCP-timeout CM-closed-TCP TCP-Bad-ACK CM-reset-TCP CM-aborted-TCP CM-NAKed KeepaliveTO Failback Phone-Keypad Phone-Re-IP Reset-Reset Reset-Restart Phone-Reg-Rej Load Rejected HC CM-ICMP-Unreach Phone-Abort	Cause of the last reset of the phone
Elapsed Time	Amount of time that has elapsed since the phone last rebooted.
Port 1	Link state and connection of the Network port (for example, `Auto 100 Mb Full-Duplex` means that the Network port is in a link-up state and has auto-negotiated a full-duplex, 100-Mbps connection)

Table 10-3   Ethernet Statistics Message Information for the Cisco Unified IP Phone (continued)

Item	Description
Port 2	Link state and connection of the PC port
IPv4	Information on the DHCP status. This includes the following states:
	CDP BOUND
	CDP INIT
	DHCP BOUND
	DHCP DISABLED
	DHCP INIT
	DHCP INVALID
	DHCP REBINDING
	DHCP REBOOT
	DHCP RENEWING
	DHCP REQUESTING
	DHCP RESYNC
	DHCP UNRECOGNIZED
	DHCP WAITING COLDBOOT TIMEOUT
	SET DHCP COLDBOOT
	SET DHCP DISABLED
	DISABLED DUPLICATE IP
	SET DHCP FAST

WLAN Statistics Screen

The WLAN Statistics screen displays statistics about the wireless Cisco Unified IP Phone 9971. Table 10-4 describes the information that appears in this screen.

To display the WLAN Statistics screen, follow these steps:

Procedure

Step 1   Press the **Applications** button ⚙.

Step 2   Select **Administrator Settings**.

Step 3   Select **Status.**

Step 4   Select **WLAN Statistics.**

To reset the WLAN statistics to 0, press the **Clear List** softkey.

To exit the WLAN Statistics screen, press the **Exit** softkey.

Table 10-4   WLAN Statistics on the Cisco Unified IP Phone

Item	Description
Transmit Frames	Number of packets transmitted by the phone.
Directed Frames Received	Number of directed packets received by the phone.
Multicast Frames Received	Number of multicast packets received by the phone.
Broadcast Frames Received	Number of broadcast packets received by the phone.
Receive Errors	Number of packets with errors received by the phone.
Receive No Buffers	The radio was unable to receive a packet, but had no buffers.
Frame Checksum (FCS) Errors	Increments when an FCS error is detected in a received MPDU.
Duplicate Frames	Number of duplicate packets received by the phone.
Fragments Received	Number of fragmented packets received by the phone.
Beacons Received	Number of beacons received by the phone.
Association Rejected	Number of AP association rejections received by the phone.
Association Timeouts	Number of AP association timeouts received by the phone.
Authentication Rejects	Number of authentication rejects received by the phone.
Authentication Timeouts	Number of authentication timeouts received by the phone.
QOS Null Frames	Number of QOS null packets received by the phone.
The following WLAN Statistics items display these AP queues: Background (BK), Best Effort (BE), Video (VI), and Voice (VO	
QOS Data Received	Number of QOS packets received by the phone.
Transmit Ok	Number of packets that the phone transmitted without error.
Transmit Errors	Number of packets with errors that the phone transmitted.
Direct Frames Transmitted	Number of direct packets transmitted by the phone.
Multicast Frames Transmitted	Number of multicast packets transmitted by the phone.
Broadcast Frames Transmitted	Number of broadcast packets transmitted by the phone.
RTS Failed	A corresponding CTS was not received.
ACK Failed	AP did not acknowledge a transmission.
Retries	Counter of total retries.
Multiple Retries	Transmission of packet required two or more retries prior to success.
Retry Failures	Transmission of packet failed.
Transmit Timeouts	Transmission of packet failed due to queue time.
Success Counter	Counter of successful transmissions.
Max Retry Failure	Counter of successive transmission failures that caused a roaming attempt.

Call Statistics Screen

You can access the Call Statistics screen (see Table 10-5) on the phone to display counters, statistics, and voice-quality metrics of the most recent call.

Note   You can also remotely view the call statistics information by using a web browser to access the Streaming Statistics web page. This web page contains additional RTCP statistics not available on the phone. For more information about remote monitoring, see *Chapter 11, "Monitoring the Cisco Unified IP Phone Remotely."*

A single call can have multiple voice streams, but data is captured for only the last voice stream. A voice stream is a packet stream between two endpoints. If one endpoint is put on hold, the voice stream stops even though the call is still connected. When the call resumes, a new voice packet stream begins, and the new call data overwrites the former call data.

To display the Call Statistics screen for information about the latest voice stream, follow these steps:

Procedure

Step 1   Press the **Applications** button.

Step 2   Select **Administrator Settings**.

Step 3   Select **Status**.

Step 4   Select **Call Statistics**.

The Call Statistics screen displays these items:

Table 10-5   Call Statistics Items for the Cisco Unified Phone

Item	Description
Rcvr Codec	Type of voice stream received (RTP streaming audio from codec): G.729, G.722, G.711 u-law, G.711 A-law, and iLBC.
Sender Codec	Type of voice stream transmitted (RTP streaming audio from codec): G.729, G.722, G.711 u-law, G.711 A-law, and iLBC.
Rcvr Size	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).
Sender Size	Size of voice packets, in milliseconds, in the transmitting voice stream.
Rcvr Packets	Number of RTP voice packets received since voice stream was opened. **Note** This number is not necessarily identical to the number of RTP voice packets received since the call began because the call might have been placed on hold.
Sender Packets	Number of RTP voice packets transmitted since voice stream was opened. **Note** This number is not necessarily identical to the number of RTP voice packets transmitted since the call began because the call might have been placed on hold.

Table 10-5   Call Statistics Items for the Cisco Unified Phone (continued)

Item	Description
Avg Jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network), in milliseconds, observed since the receiving voice stream was opened.
Max Jitter	Maximum jitter, in milliseconds, observed since the receiving voice stream was opened.
Rcvr Discarded	Number of RTP packets in the receiving voice stream that have been discarded (bad packets, too late, and so on). **Note** The phone will discard payload type 19 comfort noise packets that are generated by Cisco Gateways, which will increment this counter.
Rcvr Lost Packets	Missing RTP packets (lost in transit).
Voice-Quality Metrics	
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding eight-second interval of the voice stream. For more information, see the "Monitoring the Voice Quality of Calls" section on page 12-16. **Note** The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score observed from start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 gives 4.5 • G.729 A /AB gives 3.7
MOS LQK Version	Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).

Table 10-5   Call Statistics Items for the Cisco Unified Phone (continued)

Item	Description
Severely Conceal Secs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.

Video Statistics Screen

You can access the Video Statistics screen (see Table 10-5) on the phone to display counters, statistics of the most recent call.

✎
Note   You can also remotely view the video statistics information by using a web browser to access the Streaming Statistics web page. This web page contains additional RTCP statistics not available on the phone. For more information about remote monitoring, see Chapter 11, "Monitoring the Cisco Unified IP Phone Remotely."

A video stream is a frame stream between two endpoints. If one endpoint pauses the video streaming, the video stream stops even though the call is still connected. When the video streaming resumes, a new video frame stream begins, and the new video data overwrites the former video data.

To display the Video Statistics screen for information about the latest video stream, follow these steps:

Procedure

Step 1   Press the **Applications** button.

Step 2   Select **Administrator Settings**.

Step 3   Select **Call Statistics**.

Step 4   Select **Video**.

The Video Statistics screen displays these items (Table 10-6):

Table 10-6   Video Statistics Items for the Cisco Unified Phone

Item	Description
Rcvr Codec	Type of video stream received (RTP streaming video from codec)
Sender Codec	Type of video stream transmitted (RTP streaming video from codec)
Rcvr Packets	Number of RTP video packets received since video stream was opened **Note** This number is not necessarily identical to the number of RTP video packets received since the call began because the call might have been placed on hold.

Table 10-6   *Video Statistics Items for the Cisco Unified Phone (continued)*

Item	Description
Sender Packets	Number of RTP video packets transmitted since video stream was opened. **Note** This number is not necessarily identical to the number of RTP video packets transmitted since the call began because the call might have been placed on hold.
Avg Jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network), in milliseconds, observed since the receiving video stream was opened.
Max Jitter	Maximum jitter, in milliseconds, observed since the receiving video stream was opened.
Rcvr Discarded	Number of RTP packets in the receiving video stream that have been discarded (bad packets, too late, and so on)
Rcvr Lost Packets	Missing RTP video packets (lost in transit)
Rcvr Size	Size of video frames, in milliseconds, in the receiving video stream (RTP streaming video).
Sender Size	Size of video frames, in milliseconds, in the transmitting video stream.
Sender Frames	Number of video frames transmitted by the camera/phone since the video stream was opened.
Sender Partial Frames	Number of P-frames sent by the camera, since the video stream was opened.
Sender IFrames	Number of I-frames sent by the camera, since the video stream was opened.
Sender Frame Rate	Rate at which video frames are transmitted. (Frames per second).
Sender Bandwidth	Bandwidth of the video steam that is being transmitted, in kbps (kilo bits per second).
Sender Resolution	Resolution of the video stream transmitted by the camera. VGA(640x480), CIF (352x288), QCIF (176x144)
Rcvr Frames	Number of video frames received by the phone since the video stream was opened.
Rcvr Partial Frames	Number of P-frames received by the phone, since the video stream was opened.
Rcvr IFrames	Number of I-frames received by the phone, since the video stream was opened.
Rcvr IFrames Req	Number of times IDR requests sent by the phone to the remote end point, since the video stream was opened.
Rcvr Frame Rate	Rate at which video frames are received. (Frames per second).
Rcvr Frame Errors	Number of errors reported by video decoder, since the video stream was opened.
Rcvr Bandwidth	Bandwidth of the video steam that is being received, in kbps (kilo bits per second).

Table 10-6   Video Statistics Items for the Cisco Unified Phone (continued)

Item	Description
Rcvr Resolution	Resolution of the video stream received by the phone from the remote end point. VGA(640x480), CIF (352x288), QCIF (176x144), etc.
Sender Start Time	Timestamp indicating when the first RTP packet is sent to the network.
Rcvr Start Time	Timestamp indicating when the first RTP packet is received from the network.
Latency	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.

Current Access Point Screen

The Current Access Point screen displays statistics about the current access point on the wireless Cisco Unified IP Phone 9971. Table 10-7 describes the information that appears in this screen.

To display the Current Access Point screen, follow these steps:

Procedure

Step 1   Press the **Applications** button.

Step 2   Select **Administrator Settings**.

Step 3   Select **Status.**

Step 4   Select **Current Access Point.**

To exit the Current Access Point screen, press the **Exit** softkey.

Table 10-7   Current Access Point on the Cisco Unified IP Phone 9971

Item	Description
AP Name	Name of the AP if it is CCX-compliant; otherwise the MAC address is displayed here.
MAC Address	MAC address of the AP.
Frequency	The latest frequency where this AP was observed.
Last RSSI	The latest RSSI in which this AP was observed.
Beacon Interval	Number of time units between beacons. A time unit is 1.024 ms.
Capability	This field contains a number of subfields that are used to indicate requested or advertised optional capabilities.
Basic Rates	Data rates required by the AP at which the station must be capable of operating.
Optional Rates	Data rates supported by the AP that are optional for the station to operate at.
Current Channel	The latest channel where this AP was observed.

Table 10-7   Current Access Point on the Cisco Unified IP Phone 9971 (continued)

Item	Description
dtime Period	Every *nth* beacon is a dtime period. After each DTIM beacon, the AP would send any broadcast or multicast packets that may have been queued for power-save devices.
Country Code	A two-digit country code. Country information might not be displayed if the country information element (IE) is not present in the beacon.
Channels	A list of supported channels (from the country IE).
Power Constraint	The amount of power by which the maximum transmit power should be reduced from the regulatory domain's limit.
Power Limit	Maximum transmit power in dBm permitted for that channel.
Channel Utilization	The percentage of time, normalized to 255, in which the AP sensed the medium was busy, as indicated by the physical or virtual carrier sense (CS) mechanism.
Station Count	Data rates required by the AP at which the station must be capable of operating.
Admission Capacity	An unsigned integer that specifies the remaining amount of medium time available through explicit admission control, in units of 32 µs/s.

If the value is 0, the AP does not support this information element and the capacity is unknown. |
WMM Supported	Support for Wi-Fi multi-media extensions.
UAPSD Supported	Unscheduled Automatic Power Save Delivery is supported by the AP. May only be available if WMM is supported. This feature is critical to talk time and achieving maximum call density on the wireless IP phone.
Proxy ARP	CCX compliant AP supports responding to IP ARP requests on behalf of the associated station. This feature is critical to standby time on the wireless IP phone.
CCX Version	Version of CCX if the AP is CCX compliant.

C H A P T E R **11**

Monitoring the Cisco Unified IP Phone Remotely

Each Cisco Unified IP Phone has a web page from which you can view a variety of information about the phone, including:

- Device information
- Network setup information
- Network statistics
- Device logs
- Streaming statistics

This chapter describes the information that you can obtain from the phone's web page. You can use this information to remotely monitor the operation of a phone and to assist with troubleshooting.

You can also obtain much of this information directly from a phone. For more information, see Chapter 10, "Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone."

For more information about troubleshooting the Cisco Unified IP Phone, Chapter 12, "Troubleshooting and Maintenance."

This chapter includes these topics:

Accessing the Web Page for a Phone

To access the web page for a Cisco Unified IP Phone, perform these steps.

> **Note** If you cannot access the web page, it may be disabled (it is disabled by default). See the "Enabling and Disabling Web Page Access" section on page 11-3 for more information.

Procedure

Step 1 Obtain the IP address of the Cisco Unified IP Phone using one of these methods:

- Search for the phone in Cisco Unified Communications Manager Administration by choosing **Device > Phone**. Phones registered with Cisco Unified Communications Manager display the IP address on the Find and List Phones window and at the top of the Phone Configuration window.

- On the Cisco Unified IP Phone, press the **Applications** button, choose **Administrator Settings > Network Setup > Ethernet Setup** > **IPv4 Setup**, and then scroll to the IP Address option.

Step 2 Open a web browser and enter the following URL, where *IP_address* is the IP address of the Cisco Unified IP Phone:

http://<IP_address> or https://<IP_address> (depending on the protocol supported by the Cisco Unified IP Phone)

The web page for a Cisco Unified IP Phone includes these topics:

- **Device Information**—Displays device settings and related information for the phone. For more information, see the "Device Information" section on page 11-4.

- **Network Setup**—Displays network setup information and information about other phone settings. For more information, see the "Network Setup" section on page 11-5.

- **Network Statistics**—Includes the following hyperlinks, which provide information about network traffic:

  - **Ethernet Information**—Displays information about Ethernet traffic. For more information, see the "Network Statistics" section on page 11-8.

  - **Access**—Displays information about network traffic to and from the PC port on the phone. For more information, see the "Network Statistics" section on page 11-8.

  - **Network**—Displays information about network traffic to and from the network port on the phone. For more information, see the "Network Statistics" section on page 11-8.

- **Device Logs**—Includes the following hyperlinks, which provide information that you can use for troubleshooting:

  - **Console Logs**—Includes hyperlinks to individual log files. For more information, see the "Device Logs" section on page 11-11.

  - **Core Dumps**—Includes hyperlinks to individual dump files. For more information, see the "Device Logs" section on page 11-11.

- **Status Messages**—Displays up to the 10 most recent status messages that the phone has generated since it was last powered up. For more information, see the "Device Logs" section on page 11-11.

- **Debug Display**—Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting. For more information, see the "Device Logs" section on page 11-11.

- **Streaming Statistics**—Includes the **Audio and Video statistics, Stream 1**, **Stream 2**, **Stream 3**, **Stream 4**, **Stream 5** and **Stream 6** hyperlinks, which display a variety of streaming statistics. For more information, see the "Streaming Statistics" section on page 11-11.

Enabling and Disabling Web Page Access

For security purposes, access to the web pages for a phone is disabled by default. This prevents access to the web pages that are described in this chapter and to the Cisco Unified Communications Manager User Options web pages.

To enable access to the web pages for a phone, follow these steps from Cisco Unified Communications Manager Administration.

Procedure

Step 1   Choose **Device > Phone**.

Step 2   Specify the criteria to find the phone and click **Find**, or click **Find** to display a list of all phones.

Step 3   Click the device name to open the Phone Configuration window for the device.

Step 4   Scroll down to the Product Specific Configuration section. From the Web Access drop-down list, choose **Enabled**.

Step 5   Click **Apply Config**.

> **Note**   Some features, such as Cisco Quality Report Tool, do not function properly without access to the phone web pages. Disabling web access also affects any serviceability application that relies on web access, such as CiscoWorks.

To disable web page access if it has been enabled, see the preceding steps about enabling access. Follow the same steps, but choose **Disabled** in Step 4 to disable the web page.

Configuring the Cisco Unified IP Phone to use HTTP/HTTPS Protocols

The Cisco Unified IP Phone can be configured to use:

- HTTPS protocol only
- HTTP or HTTPS protocols

If your Cisco Unified IP Phone is configured to use the HTTP or HTTPS protocols (the second case above), use *http://<IP_address> or https://<IP_address>* for the phone's web access.

Device Information

The Device Information area on a phone's web page displays device settings and related information for the phone. Table 11-1 describes these items.

Note Some of the items in Table 11-1 do not apply to all phone models.

To display the Device Information area, access the web page for the phone as described in the "Accessing the Web Page for a Phone" section on page 11-2, and then click the **Device Information** hyperlink.

Table 11-1   Device Information Area Items

Item	Description
MAC Address	Media Access Control (MAC) address of the phone
Host Name	Unique, fixed name that is automatically assigned to the phone based on its MAC address
Phone DN	Directory number assigned to the phone
Version	Identifier of the firmware running on the phone
Key Expansion Module 1	Identifier for the first KEM, if applicable.
Key Expansion Module 2	Identifier for the second KEM, if applicable.
Key Expansion Module 3	Identifier for the third KEM, if applicable.
Hardware Revision	Revision value of the phone hardware
Serial Number	Unique serial number of the phone
Model Number	Model number of the phone
Message Waiting	Indicates if there is a voice message waiting on the primary line for this phone.
UDI	Displays the following Cisco Unique Device Identifier (UDI) information about the phone: • Device Type—Indicates hardware type. For example, phone displays for all phone models • Device Description—Displays the name of the phone associated with the indicated model type • Product Identifier—Specifies the phone model • Serial Number—Displays the unique serial number of the phone.
Key Expansion Module UDI	Cisco Unique Device Identifier (UDI) of the KEM.
Time	Time obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs
Time Zone	Time zone obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs
Date	Date obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs

Network Setup

The Network Setup area on a phone's web page displays network setup information and information about other phone settings. Table 11-2 describes these items.

You can view and set many of these items from the Network Setup menu on the Cisco Unified IP Phone. For more information, see Chapter 7, "Configuring Settings on the Cisco Unified IP Phone."

To display the Network Setup area, access the web page for the phone as described in the "Accessing the Web Page for a Phone" section on page 11-2, and then click the **Network Setup** hyperlink.

Table 11-2   Network Setup Items

Item	Description
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address.
BOOTP Server	Indicates whether the phone obtains its configuration from a Bootstrap Protocol (BootP) server.
MAC Address	Media Access Control (MAC) address of the phone.
Host Name	Host name that the DHCP server assigned to the phone.
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.
IP Address	Internet Protocol (IP) address of the phone.
Subnet Mask	Subnet mask used by the phone.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone.
TFTP Server 2	Backup Trivial File Transfer Protocol (TFTP) server used by the phone.
Default Router 1	Default router used by the phone.
DNS Server 1–3	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–3) used by the phone.
Operational VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member.
Admin. VLAN ID	Auxiliary VLAN in which the phone is a member.

Table 11-2   *Network Setup Items (continued)*

Item	Description
CUCM Server 1–5	Host names or IP addresses, in prioritized order, of the Cisco Unified Communications Manager servers with which the phone can register. An item can also show the IP address of an SRST router that is capable of providing limited Cisco Unified Communications Manager functionality, if such a router is available. For an available server, an item will show the Cisco Unified Communications Manager server IP address and one of the following states: • Active—Cisco Unified Communications Manager server from which the phone is currently receiving call-processing services. • Standby—Cisco Unified Communications Manager server to which the phone switches if the current server becomes unavailable. • Blank—No current connection to this Cisco Unified Communications Manager server. An item may also include the Survivable Remote Site Telephony (SRST) designation, which identifies an SRST router capable of providing Cisco Unified Communications Manager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communications Manager always appears last in the list of servers, even if it is active. You configure the SRST router address in the Device Pool section in Cisco Unified Communications Manager Configuration window.
Information URL	URL of the help text that appears on the phone.
Directories URL	URL of the server from which the phone obtains directory information.
Messages URL	URL of the server from which the phone obtains message services.
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.
DHCP Enabled	Indicates whether DHCP is being used by the phone.
DHCP Address Released	Indicates the setting of the DHCP Address Released option on the phone's Network Configuration menu.
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.
Idle URL	URL that the phone displays when the phone has not been used for the time specified by Idle URL Time, and no menu is open.
Idle URL Time	Number of seconds that the phone has not been used and no menu is open before the XML service specified by Idle URL is activated.
Proxy Server URL	URL of proxy server, which makes HTTP requests to non-local host addresses on behalf of the phone HTTP client and provides responses from the non-local host to the phone HTTP client.
Authentication URL	URL that the phone uses to validate requests made to the phone web server.

Table 11-2   *Network Setup Items (continued)*

Item	Description
SW Port Setup	Speed and duplex of the switch port, where: • A—Auto Negotiate • 10H—10-BaseT/half duplex • 10F—10-BaseT/full duplex • 100H—100-BaseT/half duplex • 100F—100-BaseT/full duplex • 1000F—1000-BaseT/full duplex • No Link—No connection to the switch port
PC Port Setup	Speed and duplex of the switch port, where: • A—Auto Negotiate • 10H—10-BaseT/half duplex • 10F—10-BaseT/full duplex • 100H—100-BaseT/half duplex • 100F—100-BaseT/full duplex • 1000F—1000-BaseT/full duplex • No Link—No connection to the PC port
TFTP Server 2	Backup TFTP server that the phone uses if the primary TFTP server is unavailable.
User Locale	User locale associated with the phone user. Identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
Network Locale	Network locale associated with the phone user. Identifies a set of detailed information to support the phone in a specific location, including definitions of the tones and cadences used by the phone.
Headset Enabled	Indicates whether the Headset button is enabled on the phone.
User Locale Version	Version of the user locale loaded on the phone.
Network Locale Version	Version of the network locale loaded on the phone.
PC Port Disabled	Indicates whether the PC port on the phone is enabled or disabled.
Speaker Enabled	Indicates whether the speakerphone is enabled on the phone.
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.
Video Capability Enabled	Indicates whether the phone can participate in video calls when connected to an appropriately equipped camera.
Voice VLAN Enabled	Indicates whether the phone allows a device attached to the PC port to access the Voice VLAN.
DSCP for Call Control	DSCP IP classification for call control signaling.
DSCP for Configuration	DSCP IP classification for any phone configuration transfer.
DSCP for Services	DSCP IP classification for phone-based services.
Security Mode	Displays the security mode that is set for the phone.
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.

Table 11-2   Network Setup Items (continued)

Item	Description
Span to PC Port	Indicates whether the phone will forward packets transmitted and received on the network port to the access port.
PC VLAN	VLAN used to identify and remove 802.1P/Q tags from packets sent to the PC.
CDP on PC Port	Indicates whether CDP is supported on the PC port (default is enabled).
	When CDP is disabled in Cisco Unified Communications Manager, a warning is displayed, indicating that disabling CDP on the PC port prevents CVTA from working.
	The current PC and switch port CDP values are shown on the Settings menu.
CDP on SW Port	Indicates whether CDP is supported on the switch port (default is enabled).
	Enable CDP on the switch port for VLAN assignment for the phone, power negotiation, QoS management, and 802.1x security.
	Enable CDP on the switch port when the phone is connected to a Cisco switch.
	When CDP is disabled in Cisco Unified Communications Manager, a warning is presented, indicating that CDP should be disabled on the switch port only if the phone is connected to a non-Cisco switch.
	The current PC and switch port CDP values are shown on the Settings menu.
LLDP-MED: SW Port	Indicates whether Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is enabled on the switch port.
LLDP: PC Port	Indicates whether Link Layer Discovery Protocol (LLDP) is enabled on the PC port.
LLDP Power Priority	Advertises the phone's power priority to the switch, enabling the switch to appropriately provide power to the phones. Settings include: • Unknown—Default • Low • High • Critical
LLDP Asset ID	Identifies the asset ID assigned to the phone for inventory management

Network Statistics

The following network statistics hyperlinks on a phone's web page provide information about network traffic on the phone. To display a network statistics area, access the web page for the phone as described in the "Accessing the Web Page for a Phone" section on page 11-2.

- Ethernet Information—Displays information about Ethernet traffic. Table 11-3 describes the items in this area.

- Access area—Displays information about network traffic to and from the PC port on the phone. Table 11-4 describes the items in this area.

- Network area—Displays information about network traffic to and from the network port on the phone. Table 11-4 describes the items in this area.

To display a network statistics area, access the web page for the phone as described in the "Accessing the Web Page for a Phone" section on page 11-2, and then click the **Ethernet Information**, the **Access**, or the **Network** hyperlink.

Table 11-3   Ethernet Information Items

Item	Description
Tx Frames	Total number of packets transmitted by the phone
Tx broadcast	Total number of broadcast packets transmitted by the phone
Tx multicast	Total number of multicast packets transmitted by the phone
Tx unicast	Total number of unicast packets transmitted by the phone
Rx Frames	Total number of packets received by the phone
Rx broadcast	Total number of broadcast packets received by the phone
Rx multicast	Total number of multicast packets received by the phone
Rx unicast	Total number of unicast packets received by the phone
Rx PacketNoDes	Total number of shed packets caused by no Direct Memory Access (DMA) descriptor

Table 11-4   Access Area and Network Area Items

Item	Description
Rx totalPkt	Total number of packets received by the phone
Rx crcErr	Total number of packets received with CRC failed
Rx alignErr	Total number of packets received between 64 and 1522 bytes in length that have a bad Frame Check Sequence (FCS)
Rx multicast	Total number of multicast packets received by the phone
Rx broadcast	Total number of broadcast packets received by the phone
Rx unicast	Total number of unicast packets received by the phone
Rx shortErr	Total number of FCS error packets or Align error packets received that are less than 64 bytes in size
Rx shortGood	Total number of good packets received that are less than 64 bytes size
Rx longGood	Total number of good packets received that are greater than 1522 bytes in size
Rx longErr	Total number of FCS error packets or Align error packets received that are greater than 1522 bytes in size
Rx size64	Total number of packets received, including bad packets, that are between 0 and 64 bytes in size
Rx size65to127	Total number of packets received, including bad packets, that are between 65 and 127 bytes in size
Rx size128to255	Total number of packets received, including bad packets, that are between 128 and 255 bytes in size
Rx size256to511	Total number of packets received, including bad packets, that are between 256 and 511 bytes in size

Table 11-4   *Access Area and Network Area Items (continued)*

Item	Description
Rx size512to1023	Total number of packets received, including bad packets, that are between 512 and 1023 bytes in size
Rx size1024to1518	Total number of packets received, including bad packets, that are between 1024 and 1518 bytes in size
Rx tokenDrop	Total number of packets dropped due to lack of resources (for example, FIFO overflow)
Tx excessDefer	Total number of packets delayed from transmitting due to medium being busy
Tx lateCollision	Number of times that collisions occurred later than 512 bit times after the start of packet transmission
Tx totalGoodPkt	Total number of good packets (multicast, broadcast, and unicast) received by the phone
Tx Collisions	Total number of collisions that occurred while a packet was being transmitted
Tx excessLength	Total number of packets not transmitted because the packet experienced 16 transmission attempts
Tx broadcast	Total number of broadcast packets transmitted by the phone
Tx multicast	Total number of multicast packets transmitted by the phone
LLDP FramesOutTotal	Total number of LLDP frames sent out from the phone
LLDP AgeoutsTotal	Total number of LLDP frames that have been time out in cache
LLDP FramesDiscardedTotal	Total number of LLDP frames that are discarded when any of the mandatory TLVs is missing or out of order or contains out of range string length
LLDP FramesInErrorsTotal	Total number of LLDP frames that received with one or more detectable errors
LLDP FramesInTotal	Total number of LLDP frames received on the phone.
LLDP TLVDiscardedTotal	Total number of LLDP TLVs that are discarded
LLDP TLVUnrecognizedTotal	Total number of LLDP TLVs that are not recognized on the phone
CDP Neighbor Device ID	Identifier of a device connected to this port discovered by CDP protocol
CDP Neighbor IP Address	IP address of the neighbor device discovered by CDP protocol
CDP Neighbor Port	Neighbor device port to which the phone is connected discovered by CDP protocol
LLDP Neighbor Device ID	Identifier of a device connected to this port discovered by LLDP protocol
LLDP Neighbor IP Address	IP address of the neighbor device discovered by LLDP protocol
LLDP Neighbor Port	Neighbor device port to which the phone is connected discovered by LLDP protocol
Port Information	Speed and duplex information

Device Logs

The following device logs hyperlinks on a phone's web page provide information you can use to help monitor and troubleshoot the phone. To access a device log area, access the web page for the phone as described in the "Accessing the Web Page for a Phone" section on page 11-2.

- Console Logs—Includes hyperlinks to individual log files. The console log files include debug and error messages received on the phone.

- Core Dumps—Includes hyperlinks to individual dump files. The core dump files include data from a phone crash.

- Status Messages—Displays up to the 10 most recent status messages that the phone has generated since it was last powered up. You can also see this information from the Status Messages screen on the phone. Table 10-2 describes the status messages that can appear.

- Debug Display—Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting.

Streaming Statistics

A Cisco Unified IP Phone can stream information to and from up to three devices simultaneously. A phone streams information when it is on a a call or running a service that sends or receives audio or data.

The streaming statistics areas on a phone's web page provide information about the streams.

To display a Streaming Statistics area, access the web page for the phone as described in the "Accessing the Web Page for a Phone" section on page 11-2, and then click a **Stream** hyperlink.

Table 11-5 describes the items in the Streaming Statistics areas.

Table 11-5   ***Streaming Statistics Area Items***

Item	Description
Remote Address	IP address and UDP port of the destination of the stream.
Local Address	IP address and UPD port of the phone.
Start Time	Internal time stamp indicating when Cisco Unified Communications Manager requested that the phone start transmitting packets.
Stream Status	Indication of whether streaming is active or not.
Host Name	Unique, fixed name that is automatically assigned to the phone based on its MAC address.
Sender Packets	Total number of RTP data packets transmitted by the phone since starting this connection. The value is 0 if the connection is set to receive only mode.
Sender Octets	Total number of payload octets transmitted in RTP data packets by the phone since starting this connection. The value is 0 if the connection is set to receive only mode.
Sender Codec	Type of audio encoding used for the transmitted stream.
Sender Reports Sent[1]	Number of times the RTCP Sender Report have been sent.
Sender Report Time Sent[1]	Internal time stamp indication when the last RTCP Sender Report was sent.
Rcvr Lost Packets	Total number of RTP data packets that have been lost since starting receiving data on this connection. Defined as the number of expected packets less the number of packets actually received, where the number of received packets includes any that are late or duplicate. The value displays as 0 if the connection was set to send-only mode.

Table 11-5   Streaming Statistics Area Items (continued)

Item	Description
Avg Jitter	Estimate of mean deviation of the RTP data packet inter-arrival time, measured in milliseconds. The value displays as 0 if the connection was set to send-only mode.
Rcvr Codec	Type of audio encoding used for the received stream.
Rcvr Reports Sent[1]	Number of times the RTCP Receiver Reports have been sent.
Rcvr Report Time Sent[1]	Internal time stamp indication when a RTCP Receiver Report was sent.
Rcvr Packets	Total number of RTP data packets received by the phone since starting receiving data on this connection. Includes packets received from different sources if this is a multicast call. The value displays as 0 if the connection was set to send-only mode.
Rcvr Octets	Total number of payload octets received in RTP data packets by the device since starting reception on the connection. Includes packets received from different sources if this is a multicast call. The value displays as 0 if the connection was set to send-only mode.
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate three seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding eight-second interval of the voice stream. For more information, see the "Monitoring the Voice Quality of Calls" section on page 12-16. **Note** The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score observed from start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 gives 4.5 • G.729 A /AB gives 3.7
MOS LQK Version	Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than five percent concealment events (lost frames) from the start of the voice stream.
Latency[1]	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.
Max Jitter	Maximum value of instantaneous jitter, in milliseconds.
Sender Size	RTP packet size, in milliseconds, for the transmitted stream.
Sender Reports Received[1]	Number of times RTCP Sender Reports have been received.

Table 11-5   ***Streaming Statistics Area Items (continued)***

Item	Description
Sender Report Time Received[1]	Last time at which an RTCP Sender Report was received.
Rcvr Size	RTP packet size, in milliseconds, for the received stream.
Rcvr Discarded	RTP packets received from network but discarded from jitter buffers.
Rcvr Reports Received[1]	Number of times RTCP Receiver Reports have been received.
Rcvr Report Time Received[1]	Last time at which an RTCP Receiver Report was received.
Voice Quality Metrics	
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding three-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than five percent concealment events (lost frames) from the start of the voice stream.

1. When the RTP Control Protocol is disabled, no data generates for this field and thus displays as 0.

Related Topics

"Configuring Settings on the Cisco Unified IP Phone" chapter

Troubleshooting and Maintenance

This chapter provides information that can assist you in troubleshooting problems with your Cisco Unified IP Phone or with your IP telephony network. It also explains how to clean and maintain your phone.

If you need additional assistance to resolve an issue, see the "Obtaining Documentation, Obtaining Support, and Security Guidelines" section on page xiii.

This chapter includes these topics:

Resolving Startup Problems

After installing a Cisco Unified IP Phone into your network and adding it to Cisco Unified Communications Manager, the phone should start up as described in the "Verifying the Phone Startup Process" section on page 3-21. If the phone does not start up properly, see the following sections for troubleshooting information:

Symptom: The Cisco Unified IP Phone Does Not Go Through its Normal Startup Process

When you connect a Cisco Unified IP Phone into the network port, the phone should go through its normal startup process as described in "Verifying the Phone Startup Process" section on page 3-21 and the phone screen should display information. If the phone does not go through the startup process, the cause may be faulty cables, bad connections, network outages, lack of power, and so on. Or, the phone may not be functional.

To determine whether the phone is functional, follow these suggestions to systematically eliminate these other potential problems:

1. Verify that the network port is functional:
   – Exchange the Ethernet cables with cables that you know are functional.
   – Disconnect a functioning Cisco Unified IP Phone from another port and connect it to this network port to verify the port is active.
   – Connect the Cisco Unified IP Phone that will not start up to a different network port that is known to be good.
   – Connect the Cisco Unified IP Phone that will not start up directly to the port on the switch, eliminating the patch panel connection in the office.

2. Verify that the phone is receiving power:
   – If you are using external power, verify that the electrical outlet is functional.
   – If you are using in-line power, use the external power supply instead.
   – If you are using the external power supply, switch with a unit that you know to be functional.

3. If the phone still does not start up properly, power up the phone with the handset off-hook. When the phone is powered up in this way, it attempts to launch a backup software image.

4. If the phone still does not start up properly, perform a factory reset of the phone. For instructions, see the "Monitoring the Voice Quality of Calls" section on page 12-16.

If after attempting these solutions, the phone screen on the Cisco Unified IP Phone does not display any characters after at least five minutes, contact a Cisco technical support representative for additional assistance.

Symptom: The Cisco Unified IP Phone Does Not Register with Cisco Unified Communications Manager

If the phone proceeds past the first stage of the startup process (LED buttons flashing on and off) but continues to cycle through the messages displaying on the phone screen, the phone is not starting up properly. The phone cannot successfully start up unless it is connected to the Ethernet network and it has registered with a Cisco Unified Communications Manager server.

These sections can assist you in determining the reason the phone is unable to start up properly:

- Identifying Error Messages, page 12-3
- Checking Network Connectivity, page 12-3
- Verifying TFTP Server Settings, page 12-3
- Verifying IP Addressing and Routing, page 12-3

- Verifying DNS Settings, page 12-4
- Cisco CallManager and TFTP Services Are Not Running, page 12-4
- Creating a New Configuration File, page 12-5
- Checking Network Connectivity, page 12-3

In addition, problems with security may prevent the phone from starting up properly. See the "General Troubleshooting Tips" section on page 12-10 for more information.

Identifying Error Messages

As the phone cycles through the startup process, you can access status messages that might provide you with information about the cause of a problem. See the "Status Messages Screen" section on page 10-3 for instructions about accessing status messages and for a list of potential errors, their explanations, and their solutions.

Checking Network Connectivity

If the network is down between the phone and the TFTP server or Cisco Unified Communications Manager, the phone cannot start up properly. Ensure that the network is currently running.

Verifying TFTP Server Settings

You can determine the IP address of the TFTP server used by the phone by pressing the **Applications** button, then selecting **Administrator Settings > Network Setup > Ethernet Setup > IPv4 Setup > TFTP Server 1**.

If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option. See the "Ethernet Setup Menu" section on page 7-4.

If you are using DHCP, the phone obtains the address for the TFTP server from the DHCP server. Check the IP address configured in Option 150.

You can also enable the phone to use an alternate TFTP server. Such a setting is particularly useful if the phone was recently moved from one location to another. See the "Ethernet Setup Menu" section on page 7-4 for instructions.

Verifying IP Addressing and Routing

You should verify the IP addressing and routing settings on the phone. If you are using DHCP, the DHCP server should provide these values. If you have assigned a static IP address to the phone, you must enter these values manually.

On the Cisco Unified IP Phone, press the **Applications** button, then select **Administrator Settings > Network Setup > Ethernet Setup > IPv4 Setup**, and look at the following options:

- DHCP Server—If you have assigned a static IP address to the phone, you do not need to enter a value for the DHCP Server option. However, if you are using a DHCP server, this option must have a value. If it does not, check your IP routing and VLAN configuration. Refer to the *Troubleshooting Switch Port and Interface Problems* document, available at this URL:
  http://www.cisco.com/en/US/customer/products/hw/switches/ps700/products_tech_note09186a008015bfd6.shtml

- IP Address, Subnet Mask, Default Router—If you have assigned a static IP address to the phone, you must manually enter settings for these options. See the "Ethernet Setup Menu" section on page 7-4 for instructions.

If you are using DHCP, check the IP addresses distributed by your DHCP server. Refer to the *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* document, available at this URL:
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

Verifying DNS Settings

If you are using DNS to refer to the TFTP server or to Cisco Unified Communications Manager, you must ensure that you have specified a DNS server. Verify this setting by pressing the **Applications** button, then selecting **Administrator Settings > Network Setup > Ethernet Setup > IPv4 Setup > DNS Server 1**. You should also verify that there is a CNAME entry in the DNS server for the TFTP server and for the Cisco Unified Communications Manager system.

You must also ensure that DNS is configured to do reverse look-ups.

Cisco CallManager and TFTP Services Are Not Running

If the Cisco CallManager or TFTP services are not running, phones may not be able to start up properly. However, in such a situation, it is likely that you are experiencing a system-wide failure, and other phones and devices are unable to start up properly.

If the Cisco CallManager service is not running, all devices on the network that rely on it to make phone calls will be affected. If the TFTP service is not running, many devices will not be able to start up successfully.

To start a service, follow these steps:

Procedure

Step 1   From Cisco Unified Communications Manager Administration, choose **Cisco Unified Serviceability** from the Navigation drop-down list and click **Go**.

Step 2   Choose **Tools > Control Center - Feature Services**.

Step 3   Choose the primary Cisco Unified Communications Manager server from the Server drop-down list.

The window displays the service names for the server that you chose, the status of the services, and a service control panel to start or stop a service.

Step 4   If a service has stopped, click its radio button and then click the **Start** button.

The Service Status symbol changes from a square to an arrow.

Note   A service must be activated before it can be started or stopped. To activate a service, choose **Tools > Service Activation**.

Creating a New Configuration File

If you continue to have problems with a particular phone that other suggestions in this chapter do not resolve, the configuration file may be corrupted.

To create a new configuration file, follow these steps:

Procedure

Step 1   From Cisco Unified Communications Manager, choose **Device > Phone > Find** to locate the phone experiencing problems.

Step 2   Choose **Delete** to remove the phone from the Cisco Unified Communications Manager database.

Step 3   Add the phone back to the Cisco Unified Communications Manager database. See the "Adding Phones to the Cisco Unified Communications Manager Database" section on page 2-9 for details.

Step 4   Power cycle the phone.

Note
- When you remove a phone from the Cisco Unified Communications Manager database, its configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone's directory number or numbers remain in the Cisco Unified Communications Manager database. They are called "unassigned DNs" and can be used for other devices. If unassigned DNs are not used by other devices, delete them from the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers. Refer to *Cisco Unified Communications Manager Administration Guide* for more information.

- Changing the buttons on a phone button template, or assigning a different phone button template to a phone, may result in directory numbers that are no longer accessible from the phone. The directory numbers are still assigned to the phone in the Cisco Unified Communications Manager database, but there is no button on the phone with which calls can be answered. These directory numbers should be removed from the phone and deleted if necessary.

Registering the Phone with Cisco Unified Communications Manager

A Cisco Unified IP Phone can register with a Cisco Unified Communications Manager server only if the phone has been added to the server or if auto-registration is enabled. Review the information and procedures in the "Adding Phones to the Cisco Unified Communications Manager Database" section on page 2-9 to ensure that the phone has been added to the Cisco Unified Communications Manager database.

To verify that the phone is in the Cisco Unified Communications Manager database, choose **Device > Phone > Find** from Cisco Unified Communications Manager Administration to search for the phone based on its MAC Address. For information about determining a MAC address, see the "Determining the MAC Address for a Cisco Unified IP Phone" section on page 2-13.

If the phone is already in the Cisco Unified Communications Manager database, its configuration file may be damaged. See the "Creating a New Configuration File" section on page 12-5 for assistance.

Symptom: Cisco Unified IP Phone Unable to Obtain IP Address

If a phone is unable to obtain an IP address when it starts up, the phone may be not be on the same network or VLAN as the DHCP server, or the switch port to which the phone is connected may be disabled. Make sure that the network or VLAN to which the phone is connected has access to the DHCP server, and make sure that the switch port is enabled.

Cisco Unified IP Phone Resets Unexpectedly

If users report that their phones are resetting during calls or while idle on their desk, you should investigate the cause. If the network connection and Cisco Unified Communications Manager connection are stable, a Cisco Unified IP Phone should not reset on its own.

Typically, a phone resets if it has problems connecting to the Ethernet network or to Cisco Unified Communications Manager. These sections can help you identify the cause of a phone resetting in your network:

- Verifying the Physical Connection, page 12-6
- Identifying Intermittent Network Outages, page 12-6
- Verifying DHCP Settings, page 12-7
- Checking Static IP Address Settings, page 12-7
- Verifying the Voice VLAN Configuration, page 12-7
- Verifying that the Phones Have Not Been Intentionally Reset, page 12-7
- Eliminating DNS or Other Connectivity Errors, page 12-8

Verifying the Physical Connection

Verify that the Ethernet connection to which the Cisco Unified IP Phone is connected is up. For example, check whether the particular port or switch to which the phone is connected is down and that the switch is not rebooting. Also make sure that there are no cable breaks.

Identifying Intermittent Network Outages

Intermittent network outages affect data and voice traffic differently. Your network might have been experiencing intermittent outages without detection. If so, data traffic can resend lost packets and verify that packets are received and transmitted. However, voice traffic cannot recapture lost packets. Rather than retransmitting a lost network connection, the phone resets and attempts to reconnect its network connection.

If you are experiencing problems with the voice network, you should investigate whether an existing problem is simply being exposed.

Verifying DHCP Settings

The following suggestions can help you determine if the phone has been properly configured to use DHCP:

1. Verify that you have properly configured the phone to use DHCP. See the "Ethernet Setup Menu" section on page 7-4 for more information.

2. Verify that the DHCP server has been set up properly.

3. Verify the DHCP lease duration. Cisco recommends that you set it to 8 days.

Checking Static IP Address Settings

If the phone has been assigned a static IP address, verify that you have entered the correct settings. See the "Ethernet Setup Menu" section on page 7-4 for more information.

Verifying the Voice VLAN Configuration

If the Cisco Unified IP Phone appears to reset during heavy network usage (for example, following extensive web surfing on a computer connected to the same switch as the phone), it is likely that you do not have a voice VLAN configured.

Isolating the phones on a separate auxiliary VLAN increases the quality of the voice traffic. See the "Understanding How the Cisco Unified IP Phone Interacts with the VLAN" section on page 2-2 for details.

Verifying that the Phones Have Not Been Intentionally Reset

If you are not the only administrator with access to Cisco Unified Communications Manager, you should verify that no one else has intentionally reset the phones.

You can check whether a Cisco Unified IP Phone received a command from Cisco Unified Communications Manager to reset by pressing the **Applications** button on the phone and choosing **Administrator Settings** > **Status > Network Statistics**. If the phone was recently reset, one of these messages appears:

• Reset-Reset—Phone closed due to receiving a Reset/Reset from Cisco Unified Communications Manager Administration.

• Reset-Restart—Phone closed due to receiving a Reset/Restart from Cisco Unified Communications Manager Administration.

Eliminating DNS or Other Connectivity Errors

If the phone continues to reset, follow these steps to eliminate DNS or other connectivity errors:

Procedure

Step 1   Use the Reset Settings menu to reset phone settings to their default values. See the "Resetting the Cisco Unified IP Phone" section on page 12-15 for details.

Step 2   Modify DHCP and IP settings:

  a.   Disable DHCP. See the "Ethernet Setup Menu" section on page 7-4 for instructions.

  b.   Assign static IP values to the phone. See the "Ethernet Setup Menu" section on page 7-4 for instructions. Use the same default router setting used for other functioning Cisco Unified IP Phones.

  c.   Assign a TFTP server. See the "Ethernet Setup Menu" section on page 7-4 for instructions. Use the same TFTP server used for other functioning Cisco Unified IP Phones.

Step 3   On the Cisco Unified Communications Manager server, verify that the local host files have the correct Cisco Unified Communications Manager server name mapped to the correct IP address.

Step 4   From Cisco Unified Communications Manager, choose **System > Server** and verify that the server is referred to by its IP address and not by its DNS name.

Step 5   From Cisco Unified Communications Manager, choose **Device > Phone > Find** and verify that you have assigned the correct MAC address to this Cisco Unified IP Phone. For information about determining a MAC address, see the "Determining the MAC Address for a Cisco Unified IP Phone" section on page 2-13.

Step 6   Power cycle the phone.

Checking Power Connection

In most cases, a phone will restart if it powers up by using external power but loses that connection and switches to PoE. Similarly, a phone may restart if it powers up by using PoE and then gets connected to an external power supply.

Troubleshooting Cisco Unified IP Phone Security

Table 12-1 provides troubleshooting information for the security features on the Cisco Unified IP Phone. For information relating to the solutions for any of these issues, and for additional troubleshooting information about security, refer to *Cisco Unified Communications Manager Security Guide*.

Table 12-1   ***Cisco Unified IP Phone Security Troubleshooting***

Problem	Possible Cause
CTL File Problems	
Device authentication error.	CTL file does not have a Cisco Unified Communications Manager certificate or has an incorrect certificate.
Phone cannot authenticate CTL file.	The security token that signed the updated CTL file does not exist in the CTL file on the phone.
Phone cannot authenticate any of the configuration files other than the CTL file.	There is a bad TFTP record. The configuration file may not be signed by the corresponding certificate in the phone's Trust List.
Phone cannot authenticate any of the configuration files other than ITL file.	The configuration file may not be signed by the corresponding certificate in the phone's Trust List.
Phone reports TFTP authorization failure.	• The TFTP address for the phone does not exist in the CTL file. • If you created a new CTL file with a new TFTP record, the existing CTL file on the phone may not contain a record for the new TFTP server.
Phone does not register with Cisco Unified Communications Manager.	The CTL file does not contain the correct information for the Cisco Unified Communications Manager server.
Phone does not request signed configuration files.	The CTL file does not contain any TFTP entries with certificates.
802.1X Enabled on Phone but Not Authenticating	
Phone cannot obtain a DHCP-assigned IP address.	These errors typically indicate that 802.1X authentication is enabled on the phone, but the phone is unable to authenticate. 1. Verify that you have properly configured the required components (see the "Supporting 802.1X Authentication on Cisco Unified IP Phones" section on page 1-22 for more information). 2. Confirm that the shared secret is configured on the phone (see the"802.1X Authentication and Transaction Status" section on page 7-15 for more information). – If the shared secret is configured, verify that you have the same shared secret entered on the authentication server. – If the shared secret is not configured, enter it, and ensure that it matches the one on the authentication server.
Phone does not register with Cisco Unified Communications Manager.	
Phone status display as "Configuring IP" or "Registering".	
802.1X Authentication Status displays as "Held" (see the "802.1X Authentication and Transaction Status" section on page 7-15 for more details).	
Status menu displays 802.1X status as "Failed" (see the "Status Menu" section on page 10-2 for more details).	

Table 12-1   Cisco Unified IP Phone Security Troubleshooting (continued)

Problem	Possible Cause
802.1X Not Enabled	
Phone cannot obtain a DHCP-assigned IP address	These errors typically indicate that 802.1X authentication is not enabled on the phone. To enable it, see the "802.1X Authentication and Transaction Status" section on page 7-15.
Phone does not register with Cisco Unified Communications Manager	
Phone status display as "Configuring IP" or "Registering"	
802.1X Authentication Status displays as "Disabled"	
Status menu displays DHCP status as timing out	
Factory Reset Deleted 802.1X Shared Secret	
Phone cannot obtain a DHCP-assigned IP address	These errors typically indicate that the phone has completed a factory reset (see the "Resetting the Cisco Unified IP Phone" section on page 12-15) while 802.1X was enabled. A factory reset deletes the shared secret, which is required for 802.1X authentication and network access.
Phone does not register with Cisco Unified Communications Manager	To resolve this, temporarily move the phone to a network environment that is not using 802.1X authentication.
Phone status display as "Configuring IP" or "Registering"	Once the phone starts up normally, you can access the 802.1X configuration menus to enable device authentication and to re-enter the shared secret (see the "802.1X Authentication and Transaction Status" section on page 7-15).
Cannot access phone menus to verify 802.1X status	

General Troubleshooting Tips

Table 12-2 provides general troubleshooting information for the Cisco Unified IP Phone.

Table 12-2   Cisco Unified IP Phone Troubleshooting

Summary	Explanation
Connecting a Cisco Unified IP Phone to another Cisco Unified IP Phone	Cisco does not support connecting an IP phone to another IP phone through the PC port. Each IP phone should directly connect to a switch port. If phones are connected together in a line (by using the PC port), the phones will not work.
Poor quality with tandem audio encoding	Tandem encoding can occur when making calls between an IP phone and a digital cellular phone, when using a conference bridge, or in situations where IP to IP calls are partially routed across the PSTN. In these cases, use of voice codecs such as G.729 and iLBC may result in poor voice quality. Use these codecs only when absolutely necessary.
Prolonged broadcast storms cause IP phones to reset, or be unable to make or answer a call	A prolonged Layer 2 broadcast storm (lasting several minutes) on the voice VLAN may cause IP phones to reset, lose an active call, or be unable to initiate or answer a call. Phones may not come up until a broadcast storm ends.

Table 12-2   Cisco Unified IP Phone Troubleshooting (continued)

Summary	Explanation
Moving a network connection from the phone to a workstation	If you are powering your phone through the network connection, you must be careful if you decide to unplug the phone's network connection and plug the cable into a desktop computer. ⚠️ **Caution** The computer's network card cannot receive power through the network connection; if power comes through the connection, the network card can be destroyed. To protect a network card, wait 10 seconds or longer after unplugging the cable from the phone before plugging it into a computer. This delay gives the switch enough time to recognize that there is no longer a phone on the line and to stop providing power to the cable.
Changing the telephone configuration	By default, the network configuration options are locked to prevent users from making changes that could impact their network connectivity. You must unlock the network configuration options before you can configure them. See the "Unlocking and Locking Options" section on page 7-3 for details.
Phone resetting	The phone resets when it loses contact with the Cisco Unified Communications Manager software. This lost connection can be due to any network connectivity disruption, including cable breaks, switch outages, and switch reboots.
Phone display issues	If the display appears to have rolling lines or a wavy pattern, it might be interacting with certain types of older fluorescent lights in the building. Moving the phone away from the lights, or replacing the lights, should resolve the problem.
Dual-Tone Multi-Frequency (DTMF) delay	When you are on a call that requires keypad input, if you press the keys too quickly, some of them might not be recognized.
Codec mismatch between the phone and another device	The RxType and the TxType statistics show the codec that is being used for a conversation between this Cisco Unified IP phone and the other device. The values of these statistics should match. If they do not, verify that the other device can handle the codec conversation, or that a transcoder is in place to handle the service. See the "Call Statistics Screen" section on page 10-11 for information about displaying these statistics.
Sound sample mismatch between the phone and another device	The RxSize and the TxSize statistics show the size of the voice packets that are being used in a conversation between this Cisco Unified IP phone and the other device. The values of these statistics should match. See the "Call Statistics Screen" section on page 10-11 for information about displaying these statistics.
Gaps or delays in voice calls	Check the AvgJtr and the MaxJtr statistics. A large variance between these statistics might indicate a problem with jitter on the network or periodic high rates of network activity. See the "Call Statistics Screen" section on page 10-11 for information about displaying these statistics.

Table 12-2   Cisco Unified IP Phone Troubleshooting (continued)

Summary	Explanation
Loopback condition	A loopback condition can occur when the following conditions are met: • The SW Port Configuration option in the Network Configuration menu on the phone is set to **10 Half** (10-BaseT / half duplex) • The phone receives power from an external power supply • The phone is powered down (the power supply is disconnected) In this case, the switch port on the phone can become disabled and the following message will appear in the switch console log: HALF_DUX_COLLISION_EXCEED_THRESHOLD To resolve this problem, re-enable the port from the switch.
One-way audio	When at least one person in a call does not receive audio, IP connectivity between phones is not established. Check the configurations in routers and switches to ensure that IP connectivity is properly configured.
Phone call cannot be established	The phone does not have a DHCP IP address, is unable to register to Cisco Unified Communications Manager, and shows a Configuring IP or Registering message. Verify the following: 1. The Ethernet cable is attached. 2. The Cisco CallManager service is running on the Cisco Unified Communications Manager server. 3. Both phones are registered to the same Cisco Unified Communications Manager. 4. Audio server debug and capture logs are enabled for both phones. If needed, enable Java debug.
Video transmitted by the camera is too dark	The lighting conditions within the camera's field of view affect the brightness of the video. • Adjust the View Area for your camera. Try moving the location of the camera and check if the brightness improves. • Adjust the camera brightness setting. See "Adjusting the Brightness Setting" section on page 5-3 for instructions on how to adjust the brightness.
Poor video quality/grainy video	When the resolution of the received video is grainy, the user may perceive that the video quality is poor. However, this will not cause video distortion or artifacts. • Check the Cisco Unified Communications Manager bandwidth settings under Region settings. • Check the Receiver Resolution in video statistics. This may be an issue if the Cisco Unified CM bandwidth setting limits the resolution to less than CIF(352x288). Try increasing the bandwidth to at least 275 kbps.

Table 12-2   Cisco Unified IP Phone Troubleshooting (continued)

Summary	Explanation
Blocky or distorted video	Blocky or distorted video is generally a symptom of a degraded network. It is also caused by endpoints that do not closely adhere to video transmission standards. If the network is degraded, navigate to **AdminSettings > Status > CallStatistics > Video > Video statistics**, and check the following: • Rcvr Lost Packets • Rcvr Discarded • Avg Jitter • Max Jitter
No Video or black video screen	The video is black and no picture appears on the screen. • Verify that video is enabled in the Cisco Unified CM. • Cisco Unified IP Phone 8961, 9951, and 9971 phones do not display videos with a resolution higher than VGA (640x480). If the other endpoint transmits at a resolution greater than VGA, it will result in a black screen. Check the resolution of the transmitting endpoint. • There might not be any packets received for video display. Check the Rcvr Packets (would be zero in this case) in the **AdminSettings > Status > CallStatistics > Video > Video statistics.** • Ensure that the transmitting phone has the camera shutter completely open.
Frozen video	When the phone stops receiving video packets, the video displayed will pause, displaying the last decoded video frame. • Check if the received packets count is incrementing or not, by navigating to **AdminSettings > Status > CallStatistics > Video > Video statistics > Rcvr Packets** statistics. • Try to hold and then resume the call to clear the issue. • If the transmitting phone is also Cisco Unified IP Phone 8961 or 9951 or 9971, check the LED on top of the camera. If there is no light illuminated (either green or red) then the remote camera might not be transmitting video.
Slow moving video or jittery video	The frame rate of the received video is low. Check the rate by navigating to **AdminSettings > Status > CallStatistics > Video > Video statistics > Rcvr Frame Rate**. Frame rates less than 15 fps will result in slow-moving video.
Audio/Video synchronization is poor	• Check if RTCP is enabled in the Cisco Unified Communications Manager. • Audio/video synronization is generally caused a by degraded network connection. Check by navigating to navigating to **AdminSettings > Status > CallStatistics > Video > Video statistics > Avg Jitter** and **AdminSettings > Status > CallStatistics > Video > Video statistics > Max Jitter** values. • Try to hold and then resume the call to restore the audio/video synchronization.

Table 12-2   *Cisco Unified IP Phone Troubleshooting (continued)*

Summary	Explanation
Subject too dark in video	The lighting conditions within the camera's field of view of the camera affects the brightness of the video. • Adjust the View Area for your camera. Try moving the location of the camera and check if the brightness improves. • Adjust the camera brightness by navigating to **Accessories > Cisco Unified Video Camera > Brightness** and adjusting the brightness settings.
The recipient endpoint only sees a mute image	If the "Auto Transmit Video" is set to "Off", the camera will automatically transmit the mute image. The red LED illuminated on the top of the camera indicates that the video is muted. Set the Auto Transmit Video setting to **On** to restore video on the other side.
Camera not detected by phone	Unplug and then re-connect the camera back to the phone.

Resetting the Cisco Unified IP Phone

Performing a reset of a Cisco Unified IP Phone provides a way to recover if the phone experiences an error and provides a way to reset or restore various configuration and security settings.

Table 12-3 describes the types of resets you can perform. You can reset a phone with any of these operations after the phone has started up. Choose the operation that is appropriate for your situation.

Table 12-3   Basic Reset Methods

Operation	Performing	Explanation
Reset Settings	From the Administrator Settings menu, unlock phone options (see the "Unlocking and Locking Options" section on page 7-3), then choose **Reset Settings > All Settings**.	Resets user and network configuration settings to their factory-default values, and restarts the phone. Before you perform a factory reset, ensure that the following conditions are met: • The phone must be on a DHCP-enabled network. • A valid TFTP server must be set in DHCP option 150 or option 66 on the DHCP server. The following occurs on the phone when you perform a reset: • User configuration settings—Resets to default values • Network configuration settings—Resets to default values • Call histories—Gets erased • Locale information—Resets to default values • Phone application—Gets erased (phone recovers by using the image in the inactive partition of flash to boot up). • Security settings—Resets to default values; this includes deleting the CTL file, deleting the MD5 secret, and changing the 802.1x Device Authentication parameter to "Disabled." **Note** Do not power down the phone until it completes the factory reset process, and the main screen appears.
	From the Admin Settings menu, unlock phone options (see the "Unlocking and Locking Options" section on page 7-3), then choose **Reset Settings > Network Settings**.	Resets network configuration settings to their default values and resets the phone. (This method causes DHCP to reconfigure the IP address of the phone.)
	From the Administrator Settings menu, unlock phone options (see the "Unlocking and Locking Options" section on page 7-3), then choose **Reset Settings > Reset Device**.	Resets any user and network configuration changes that you have made, but that the phone has not written to its Flash memory, to previously saved settings.
	From the Administrator Settings menu, unlock phone options (see the "Unlocking and Locking Options" section on page 7-3), then choose **Reset Settings > Security Settings**.	Deletes only the CTL file.

Using the Quality Report Tool

The Quality Report Tool (QRT) is a voice quality and general problem-reporting tool for the Cisco Unified IP Phone. The QRT feature is installed as part of the Cisco Unified Communications Manager installation.

You can configure users' Cisco Unified IP Phones with QRT. When you do so, users can report problems with phone calls by pressing the **QRT** softkey. This softkey is available only when the Cisco Unified IP Phone is in the Connected, Connected Conference, Connected Transfer, and/or OnHook states.

When a user presses the **QRT** softkey, a list of problem categories appears. The user selects the appropriate problem category, and this feedback is logged in an XML file. Actual information logged depends on the user selection and whether the destination device is a Cisco Unified IP Phone.

For more information about using QRT, refer to *Cisco Unified Communications Manager Features and Services Guide*.

Monitoring the Voice Quality of Calls

To measure the voice quality of calls that are sent and received within the network, Cisco Unified IP Phones use these statistical metrics that are based on concealment events. The DSP plays concealment frames to mask frame loss in the voice packet stream.

- Concealment Ratio metrics—Show the ratio of concealment frames over total speech frames. An interval conceal ratio is calculated every 3 seconds.

- Concealed Second metrics—Show the number of seconds in which the DSP plays concealment frames due to lost frames. A severely "concealed second" is a second in which the DSP plays more than five percent concealment frames.

Note Concealment ratio and concealment seconds are primary measurements based on frame loss. A Conceal Ratio of zero indicates that the IP network is delivering frames and packets on time with no loss.

You can access voice quality metrics from the Cisco Unified IP Phone by using the Call Statistics screen (see the "Call Statistics Screen" section on page 10-11) or remotely by using Streaming Statistics (see the Monitoring the Cisco Unified IP Phone Remotely chapter).

Troubleshooting Tips

When you observe significant and persistent changes to metrics, use Table 12-4 for general troubleshooting information:

Table 12-4   Changes to Voice Quality Metrics

Metric Change	Condition
Conceal Ratio and Conceal Seconds increase significantly	Network impairment from packet loss or high jitter.
Conceal Ratio is near or at zero, but the voice quality is poor.	• Noise or distortion in the audio channel such as echo or audio levels. • Tandem calls that undergo multiple encode/decode such as calls to a cellular network or calling card network. • Acoustic problems coming from a speakerphone, handsfree cellular phone or wireless headset. Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.

Note   Voice quality metrics do not account for noise or distortion, only frame loss.

Where to Go for More Troubleshooting Information

If you have additional questions about troubleshooting the Cisco Unified IP Phones, go to the following Cisco web site and then navigate to the desired Cisco Unified IP Phone:

http://www.cisco.com/cisco/web/psa/troubleshoot.html

Cleaning the Cisco Unified IP Phone

To clean your Cisco Unified IP phone, use only a dry soft cloth to gently wipe the phone and the phone screen. Do not apply liquids or powders directly on the phone. As with all non-weather-proof electronics, liquids and powders can damage the components and cause failures.

Providing Information to Users Via a Website

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. It is important to provide current and thorough information to end users.

Cisco recommends that you create a web page on your internal support site that provides end users with important information about their Cisco Unified IP Phones.

Consider including the following types of information on this site:

- How Users Obtain Support for the Cisco Unified IP Phone, page A-1
- How Users Subscribe to Services and Configure Phone Features, page A-2
- How Users Access a Voice Messaging System, page A-2
- How Users Configure Personal Directory Entries, page A-3

How Users Obtain Support for the Cisco Unified IP Phone

To successfully use some of the features on the Cisco Unified IP Phone (including speed dial, services, and voice messaging system options), users must receive information from you or from your network team or be able to contact you for assistance. Make sure to provide end users with the names of people to contact for assistance and with instructions for contacting those people.

Giving Users Access to the User Options Web Pages

Before a user can access the User Options web pages, you must use Cisco Unified Communications Manager Administration to add the user to a standard Cisco Unified Communications Manager end user group: choose **User Management > User Groups**. For additional information, refer to:

- *Cisco Unified Communications Manager Administration Guide*, "User Group Configuration" chapter
- *Cisco Unified Communications Manager System Guide*, "Roles and User Groups" chapter"

How Users Subscribe to Services and Configure Phone Features

End users can perform a variety of activities by using the Cisco Unified Communications Manager User Options web pages. These activities include subscribing to services, setting up speed dial and call forwarding numbers, configuring ring settings, and creating a personal address book. Keep in mind that configuring settings on a phone by using a website might be new for your end users. You need to provide as much information as possible to ensure that they can successfully access and use the User Options web pages.

Make sure to provide end users with the following information about the User Options web pages:

- The URL required to access the application. This URL is:

  http://<*server_name:portnumber*>**/ccmuser/**, where *server_name* is the host on which the web server is installed.

- A user ID and default password are needed to access the application.

  These settings correspond to the values you entered when you added the user to Cisco Unified Communications Manager (see the "Adding Users to Cisco Unified Communications Manager" section on page 8-33).

- A brief description of what a web-based, graphical user interface application is, and how to access it with a web browser.

- An overview of the tasks that users can accomplish by using the web page.

How Users Access a Voice Messaging System

Cisco Unified Communications Manager lets you integrate with many different voice messaging systems, including the Cisco Unity voice messaging system. Because you can integrate with a variety of systems, you must provide users with information about how to use your specific system.

You should provide this information to each user:

- How to access the voice messaging system account.

  Make sure that you have used Cisco Unified Communications Manager to configure the **Messages** button on the Cisco Unified IP Phone.

- Initial password for accessing the voice messaging system.

  Make sure that you have configured a default voice messaging system password for all users.

- How the phone indicates that voice messages are waiting.

  Make sure that you have used Cisco Unified Communications Manager to set up a message waiting indicator (MWI) method.

How Users Configure Personal Directory Entries

Users can configure personal directory entries on the Cisco Unified IP Phone. To configure a personal directory, users must have access to the following:

- User Options web pages—Make sure that users know how to access their User Options web pages. See the "How Users Subscribe to Services and Configure Phone Features" section on page A-2 for details.

- Cisco Unified IP Phone Address Book Synchronizer—Make sure to provide users with the installer for this application. To obtain the installer, choose **Application > Plugins** from Cisco Unified Communications Manager Administration and click **Download**, which is located next to the **Cisco Unified IP Phone Address Book Synchronizer** plugin name. When the file download dialog box displays, click **Save**. Send the TabSyncInstall.exe file to all users who require this application.

See the "Installing and Configuring the Cisco Unified IP Phone Address Book Synchronizer" section on page A-3 for information about installing the Cisco Unified IP Phone Address Book Synchronizer.

Installing and Configuring the Cisco Unified IP Phone Address Book Synchronizer

Use this tool to synchronize data stored in your Microsoft Windows address book with the Cisco Unified Communications Manager directory and the User Options Personal Address Book.

$\mathcal{Q}$

Tip   To successfully synchronize the Windows address book with the Personal Address Book, all Windows address book users should be entered in the Windows address book before performing the following procedures.

Installing the Synchronizer

Step 1   Get the Cisco Unified IP Phone Address Book Synchronizer installer file from your system administrator.

Step 2   Double-click the TabSyncInstall.exe file provided by your system administrator.

The publisher dialog box displays.

Step 3   Click **Run**.

The Welcome to the InstallShield Wizard for Cisco Unified CallManager Personal Address Book Synchronizer window displays.

Step 4   Click **Next**.

The License Agreement window displays.

Step 5   Read the license agreement information, and click the I Accept radio button. Click **Next**.

The Destination Location window displays.

Step 6   Choose the directory in which you want to install the application and click **Next**.

The Ready to Install window displays.

Step 7   Click **Install**.

The installation wizard installs the application to your computer. When the installation is complete, the InstallShield Wizard Complete window displays.

Step 8   Click **Finish**.

Step 9   To complete the process, follow the steps in the "Configuring the Synchronizer" section on page A-4.

Configuring the Synchronizer

Step 1   Open the Cisco Unified IP Phone Address Book Synchronizer.

If you accepted the default installation directory, you can open the application by choosing **Start > All Programs > Cisco Systems > TabSync**.

Step 2   To configure user information, click the **User** button.

The Cisco Unified CallManager User Information window displays.

Step 3   Enter the Cisco Unified IP Phone user name and password and click **OK**.

Step 4   To configure Cisco Unified Communications Manager server information, click the **Server** button.

The Configure Cisco Unified CallManager Server Information window displays.

Step 5   Enter the IP address or host name and the port number of the Cisco Unified Communications Manager server and click **OK**.

If you do not have this information, contact your system administrator.

Step 6   To start the directory synchronization process, click the **Synchronize** button.

The Synchronization Status window provides information on the status of the address book synchronization. If you chose the user intervention for duplicate entries rule and you have duplicate address book entries, the Duplicate Selection window displays. Choose the entry that you want to include in your Personal Address Book and click **OK**.

When synchronization completes, click **Exit** to close the Cisco Unified CallManager Address Book Synchronizer. To verify if the synchronization worked, log in to your User Options web pages and choose Personal Address Book. The users from your Windows address book should be listed.

Supporting International Users

Translated and localized versions of the Cisco Unified IP Phones are available in several languages. If you are supporting Cisco Unified IP Phones in a non-English environment, refer to the following sections to ensure that the phones are set up properly for your users:

Installing the Cisco Unified Communications Manager Locale Installer

If you are using Cisco Unified IP Phones in a locale other than English (United States), you must install the locale-specific version of the Cisco Unified Communications Manager Locale Installer on every Cisco Unified Communications Manager server in the cluster. Installing the locale installer ensures that you have the latest translated text, user and network locales, and country-specific phone tones available for the Cisco Unified IP Phones. You can find locale-specific versions of the Cisco Unified Communications Manager Locale Installer at http://www.cisco.com/kobayashi/sw-center/telephony/callmgr/locale-installer.shtml.

For more information, refer to the "Locale Installation" section in the *Cisco Unified Communications Operating System Administration Guide.*

Note All languages may not be immediately available, so continue to check the website for updates.

Support for International Call Logging

If your phone system is configured for international call logging (calling party normalization), the call logs, redial, or call directory entries may display a "+" symbol to represent the international escape code for your location. Depending on the configuration for your phone system, the "+" may be replaced with the correct international dialing code, or you may need to edit the number before dialing to manually replace the "+" with the international escape code for your location. In addition, while the call log or directory entry may display the full international number for the received call, the phone display may show the shortened local version of the number, without international or country codes.

A P P E N D I X C

Technical Specifications

The following sections describe the technical specifications for the Cisco Unified IP Phone 8961, 9951, and 9971.

- Physical and Operating Environment Specifications, page C-1
- Cable Specifications, page C-2
- Network and Computer Port Pinouts, page C-2

Physical and Operating Environment Specifications

Table C-1 shows the physical and operating environment specifications for the Cisco Unified IP Phone 8961, 9951, and 9971.

Table C-1   Physical and Operating Specifications

Specification	Value or Range
Operating temperature	32° to 104°F (0° to 40°C)
Operating relative humidity	10% to 95% (non-condensing)
Storage temperature	14° to 140°F (–10° to 60°C)
Height	8 in. (20.32 cm)
Width	10.5 in. (26.67 cm)
Depth	6 in. (15.24 cm)
Weight	3.5 lb. (1.6 kg)
Power	• 100-240 VAC, 50-60 Hz, 0.5 A—when using the AC adapter • 48 VDC, 0.2 A—when using the in-line power over the network cable
Power consumed by the camera[1]	290mA (1.45W) (excluding the power consumed by the phone)
Cables	Category 3/5/5e/6 for 10-Mbps cables with 4 pairs Category 5/5e/6 for 100-Mbps cables with 4 pairs Category 5e/6 for 1000-Mbps cables with 4 pairs **Note** Cables have 4 pairs of wires for a total of 8 conductors.
Distance requirements	As supported by the Ethernet Specification, it is assumed that the maximum cable length between each Cisco Unified IP Phone and the switch is 330 feet (100 meters).

1.   Applicable only for Cisco Unified IP Phone 9951 and 9971 only.

Note For power information regarding the Cisco Unified IP Key Color Expansion Module, see the "Power Information" section on page 4-2.

Cable Specifications

- RJ-9 jack (4-conductor) for handset and headset connection.
- RJ-45 jack for the LAN 10/100/1000BaseT connection (10/100/1000 Network port on the Cisco Unified IP Phone 8961, 9951, and 9971).
- RJ-45 jack for a second 10/100/1000BaseT compliant connection (10/100/1000 Computer port on the Cisco Unified IP Phone 8961, 9951, and 9971).
- 3.5 mm jack for microphone and speaker connection (for Cisco Unified IP Phones 9951 and 9971 only).
- 48-volt power connector.

Network and Computer Port Pinouts

Although both the network and computer (access) ports are used for network connectivity, they serve different purposes and have different port pinouts.

- The Network port is the 10/100/1000 SW port on the Cisco Unified IP Phone.
- The Computer (access) port is the 10/100/1000 PC port on the Cisco Unified IP Phone.

Network Port Connector

Table C-2 describes the Network port connector pinouts.

Table C-2   Network Port Connector Pinouts

Pin Number	Function
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-

Note "BI" stands for bi-directional, while DA, DB, DC and DD stand for "Data A", "Data B", "Data C" and "Data D", respectively.

Computer Port Connector

Table C-3 describes the Computer port connector pinouts.

Table C-3   Computer (Access) Port Connector Pinouts

Pin Number	Function
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-

Note   "BI" stands for bi-directional, while DA, DB, DC and DD stand for "Data A", "Data B", "Data C" and "Data D", respectively.

■ **Network and Computer Port Pinouts**

Basic Phone Administration Steps

This appendix provides minimum, basic configuration steps for you to do the following:

- Add a new user to Cisco Unified Communications Manager Administration
- Configure a new phone for that user
- Associate that user to that phone
- Complete other basic end-user configuration tasks

The procedures provide one method for performing these tasks and are not the only way to perform these tasks. They are a streamlined approach to get a new user and corresponding phone running on the system.

These procedures are designed to be used on a mature Cisco Unified Communications Manager system where calling search spaces, partitions, and other complicated configuration have already been done and are in place for existing users.

This section contains these topics:

Example User Information for these Procedures

In the procedures that follow, example are given when possible to illustrate some of the steps. Sample user and phone information used throughout these procedures includes:

- User's Name: John Doe
- User ID: johndoe
- Phone model: 9971
- Protocol: SIP
- MAC address listed on phone: 00127F576611
- Five-digit internal telephone number: 26640

Adding a User to Cisco Unified Communications Manager

This section describes steps for adding a user to Cisco Unified Communications Manager. Follow one of the procedures in this section, depending on your operating system and the manner in which you are adding the user:

Adding a User From an External LDAP Directory

If you added a user to an LDAP Directory (a non-Cisco Unified Communications Server directory), you can immediately synchronize that directory to the Cisco Unified Communications Manager on which you are adding this same user and the user's phone by following these steps:

Procedure

Step 1   Log onto Cisco Unified Communications Manager Administration.

Step 2   Choose **System > LDAP > LDAP Directory**.

Step 3   Use the **Find** button to locate your LDAP directory.

Step 4   Click on the LDAP directory name.

Step 5   Click **Perform Full Sync Now**.

> **Note**   If you do not need to immediately synchronize the LDAP Directory to the Cisco Unified Communications Manager, the LDAP Directory Synchronization Schedule on the LDAP Directory window determines when the next auto-synchronization is scheduled. However, the synchronization must occur before you can associate a new user to a device.

Step 6   Proceed to Configuring the Phone, page D-3

Adding a User Directly to Cisco Unified Communications Manager

If you are not using an LDAP directory, you can add a user directly to Cisco Unified Communications Manager Administration by following these steps:

> **Note**   If LDAP is synchronized, you cannot add a user to the Cisco Unified Communications Manager Administration.

Procedure

Step 1   Choose **User Management > End User**, then click **Add New.** The End User Configuration window appears.

Step 2   In the User Information pane of this window, enter the following:

- User ID—Enter the end user identification name. Cisco Unified Communications Manager does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.

  Example: *johndoe*

- Password and Confirm Password—Enter five or more alphanumeric or special characters for the end user password. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.

- Last Name—Enter the end user last name. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.)

  Example: *doe*

- Telephone Number—Enter the primary directory number for the end user. End users can have multiple lines on their phones.

  Example: 26640 (John Doe's internal company telephone number)

Step 3   Click **Save**.

Step 4   Proceed to the section .

Configuring the Phone

To identify the user's phone model and protocol, follow these steps:

Procedure

Step 1   From Cisco Unified Communications Manager administration, choose **Device > Phone >.**

Step 2   Click **Add New**.

Step 3   Select the user's phone model from the Phone Type drop-down list, then click **Next**. The Phone Configuration window appears.

On the Phone Configuration window, you can use the default values for most of the fields.

To configure the required fields and some key additional fields, follow these steps:

Procedure

Step 1   For the required fields, possible values, some of which are based on the example of user *johndoe*, can be configured as follows:

  a.   In the Device Information pane of this window:

- MAC Address—Enter the MAC address of the phone, which is listed on a sticker on the phone.

  Make sure that the value comprises 12 hexadecimal characters.

  Example: 00127F576611 (MAC address on john doe's phone)

- Description—This is an optional field in which you can enter a useful description, such as *john doe's phone*. This will help you if you need to search on information about this user.

- **Device Pool**—Choose the device pool to which you want this phone assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, softkey template, and MLPP information.

  ✎

  Note   Device Pools are defined on the Device Pool Configuration window of Cisco Unified Communications Server Administration (**System > Device Pool)**.

- **Phone Button Template**—Choose the appropriate phone button template from the drop-down list. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.

  ✎

  Note   Phone button templates are defined on the Phone Button Template Configuration window of Cisco Unified Communications Manager Administration (**Device > Device Settings > Phone Button Template**). You can use the search field(s) in conjunction with the **Find** button to find all configured phone button templates and their current settings.

- **Common Phone Profile**—From the drop-down list box, choose a common phone profile from the list of available common phone profiles.

  ✎

  Note   Common Phone Profiles are defined on the Common Phone Profile Configuration window of Cisco Unified Communications Manager Administration (**Device > Device Settings > Common Phone Profile**). You can use the search field(s) in conjunction with the **Find** button to find all configured common phone profiles and their current settings.

- **Calling Search Space**—From the drop-down list box, choose the appropriate calling search space (CSS). A calling search space comprises a collection of partitions (analogous to a collection of available phone books) that are searched to determine how a dialed number should be routed. The calling search space for the device and the calling search space for the directory number get used together. The directory number CSS takes precedence over the device CSS.

  ✎

  Note   Calling Search Spaces are defined on the Calling Search Space Configuration window of Cisco Unified Communications Manager Administration (**Calling routing > Class of Control> Calling Search Space**). You can use the search field(s) in conjunction with the **Find** button to find all configured Calling Search Spaces and their current settings.

- **Location**—Choose the appropriate location for this Cisco Unified IP Phone.
- **Owner User ID**—From the drop-down menu, choose the user ID of the assigned phone user.

b. In the Protocol Specific Information pane of this window, choose a Device Security Profile from the drop-down list. To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. If the phone does not support security, choose a non-secure profile.

To identify the settings that are contained in the profile, choose **System > Security Profile > Phone Security Profile**.

> **Note**   The security profile chosen should be based on the overall security strategy of the company.

   c. In the Extension Information pane of this window, check the Enable Extension Mobility box if this phone supports Cisco Extension Mobility.

   d. Click **Save**.

Step 2   Configure line settings:

   a. On the Phone Configuration window, click Line 1 on the left pane of the window. The Directory Number Configuration window appears.

   b. In the Directory Number field, enter a valid number that can be dialed.

> **Note**   This field should contain the same number that appears in the Telephone Number field on the User Configuration window.

   Example: 26640 is the directory number of user John Doe in the example above.

   c. From the Route Partition drop-down list, choose the partition to which the directory number belongs. If you do not want to restrict access to the directory number, choose <None> for the partition.

   d. From the Calling Search Space drop-down list (Directory Number Settings pane of the Directory Number Configuration window), choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. The value that you choose applies to all devices that are using this directory number.

   e. In the Call Pickup and Call Forward Settings pane of the Directory Number Configuration window, choose the items (i.e. Forward All, Forward Busy Internal) and corresponding destinations to which calls should be sent.

   Example: If you want incoming internal and external calls that receive a busy signal to be forwarded to the voice mail for this line, check the Voice Mail box next to the "Forward Busy Internal" and "Forward Busy External" items in the left column of the Call Pickup and Call Forward Settings pane.

   f. In the "Line 1 on Device..." pane of the Directory Number Configuration window, configure the following:

   – Display (Internal Caller ID field)—You can enter the first name and last name of the user of this device so that this name will be displayed for all internal calls. You can also leave this field blank to have the system display the phone extension.

   – External Phone Number Mask—Indicate phone number (or mask) that is used to send Caller ID information when a call is placed from this line.

   You can enter a maximum of 24 number and "X" characters. The Xs represent the directory number and must appear at the end of the pattern.

   Example: Using the john doe extension in the example above, if you specify a mask of 408902XXXX, an external call from extension 6640 displays a caller ID number of 4089026640.

> **Note**   This setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the **Propagate Selected** button. (The check box at right displays only if other devices share this directory number.)

g. Click **Save**.

h. Click **Associate End Users** at the bottom of the window to associate a user to the line being configured. Use the Find button in conjunction with the Search fields to locate the user, then check the box next to the user's name, then click **Add Selected**. The user's name and user ID should now appear in the "Users Associated With Line" pane of the Directory Number Configuration window.

i. Click **Save**. The user is now associated with Line 1 on the phone.

j. If your phone has a second line, configure Line 2.

k. Associate the user with the device:

   – Choose **User Management > End User**.

   – Use the search boxes and the Find button to locate the user you have added (i.e. *doe* for the last name).

   – Click on the user ID (i.e. *johndoe*). The End User Configuration window appears.

   – Click **Device Associations**.

   – Use the Search fields and the Find button to locate the device with which you want to associate to the user. Select the device, then click **Save Selected/Changes**. The user is now associated with the device.

   – Click the **Go** button next to the "Back to User" Related link in the upper-right corner of the screen.

l. Proceed to .

Performing Final End User Configuration Steps

If you are not already on the End User Configuration page, choose **User Management > End User** to perform some final configuration tasks. Use the Search fields and the Find button to locate the user (i.e. John Doe), then click on the user ID to get to the End User Configuration window for the user.

In the End User configuration window, do the following:

Procedure

Step 1 In the Directory Number Associations pane of the screen, set the primary extension from the drop-down list.

Step 2 In the Mobility Information pane, check the Enable Mobility box.

Step 3 In the Permissions Information pane, use the User Group buttons to add this user to any user groups. For example, you may want to add the user to a group that has been defined as a "Standard CCM End User Group."

To view all configured user groups, choose **User Management > User Group**.

Step 4 In the Extension Mobility pane, check the Enable Extension Mobility Cross Cluster box if the user is allowed for Extension Mobility Cross Cluster service.

Step 5 Click **Save**.

Installing the Wall Mount for the Cisco Unified IP Phone

This appendix contains information on installing the wall mount for use with the following:

- Installing the Wall Mount for Cisco Unified IP Phone 8961, 9951, and 9971
- Installing a Wall Mount for a Phone with a Key Expansion Module

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

This section describes how to install a wall mount for the Cisco Unfilled IP Phone 8961, 9951, and 9971.

Figure E-1   Wall Mount Kit for a Single Phone Assembly
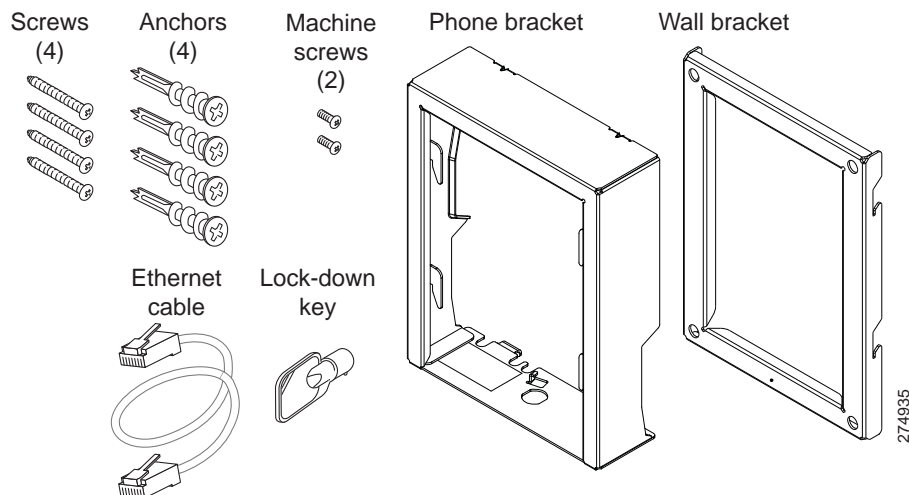
The package includes these items:

- 1 phone bracket
- 1 wall bracket
- 4 10-12x1 inch Phillips-head screws with 4 anchors
- 1 sheet metal screw

- 2 4-40x1/4 inch machine screws
- 1 six-inch Ethernet cable
- 1 key if the bracket includes the optional lock

Before You Begin

You will need these tools to install the bracket:

- #1 and #2 Phillips-head screwdrivers
- Level

You must also install an Ethernet jack for the telephone in the desired location if an Ethernet jack does not currently exist. This jack must be wired appropriately for an Ethernet connection. You cannot use a regular telephone jack. For more information on phone installation requirements and warnings, see the Setting Up the Cisco Unified IP Phone chapter.

Installing the Bracket

To install the phone on the wall, perform the following steps:

Procedure

Step 1   Mount the wall bracket in the desired location (Figure E-2). You can install the bracket over an Ethernet jack, or you can run the Ethernet network cable to a jack nearby.

    a. Use the Level to ensure the bracket is level, then use a pencil to mark the screw holes.

    b. Using a #2 Phillips-head screwdriver, carefully center the anchor over the pencil mark and press the anchor into the wall.

    c. Screw the anchor clockwise into the wall until it is seated flush.

    d. Use the included screws and a #2 Phillips-head screwdriver to attach the bracket to the wall.

Figure E-2   Mounting the Wall Bracket

A — Level wall bracket on wall

B — Mark mounting holes through bracket on wall

C — Insert anchors into wall

D — Screw bracket to wall using Phillips head screws
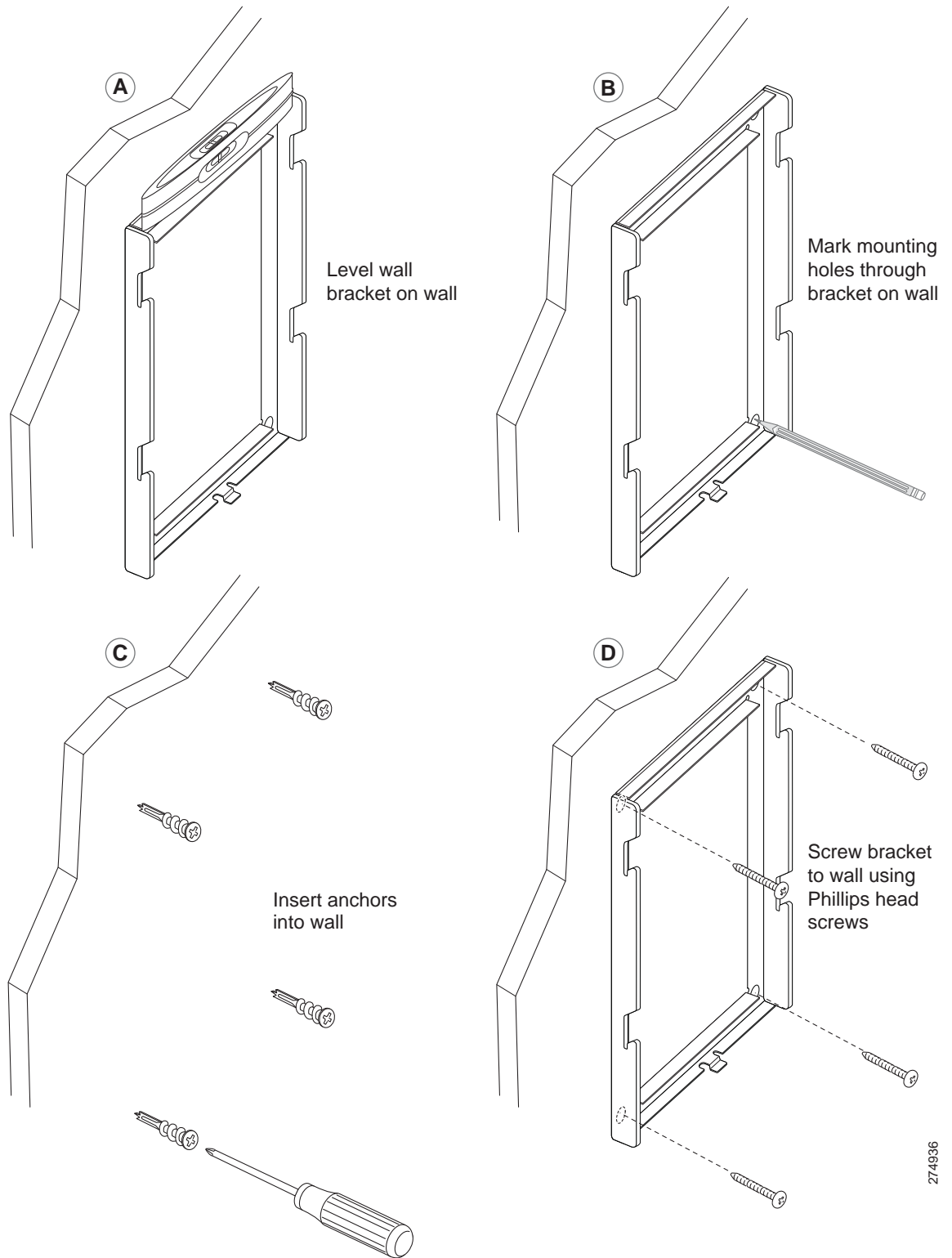
274936

**Step 2**   Attach the phone bracket to the IP phone (Figure E-3).

    a.   Detach the handset cord (and headset cord, if there is a headset), power cord, and any other attached cords from the base of the phone.

    b.   Remove the label covers that are concealing the screw holes.

    c.   Attach the phone bracket by inserting the tabs into the mounting tabs on the phone. The phone's ports should be accessible through the holes in the bracket.

    d.   Secure the phone bracket to the IP Phone with the machine screws.

    e.   Thread the handset cord (and headset cord, if using one). Reattach the cords and seat them in the clips incorporated into the phone body.

Figure E-3   *Attaching the Phone Bracket*
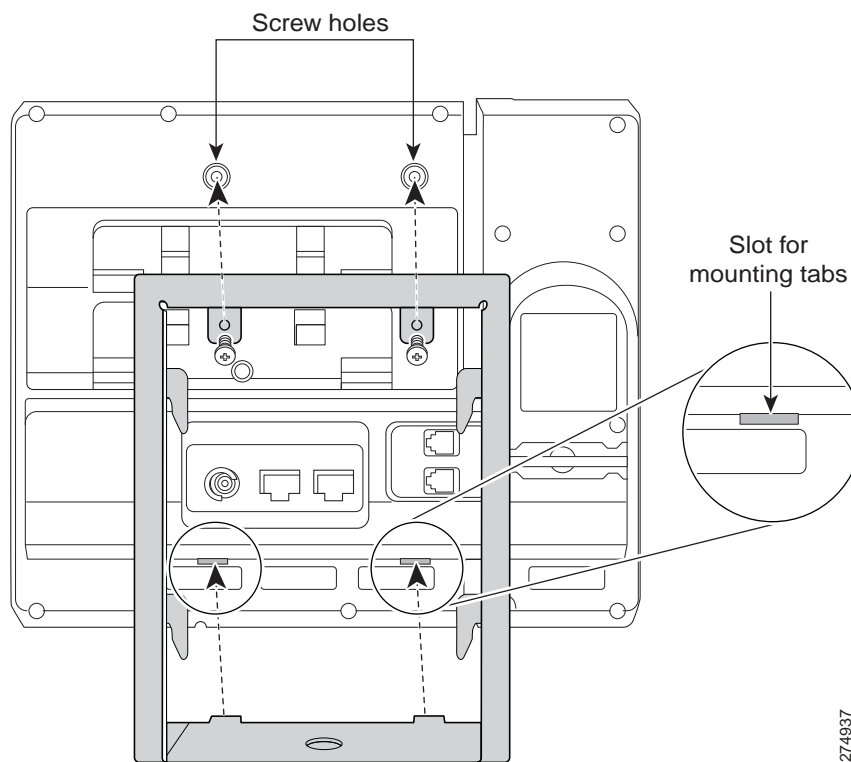
Step 3   Remove the handset wall hook in the handset rest, rotate the hook 180 degrees, and reinsert the hook. The hook should have a lip on which the handset catches when the phone is vertical (Figure E-4).

Figure E-4   Preparing the Handset Hook
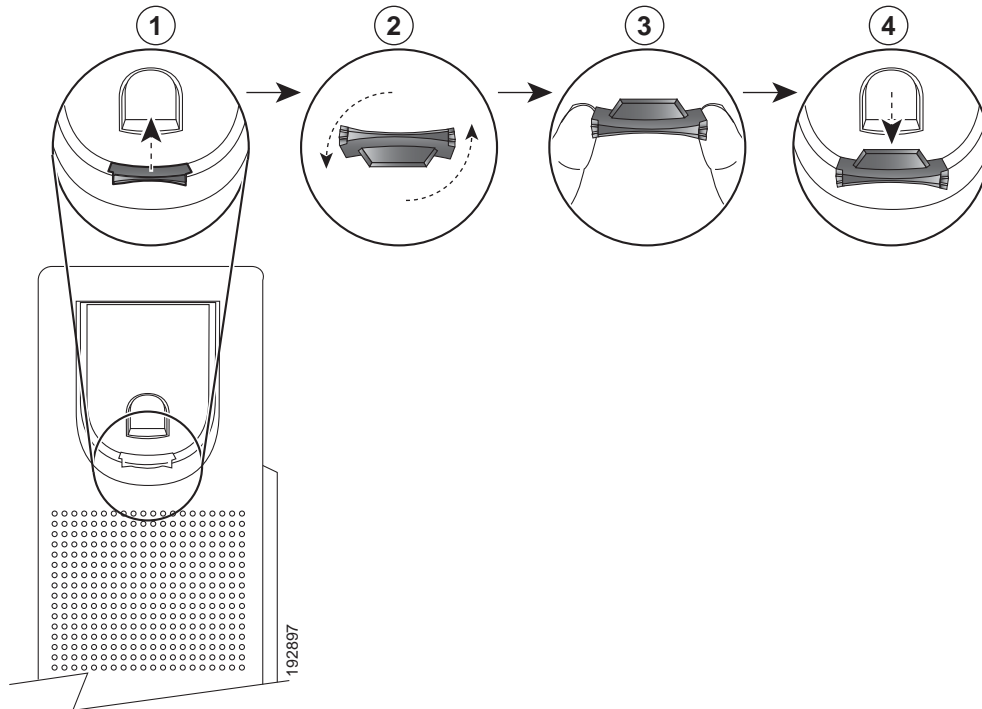
Step 4   Attach the Ethernet cable to the 10/100/1000 SW network port and wall jack.

If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100/1000 Computer (PC access) port.

If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips incorporated into the phone body next to the PC port (Figure E-5).

Figure E-5   Attaching the Cables
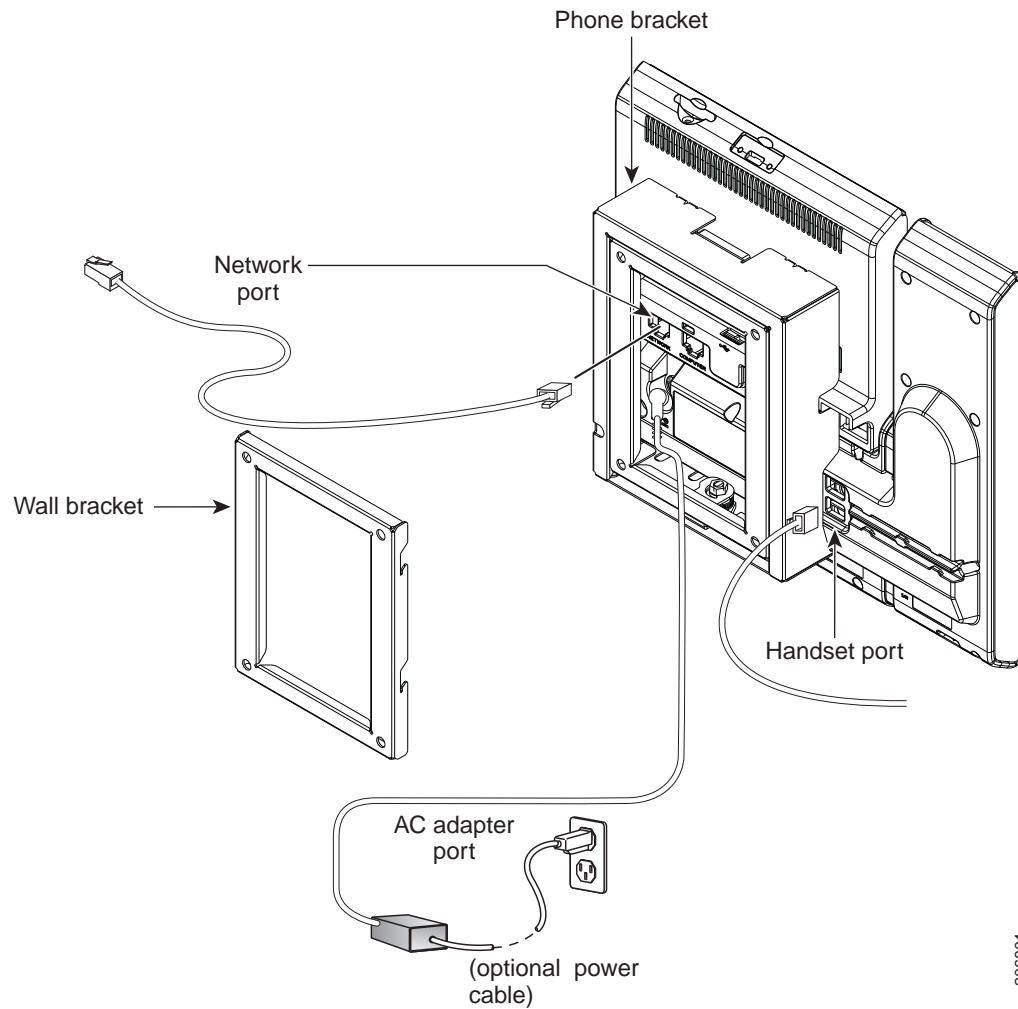
Phone bracket

Network port

Wall bracket

Handset port

AC adapter port

(optional power cable)

206801

Step 5   Attach the phone to the wall bracket by inserting the tabs on the top of the phone bracket into the slots on the wall bracket. Ensure that the power cord and any other cable that does not terminate in the wall behind the bracket are positioned in one of the cable-access openings in the bottom of the bracket. The phone and wall brackets' openings together form circular openings with room for one cable per opening (Figure E-6).

Step 6   Use the locking key to lock the phone to the wall bracket.

Figure E-6   *Attaching the Phone to the Wall Bracket*
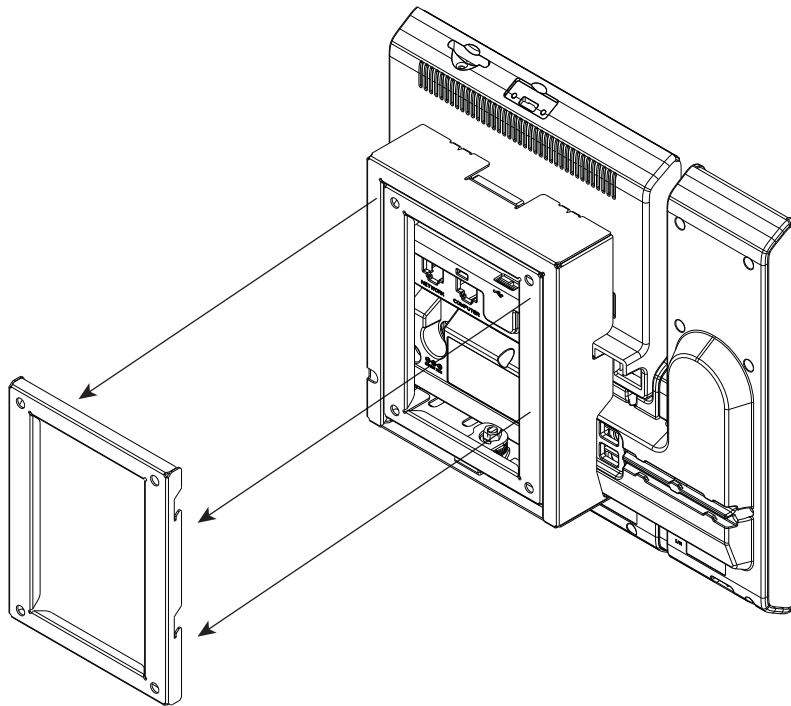
Installing a Wall Mount for a Phone with a Key Expansion Module

This section describes how to install a wall mount for the Cisco Unified IP Phone 8961, 9951, and 9971 connected with the Key Expansion Module.

Figure E-7   *Wall Mount Kit for Phone with Key Expansion Module*
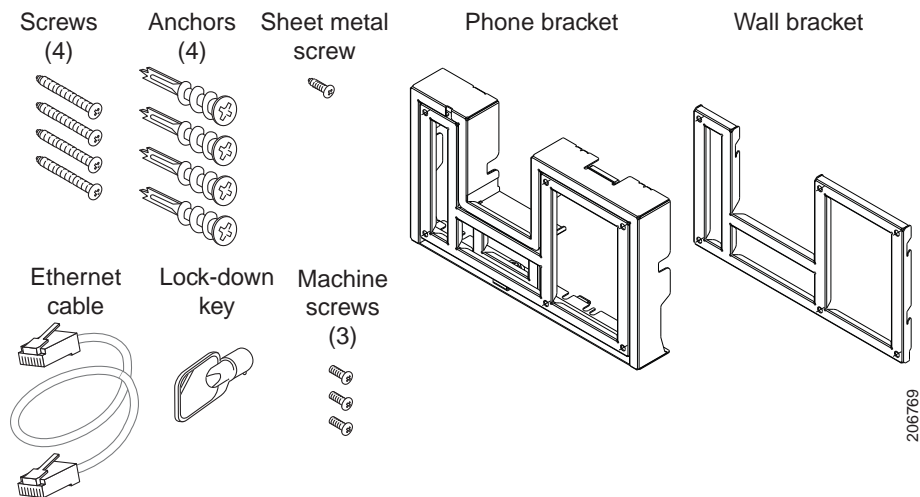
The package includes these items:

- 1 phone bracket
- 1 wall bracket
- 4 10-12x1 inch Phillips-head screws with 4 anchors
- 1 sheet metal screw
- 3 4-40x1/4 inch machine screws
- 1 six-inch Ethernet cable
- 1 key if the bracket includes the optional lock

Before You Begin

You will need these tools to install the bracket:

- #1 and #2 Phillips-head screwdrivers
- Level

You must also install an Ethernet jack for the telephone in the desired location if an Ethernet jack does not currently exist. This jack must be wired appropriately for an Ethernet connection. You cannot use a regular telephone jack. For more information on phone installation requirements and warnings, see the Setting Up the Cisco Unified IP Phone chapter.

Installing the Bracket

To install the phone on the wall, perform the following steps:

Note   Be sure to connect to connect the Cisco Unified IP Phone to the Key Expansion Module prior to installing the phone bracket.

Procedure

Step 1   Mount the wall bracket in the desired location (Figure E-8). You can install the bracket over an Ethernet jack, or you can run the Ethernet network cable to a jack nearby.

   a.   Use the level to ensure the bracket is level, then use a pencil to mark the screw holes.

   b.   Using a #2 Phillips-head screwdriver, carefully center the anchor over the pencil mark and press the anchor into the wall.

   c.   Screw the anchor clockwise into the wall until it is seated flush.

   d.   Use the included screws and a #2 Phillips-head screwdriver to attach the bracket to the wall.

Figure E-8   Mounting the Wall Bracket

A — Level wall bracket on wall

B — Mark mounting holes through bracket on wall

C — Insert anchors into wall

D — Screw bracket to wall using Phillips head screws

206799
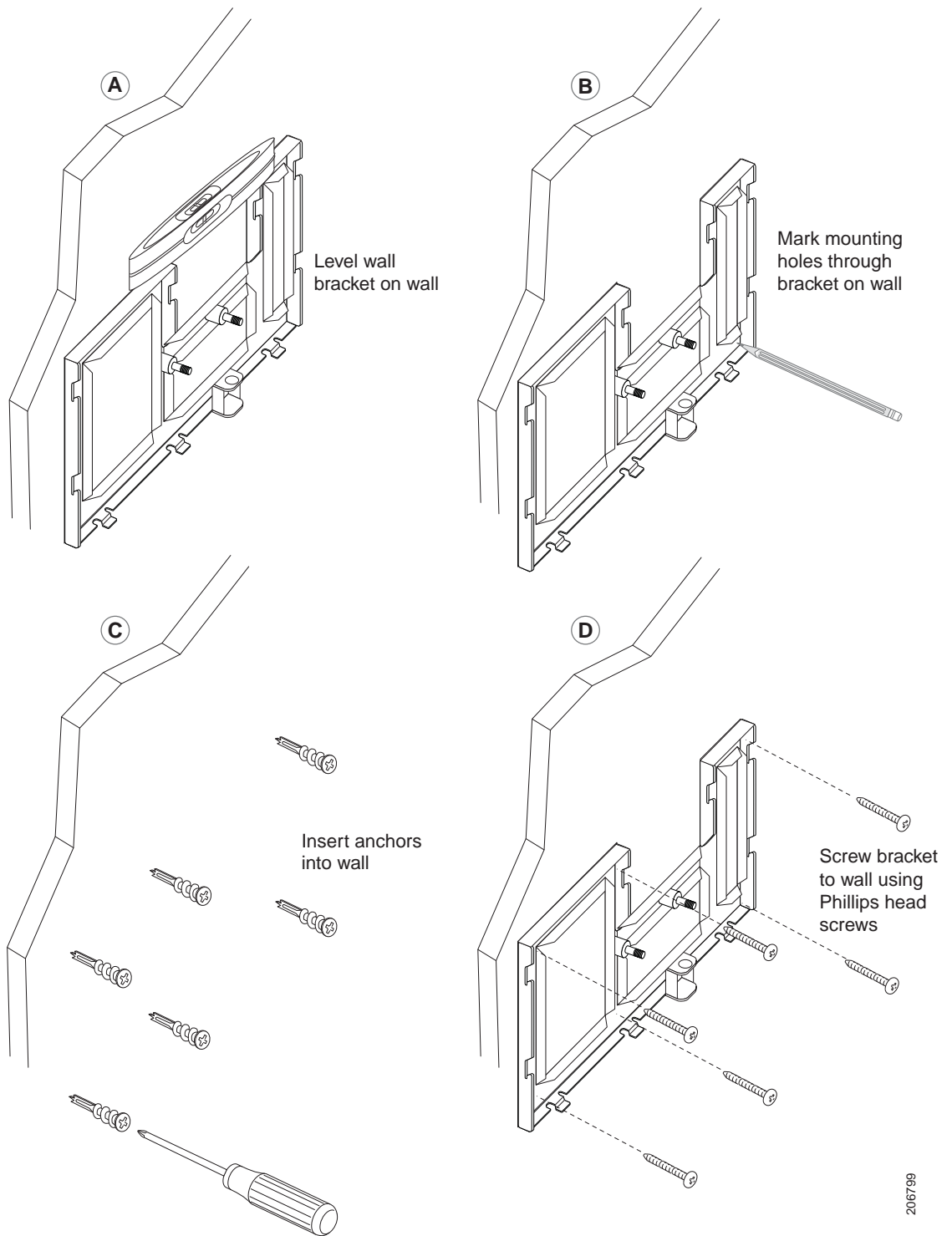
Step 2   Attach the phone bracket to the IP phone and key expansion assembly (Figure E-9).

    a.   Detach the handset cord (and headset cord, if there is a headset), power cord, and any other attached cords from the base of the phone.

    b.   Remove the label covers that are concealing the screw holes.

    c.   Attach the phone bracket by inserting the tabs into the mounting tabs on the phone. The phone's ports should be accessible through the holes in the bracket.

    d.   Secure the phone bracket to the IP Phone with the machine screws.

    e.   Thread the handset cord (and headset cord, if using one). Reattach the cords and seat them in the clips incorporated into the phone body.

Figure E-9   Attaching the Phone Bracket
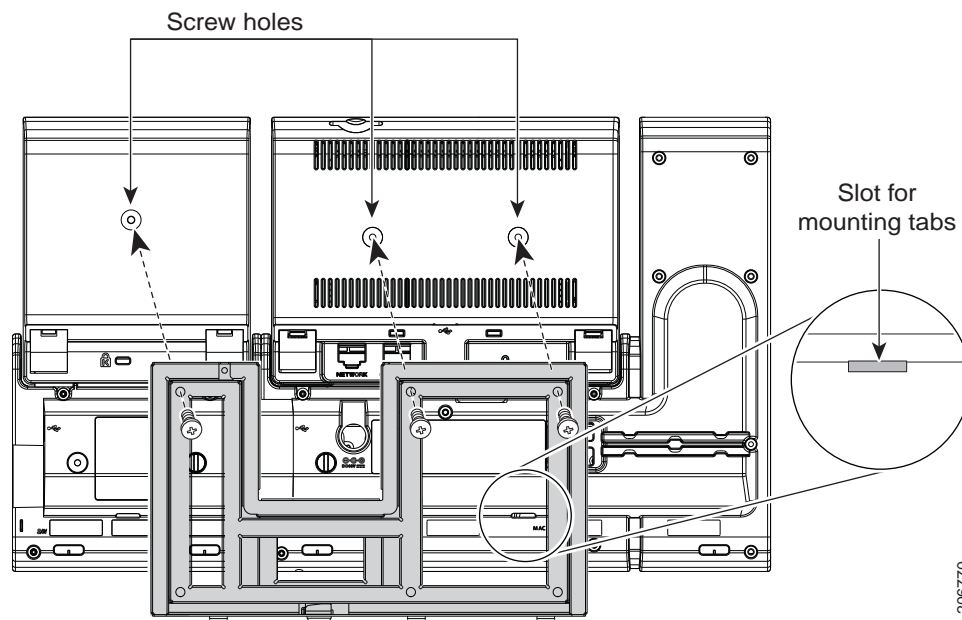
Step 3   Remove the handset wall hook in the handset rest, rotate the hook 180 degrees, and reinsert the hook. The hook should have a lip on which the handset catches when the phone is vertical (Figure E-10).

Figure E-10   Preparing the Handset Hook
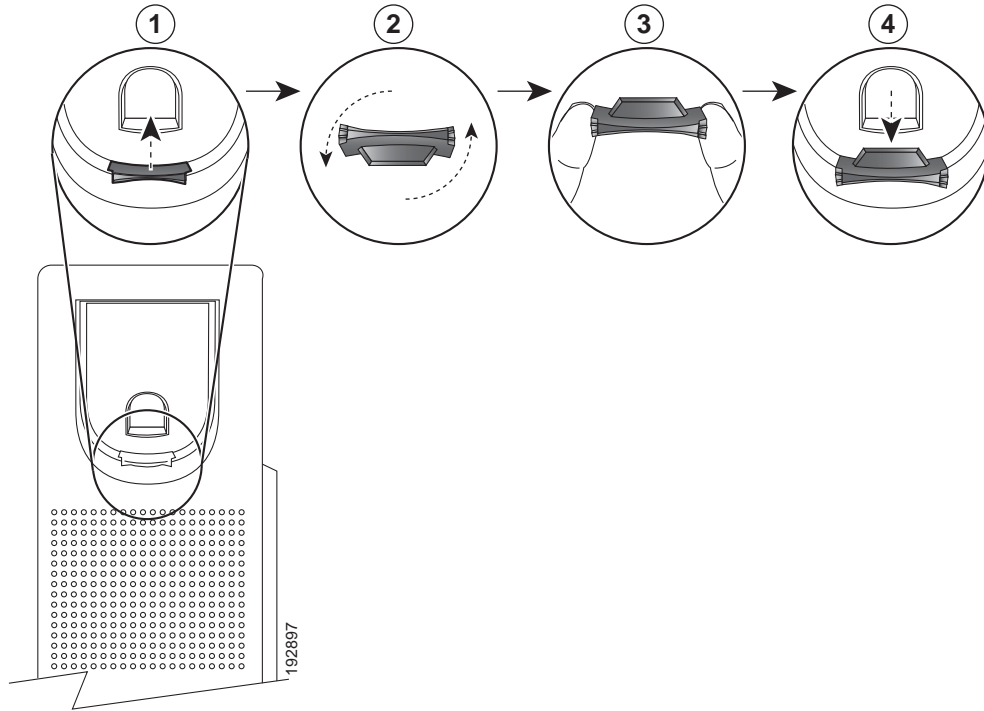
Step 4   Attach the Ethernet cable to the 10/100/1000 SW Network port and wall jack.

If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100/1000 Computer (PC access) port.

If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips incorporated into the phone body next to the port (Figure E-11).

Figure E-11   *Plugging the Power Cord into the Phone*
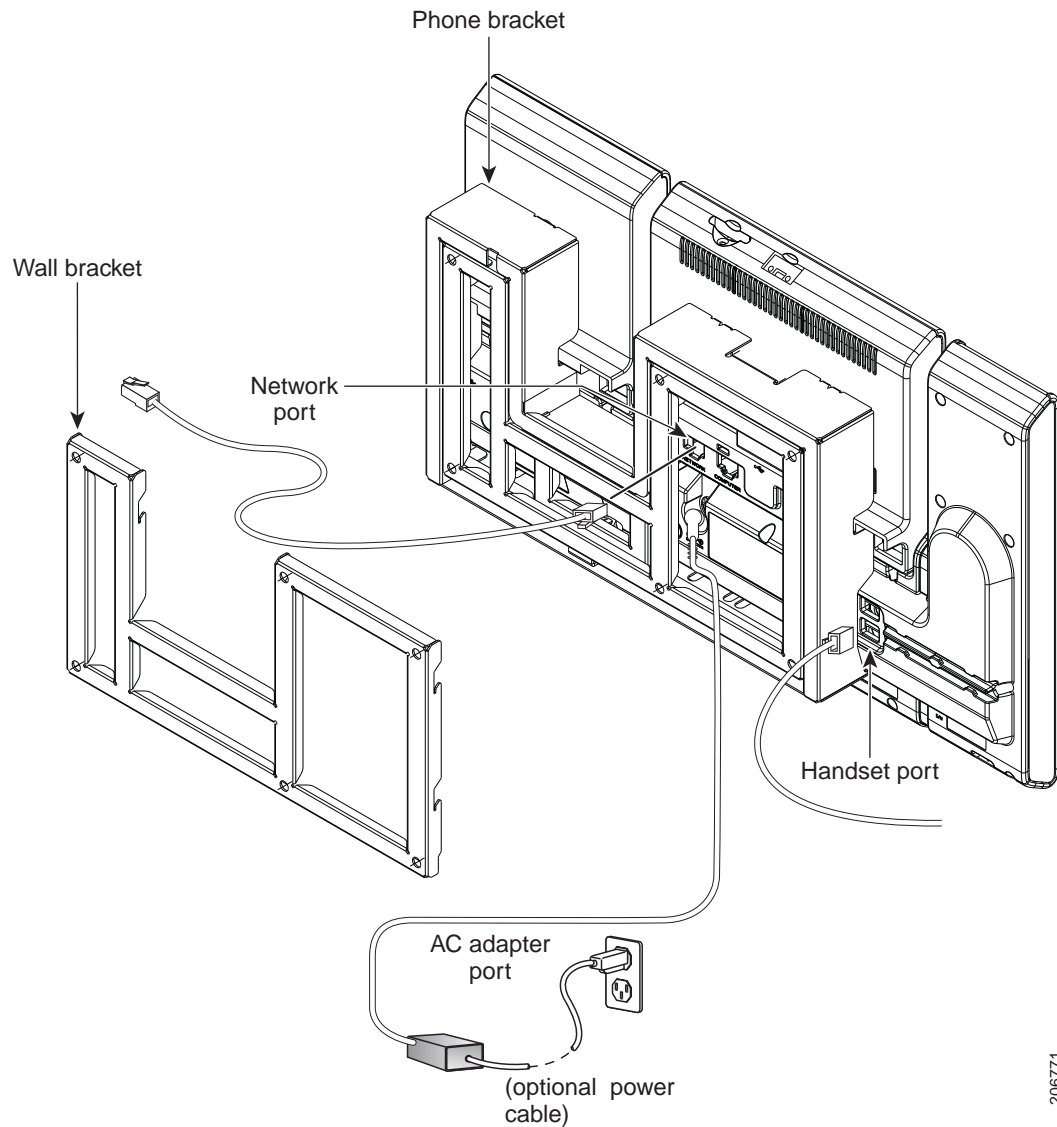
Step 5   Attach the phone to the wall bracket by inserting the tabs on the top of the phone bracket into the slots on the wall bracket. Ensure that the power cord and any other cable that does not terminate in the wall behind the bracket are positioned in one of the cable-access openings in the bottom of the bracket. The phone and wall brackets' openings together form circular openings with room for one cable per opening (Figure E-12).

Step 6   Use the locking key to lock the phone to the wall bracket.

Figure E-12   Attaching the Phone to the Wall Bracket
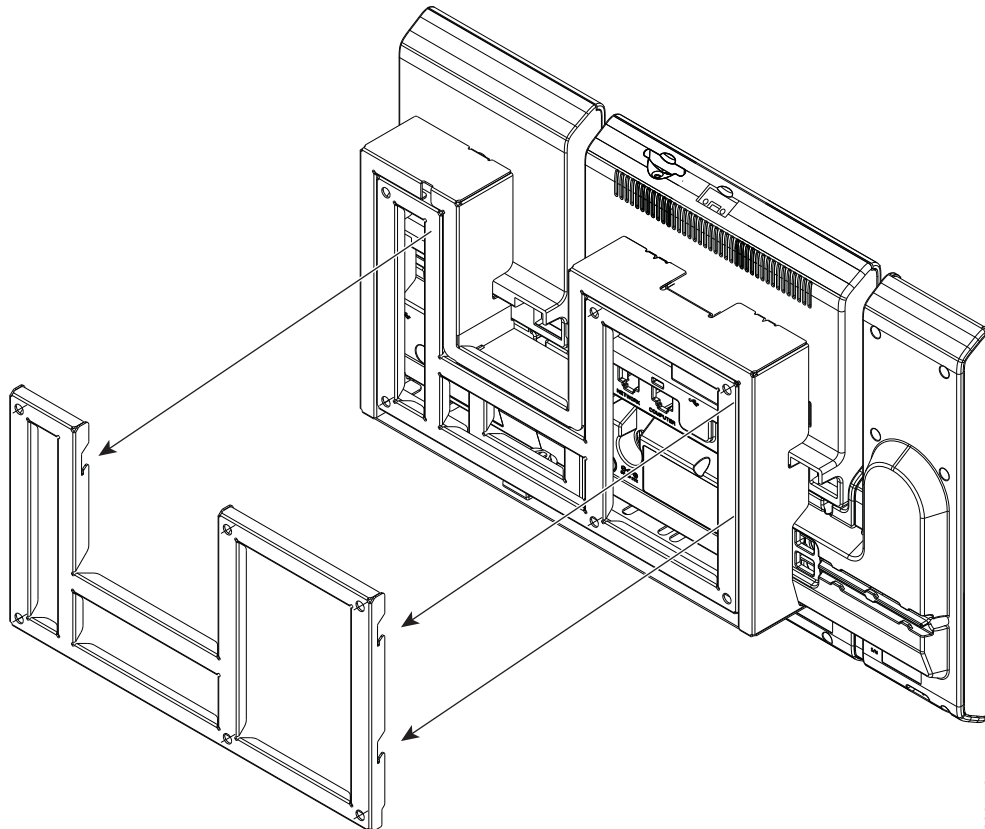
Cisco Unified IP Phone Non-Lockable Wall Mount

This appendix contains information about installing the wall mount for use with the following products:

- ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones: Installed on the Cisco Unified IP Phone 8961, 9951, and 9971.
- ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones plus a single Key Expansion Module: Installed on the Cisco Unified IP Phone 8961, 9951, and 9971 with the Key Expansion Module.

These nonlocking wall mount kits meet ADA 4.4.1 requirements.

ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones

This section describes how to install the non-lockable wall mount kit on a Cisco Unified IP Phone 8961, 9951, and 9971 when the phone is not connected to a Key Expansion Module.

The following figure shows the wall mount kit installed on the phone.

Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 8.5 (SIP)

OL-20861-01 · F-1

Figure F-1   *Back View of ADA Non-Lockable Wall Mount Kit Installed on Phone*
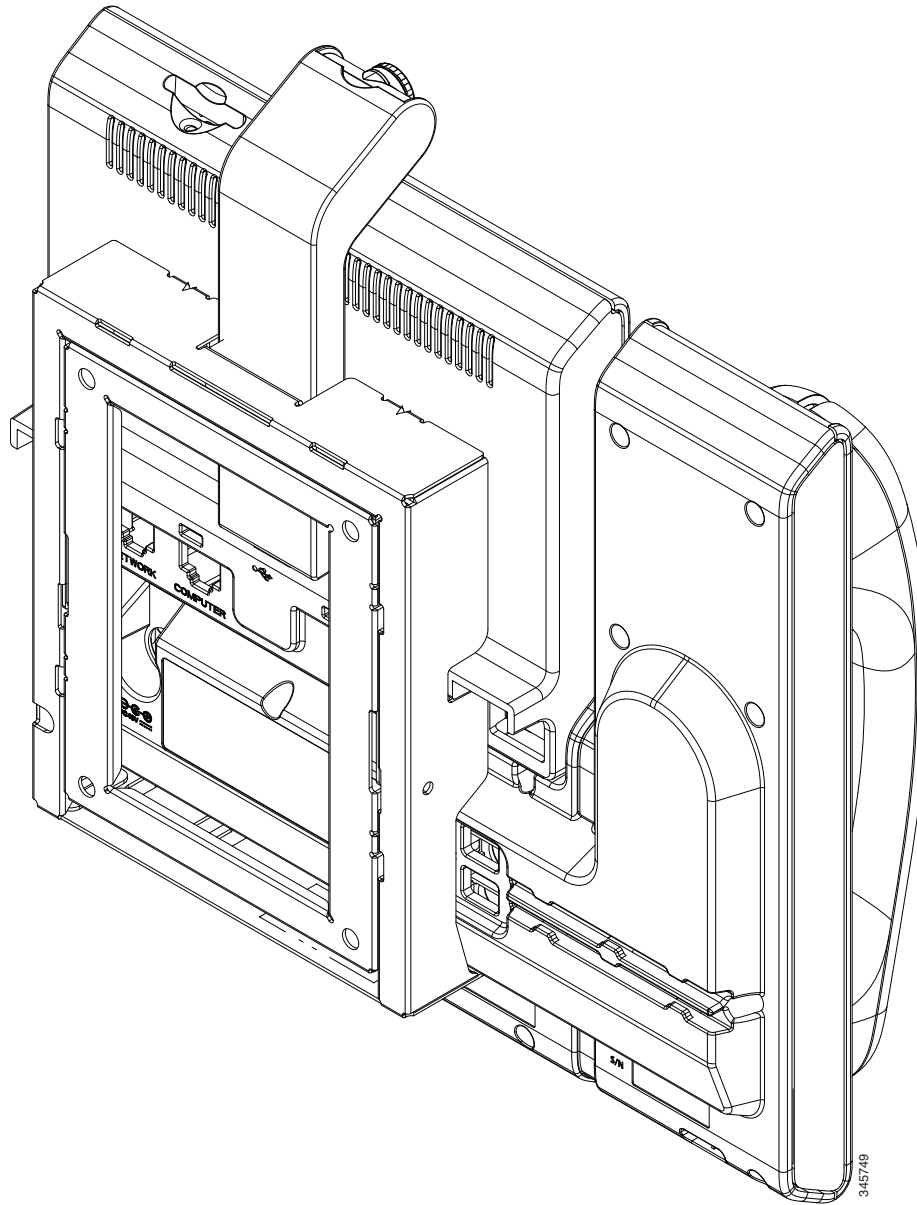
The following figure shows the phone with the wall mount kit from the side.

Figure F-2   *Side View of ADA Non-Lockable Wall Mount Kit Installed on Phone*
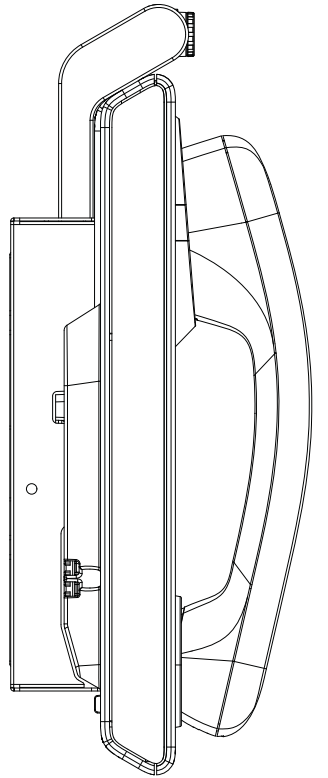
Components

The following figure shows the components of the ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones.

Figure F-3   *Components*
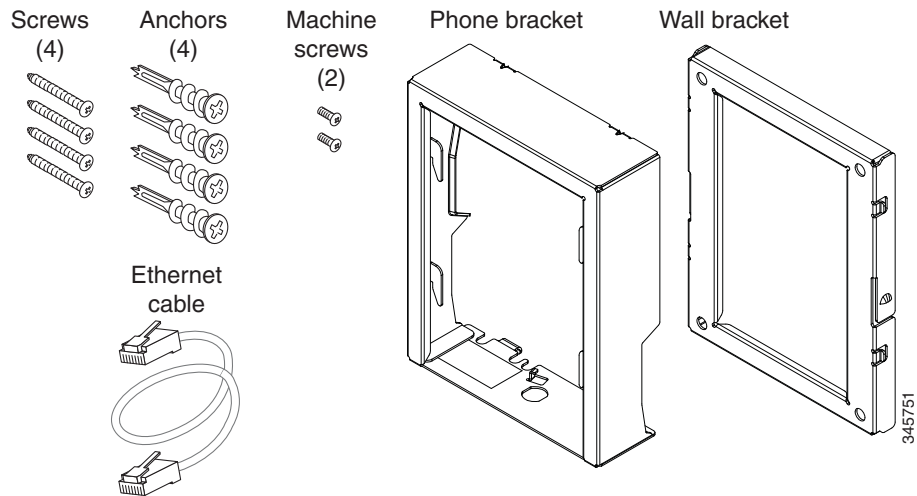
The package contains the following items:

- One phone bracket
- One wall bracket
- Four #8-18 x 1.25-inch Phillips-head screws with four anchors
- Two #4-40 x 0.31-inch machine screws
- One 6-inch Ethernet cable

Before you begin

You need these tools to install the bracket:

- #1 and #2 Phillips-head screwdrivers
- Level
- Pencil

You must also install an Ethernet jack for the telephone in the desired location if an Ethernet jack does not currently exist. This jack must be wired appropriately for an Ethernet connection. You cannot use a regular telephone jack. For more information about phone installation requirements and warnings, see Setting Up the Cisco Unified IP Phone, page 3-1.

Install Non-Lockable Wall Mount for phone

The wall mount kit can be mounted on most surfaces, including concrete, brick, and similar hard surfaces. To mount the kit on concrete, brick, or similar hard surfaces, you must provide the appropriate screws and anchors for your wall surface.

Procedure

Step 1   Mount the wall bracket in the desired location. You can install the bracket over an Ethernet jack, or you can run the Ethernet network cable to a jack nearby.

> ✎
>
> **Note**   If the jack is to be placed behind the phone, the Ether net jack must be flush to the wall or recessed.

a.   Hold the bracket on the wall, placing it so that the arrow on the back of the bracket is pointing up.

b.   Use the level to ensure the bracket is level, then use a pencil to mark the screw holes.

c.   Using a #2 Phillips-head screwdriver, carefully center the anchor over the pencil mark and press the anchor into the wall.

d.   Screw the anchor clockwise into the wall until it is seated flush.

e.   Use the included screws and a #2 Phillips-head screwdriver to attach the bracket to the wall.

The following figure shows the bracket installation steps.

Figure F-4   ***Mount the Wall Bracket***
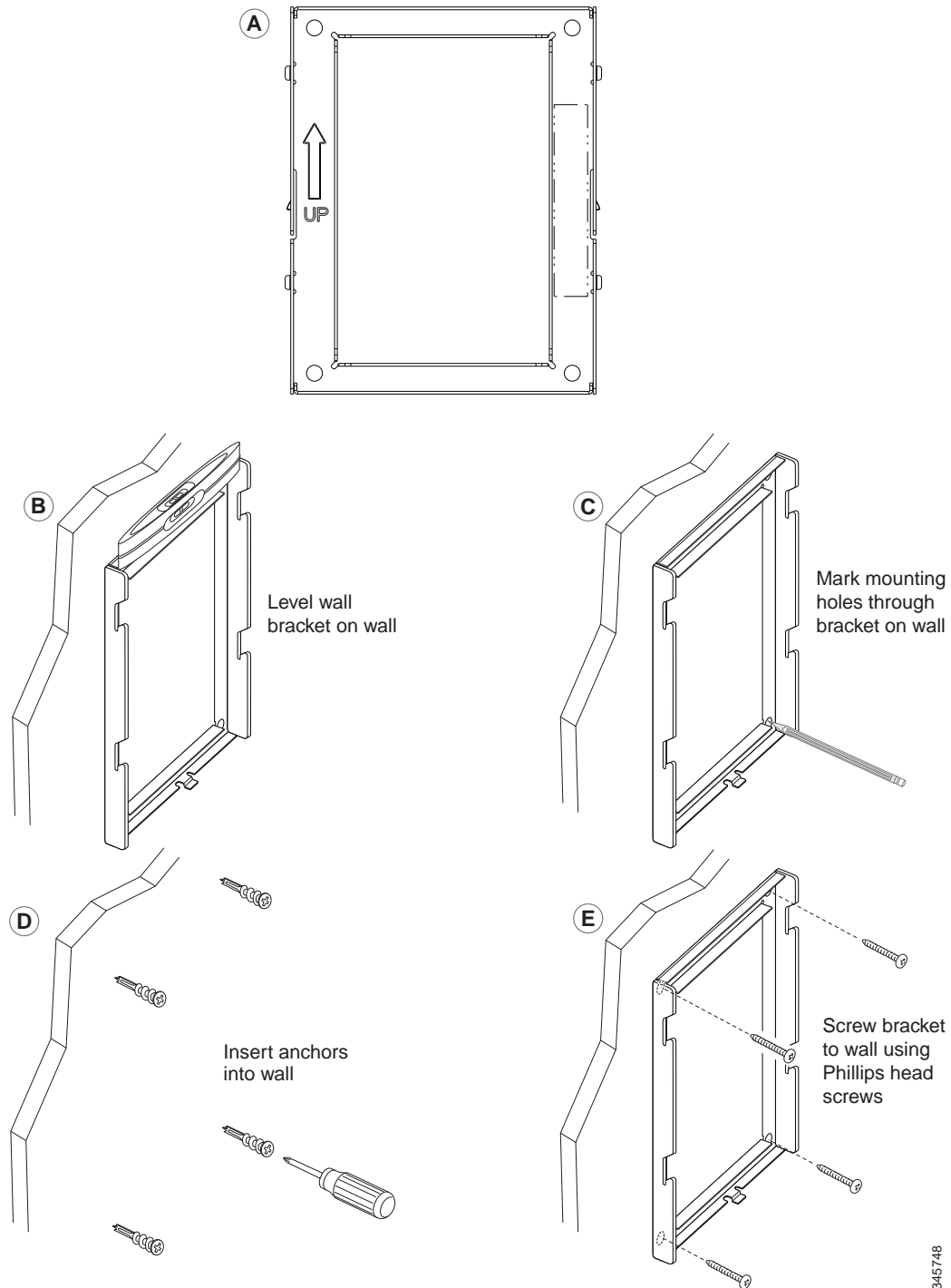
Step 2   Attach the phone bracket to the IP Phone.

    a.   Detach the handset cord (and headset cord, if there is a headset), power cord, and any other attached cords from the base of the phone.

    b.   Remove the label covers that are concealing the screw holes.

   c. Attach the phone bracket by inserting the tabs into the mounting tabs on the phone. The ports of the phone should be accessible through the holes in the bracket.

   d. Secure the phone bracket to the IP Phone with the machine screws, using the #1 Phillips-head screw driver.

   e. Thread the handset cord (and headset cord, if using one). Reattach the cords and seat them in the clips incorporated into the phone body.

The following figure shows how the bracket attaches to the phone.

Figure F-5   Attach the Phone Bracket
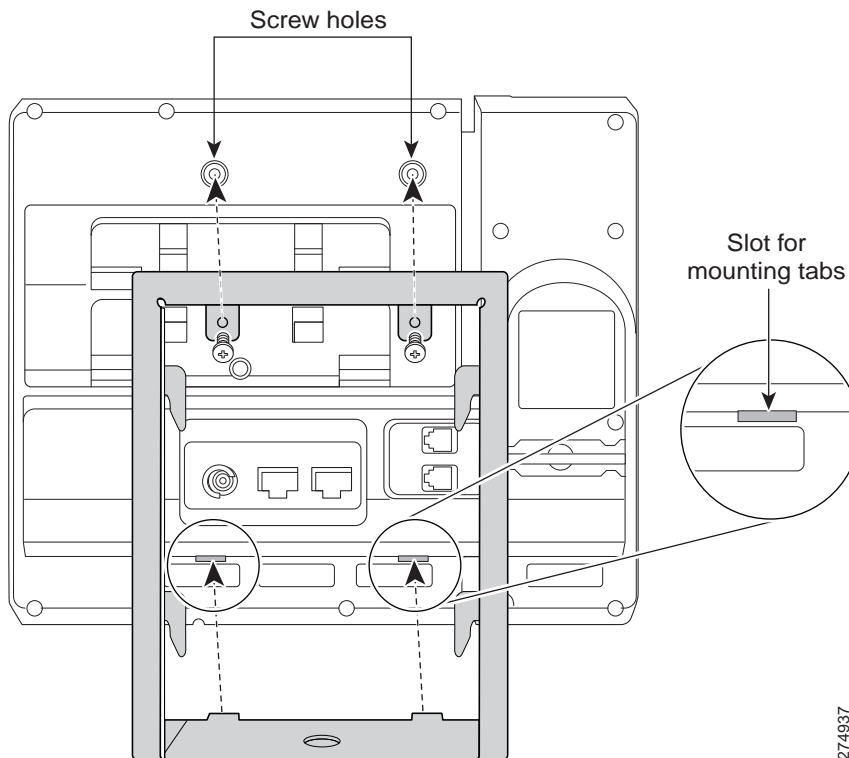
Step 3   Attach the cables to the phone:

   a. Attach the Ethernet cable to the 10/100/1000 SW network port and wall jack.

   b. (Optional) If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100/1000 Computer (PC access) port.

   c. (Optional) If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips that are incorporated into the phone body next to the PC port.

   d. (Optional) If the cables terminate inside the wall bracket, connect the cables to the jacks.

The following figure shows the cables.

■ **Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 8.5 (SIP)**

F-6   **OL-20861-01**

Figure F-6   Attach cables

Step 4   Attach the phone to the wall bracket by inserting the tabs on the top of the phone bracket into the slots on the wall bracket.

For cables that terminate outside of the brackets, use the cable-access openings in the bottom of the bracket to position the power cord and any other cable that does not terminate in the wall behind the bracket. The phone and wall bracket openings together form circular openings with room for one cable per opening.

The following figure shows how you attach the phone to the wall bracket.

Figure F-7   Attach phone to wall bracket
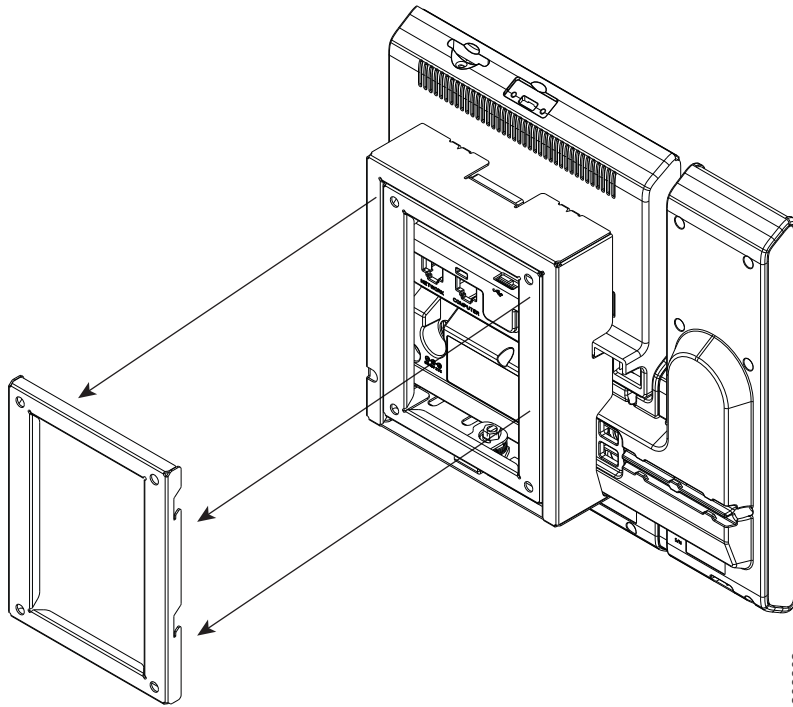
Step 5   Press the phone firmly into the wall bracket and slide the phone down. The tabs in the bracket click into position.

Step 6   Proceed to Step 3 of Installing the Wall Mount for Cisco Unified IP Phone 8961, 9951, and 9971, page E-1.

Remove Phone from Non-Lockable Wall Mount

The phone mounting plate contains two tabs to lock the plate into the wall bracket. The following figure shows the location and shape of the tabs.

Figure F-8   *Figure 23: Tab location*
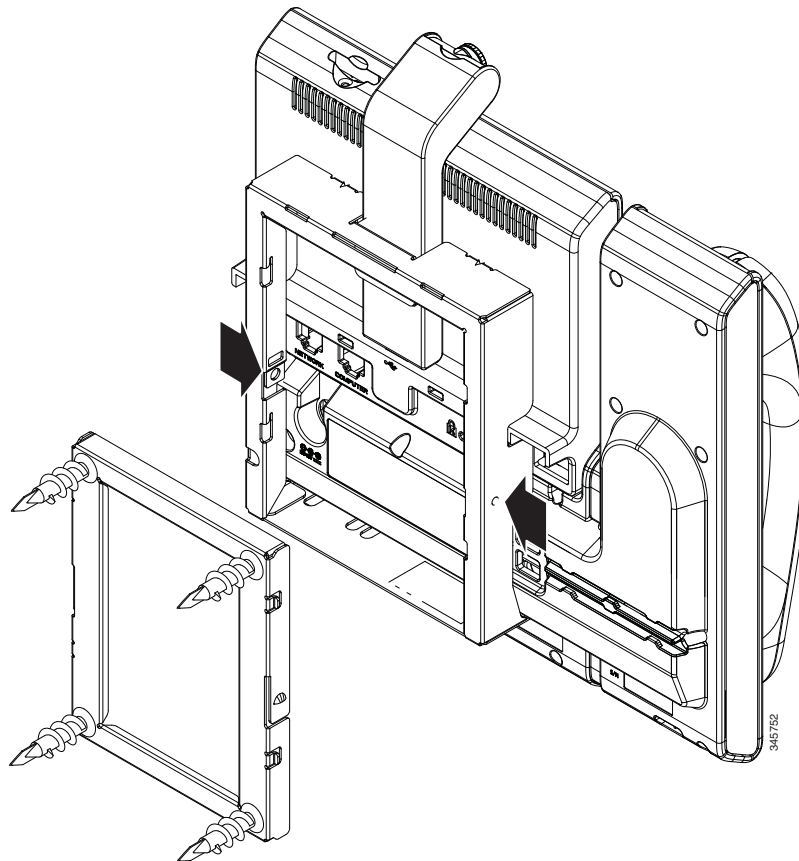
To remove the phone and mounting plate from the wall bracket, you must disengage these tabs.

Before You Begin

You require 2 screwdrivers or metal rods.

Step 1   Push the screw drivers into the left and right holes in the phone mounting plate approximately 1 in. (2.5 cm).

Step 2   Lift the screwdriver handles up to put a downward pressure on the tabs.

Figure F-9   Disengage tabs
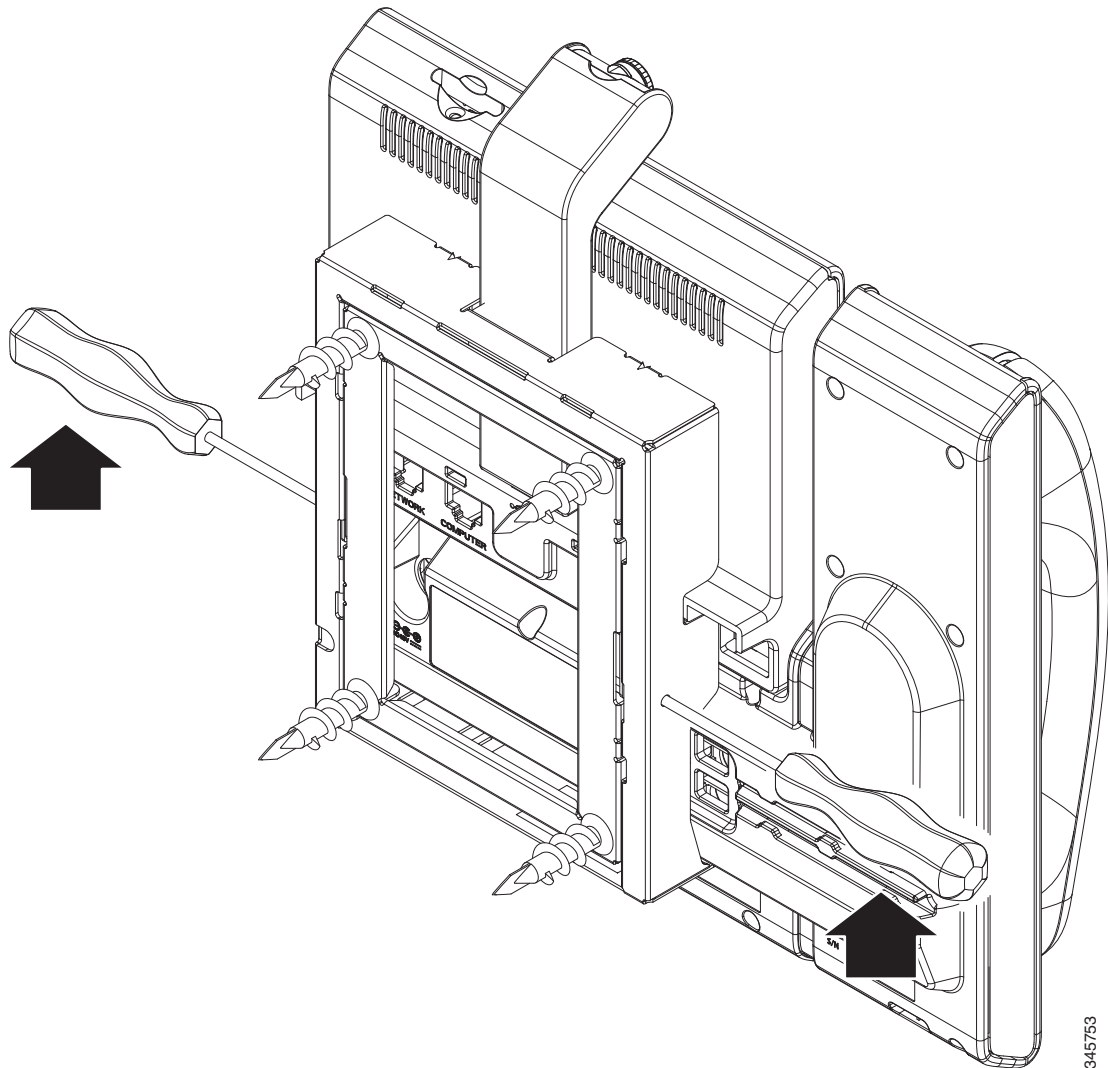
Step 3   Press firmly to disengage the tabs and lift the phone at the same time to release the phone from the wall bracket.

ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones with Key Expansion Module

This section describes how to install the non-lockable wall mount kit on a Cisco Unified IP Phone 8961, 9951, and 9971 when the phone is connected to a Key Expansion Module.

The following figure shows the wall mount kit installed on the phone.

■   **Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 8.5 (SIP)**

F-10

OL-20861-01

Figure F-10   Back View of ADA Non-Lockable Wall Mount Kit Installed on Phone with Key Expansion Module
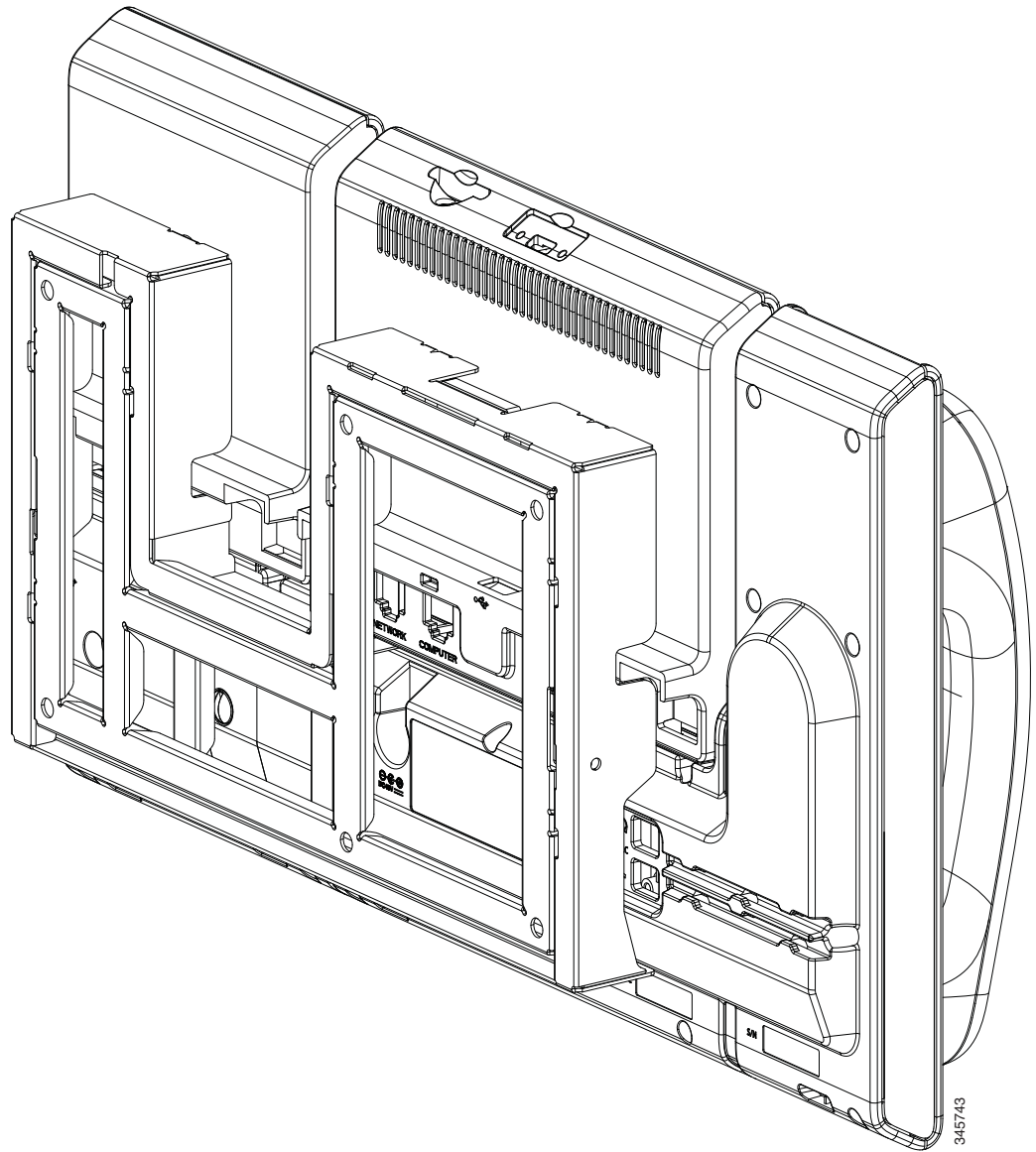
The following figure shows the phone with the wall mount kit from the side.

Figure F-11 ***Side View of ADA Non-Lockable Wall Mount Kit Installed on Phone with Key Expansion Module***
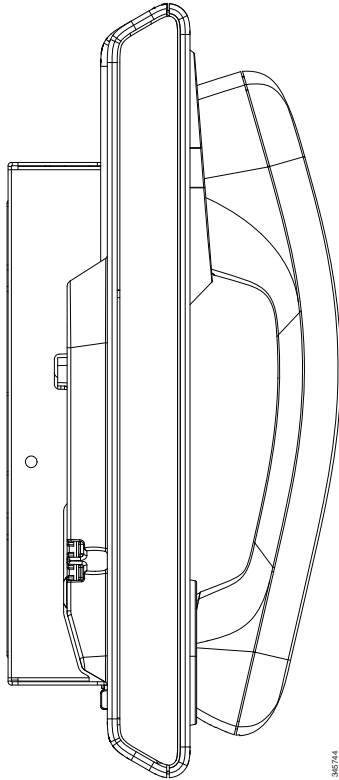
Components

The following figure shows the components of the ADA Non-Lockable Wall Mount Kit for the Cisco Unified IP Phone 8961, 9951, and 9971 with a Key Expansion Module.

Figure F-12 ***Components***

■ **Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 8.5 (SIP)**

F-12

OL-20861-01
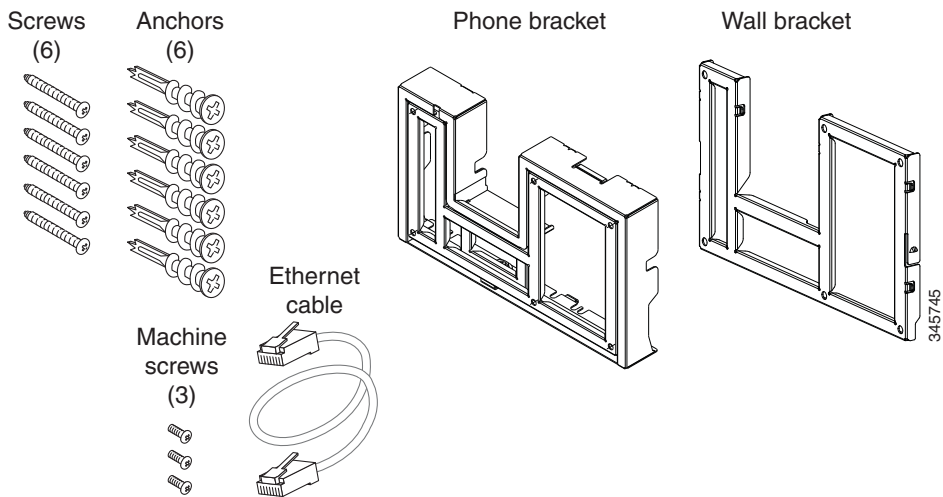
The package contains the following items:

- One phone bracket
- One wall bracket
- Six #8-18 x 1.25-inch Phillips-head screws with six anchors
- Three #4-40 x 0.31-inch machine screws
- One 6-inch Ethernet cable

Before You Begin

You need these tools to install the bracket:

- #1 and #2 Phillips-head screwdrivers
- Level
- Pencil

You must also install an Ethernet jack for the telephone in the desired location if an Ethernet jack does not currently exist. This jack must be wired appropriately for an Ethernet connection. You cannot use a regular telephone jack. For more information about phone installation requirements and warnings, see Setting Up the Cisco Unified IP Phone, page 3-1 and Setting Up the Cisco Unified IP Color Key Expansion Module, page 4-1.

Install Non-Lockable Wall Mount Kit for Phone with Key Expansion Module

The wall mount kit can be mounted on most surfaces, including concrete, brick, and similar hard surfaces. To mount the kit on concrete, brick, or similar hard surfaces, you must provide the appropriate screws and anchors for your wall surface.

Note Be sure to connect to connect the Cisco Unified IP Phone to the Key Expansion Module before installing the phone bracket.

Step 1 Mount the wall bracket in the desired location. You can install the bracket over an Ethernet jack, or you can run the Ethernet network cable to a nearby jack.

Note If the jack is to be placed behind the phone, the Ethernet jack must be flush to the wall or recessed.

   a. Hold the bracket on the wall. See the following figure for the orientation of the wall bracket.

   b. Use the level to ensure that the bracket is level and use a pencil to mark the screw holes.

   c. Using a #2 Phillips-head screwdriver, carefully center the anchor over the pencil mark and press the anchor into the wall.

   d. Screw the anchor clockwise into the wall until it is seated flush.

   e. Use the included screws and a #2 Phillips-head screwdriver to attach the bracket to the wall.

The following figure shows the steps for installing the bracket.

Figure F-13   *Bracket Installation*
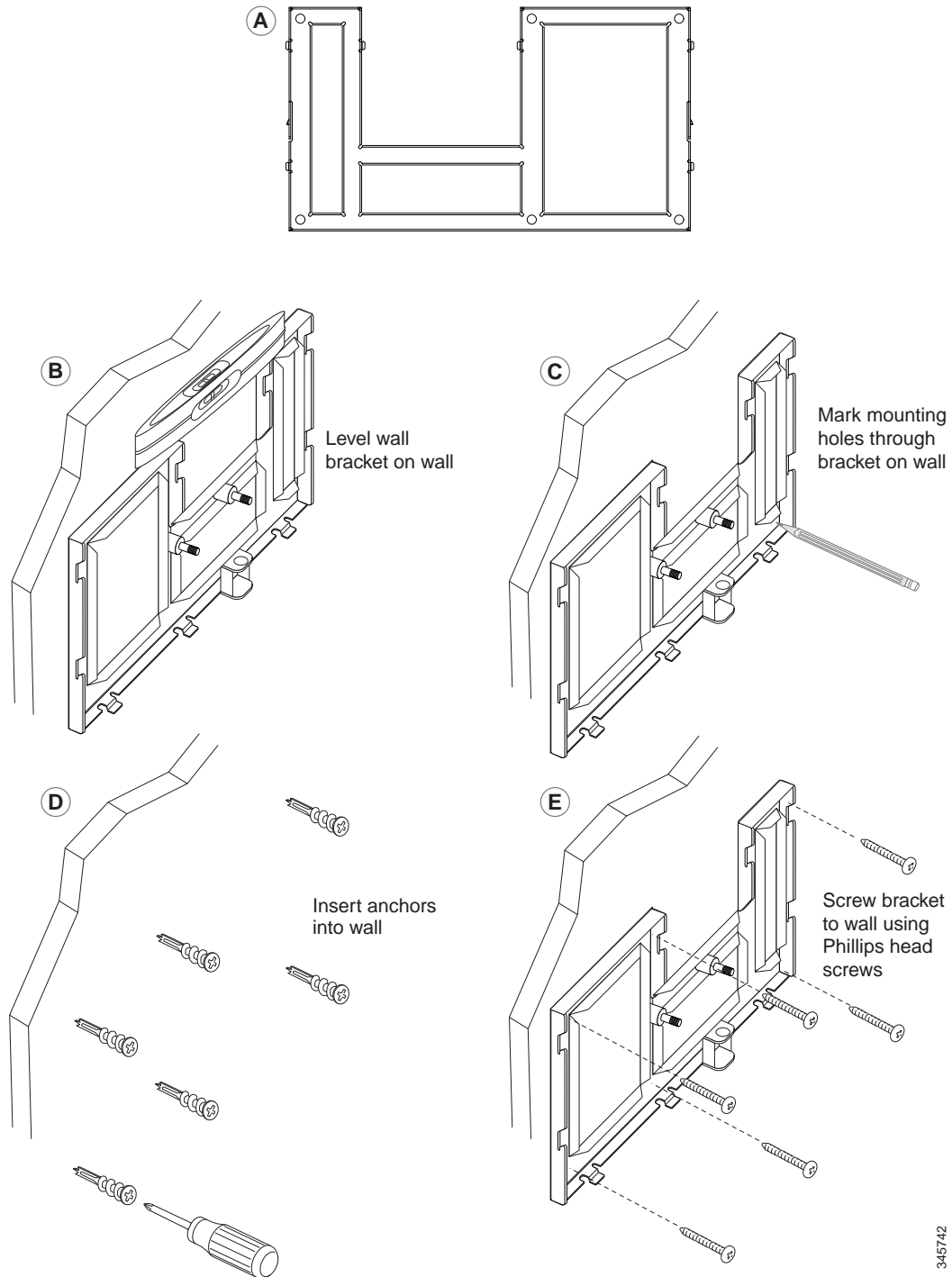
Step 2   Attach the phone bracket to the IP phone and key expansion assembly.

    a. Detach the handset cord (and headset cord, if there is a headset), power cord, and any other attached cords from the base of the phone

    b. Remove the label covers that are conceal the screw holes.

    c. Attach the phone bracket by inserting the tabs into the mounting tabs on the back of the phone. The phone ports should be accessible through the holes in the bracket.

   d. Secure the phone bracket to the IP phone with the machine screws using a #1 Philips-head screwdriver.

   e. Thread the handset cord (and headset cord, if using one). Reattach the cords and seat them in the clips that are incorporated into the phone body.

   The headset and handset connectors should be accessible from outside the wall mount bracket.

The following figure shows the steps to attach the phone bracket.

Figure F-14   Attach Phone Bracket
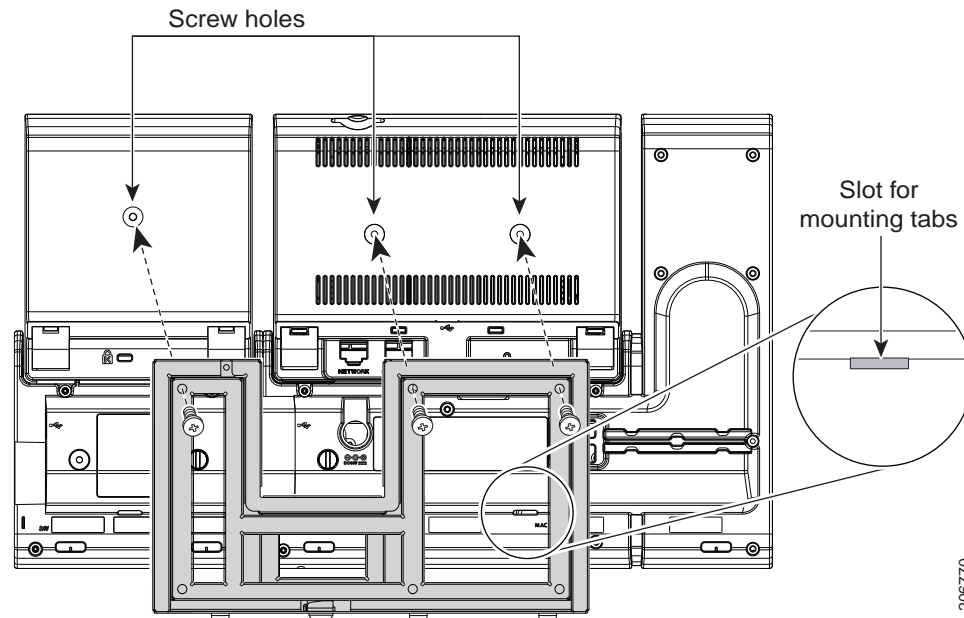
Step 3   Attach the cords.

   a. Attach the Ethernet cable to the 10/100/1000 SW network port and wall jack.

   b. (Optional) If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100/1000 Computer (PC access) port.

   c. (Optional) If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips that are incorporated into the phone body next to the PC port.

   d. (Optional) If the cables terminate inside the wall bracket, connect the cables to the jacks.

The following figure shows the cables.

Figure F-15   Attach Cables
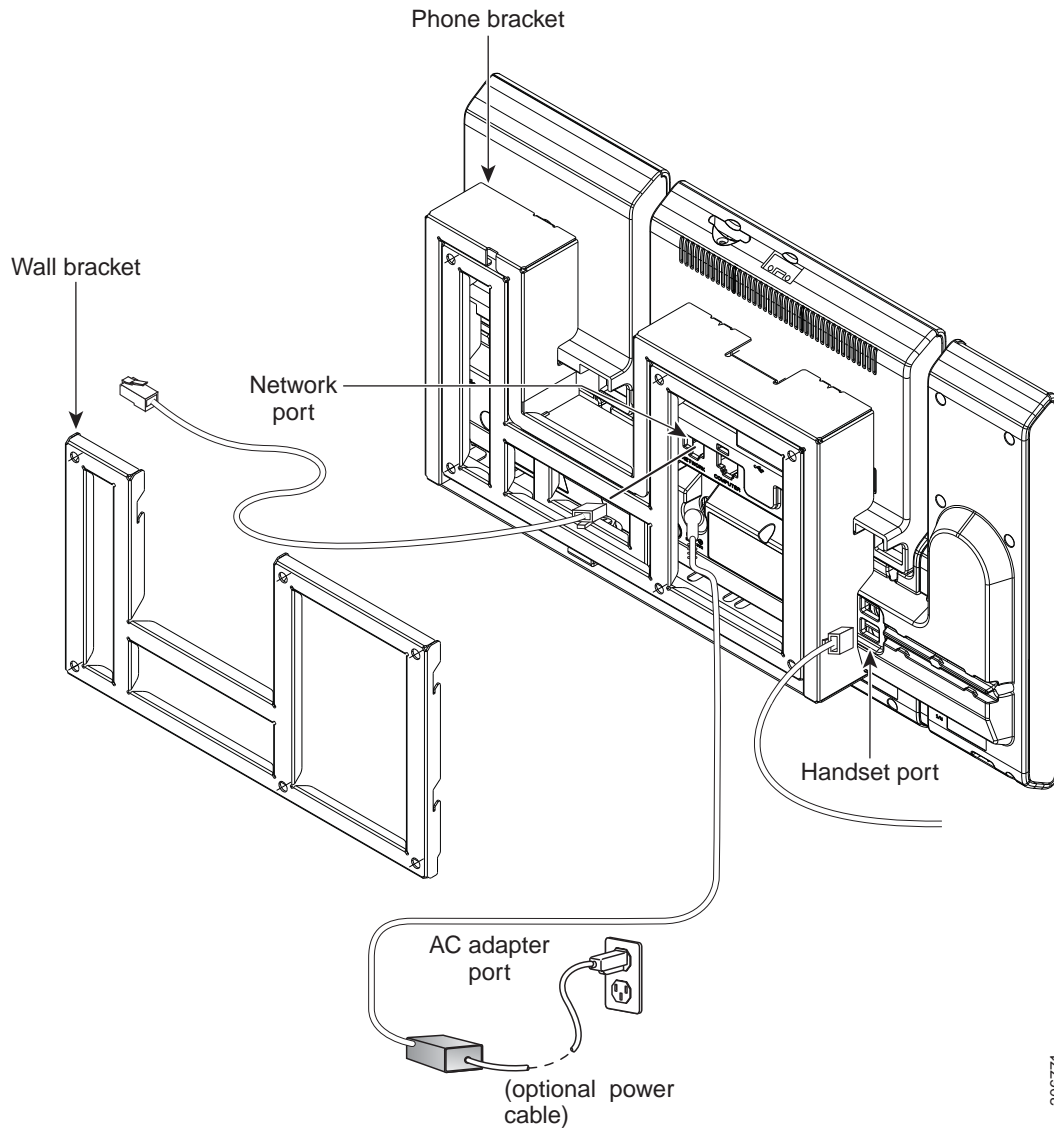
Step 4   Attach the phone to the wall bracket by inserting the tabs on the top of the phone bracket into the slots on the wall bracket.

For cables that terminate outside of the bracket, use the cable-access openings in the bottom of the bracket to position the power cord and any other cable that does not terminate in the wall behind the bracket. The phone and wall bracket openings together form circular openings with room for one cable per opening.

Figure F-16   Attach Phone to Wall Bracket
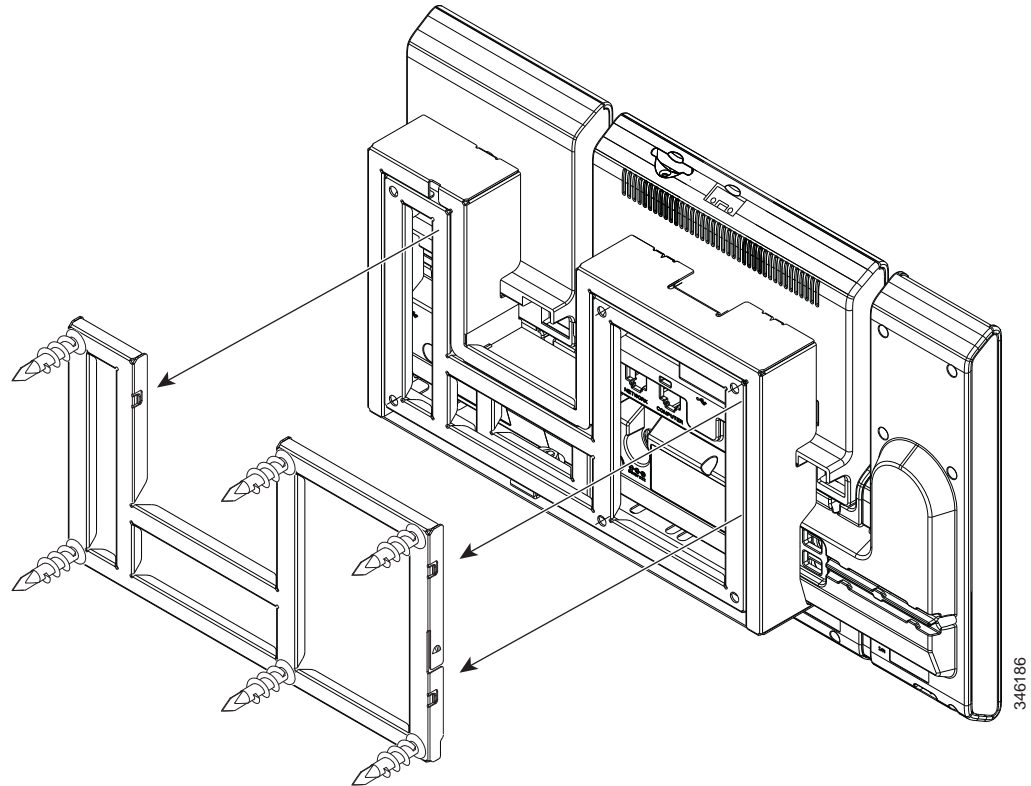
Step 5   Proceed to Step 3 of Installing a Wall Mount for a Phone with a Key Expansion Module, page E-8.

Remove Phone and Key Expansion Module from Non-Lockable Wall Mount

The phone mounting plate contains two tabs to lock the plate into the wall bracket. The following figure shows the location and shape of the tabs.

Figure F-17   Tab Location
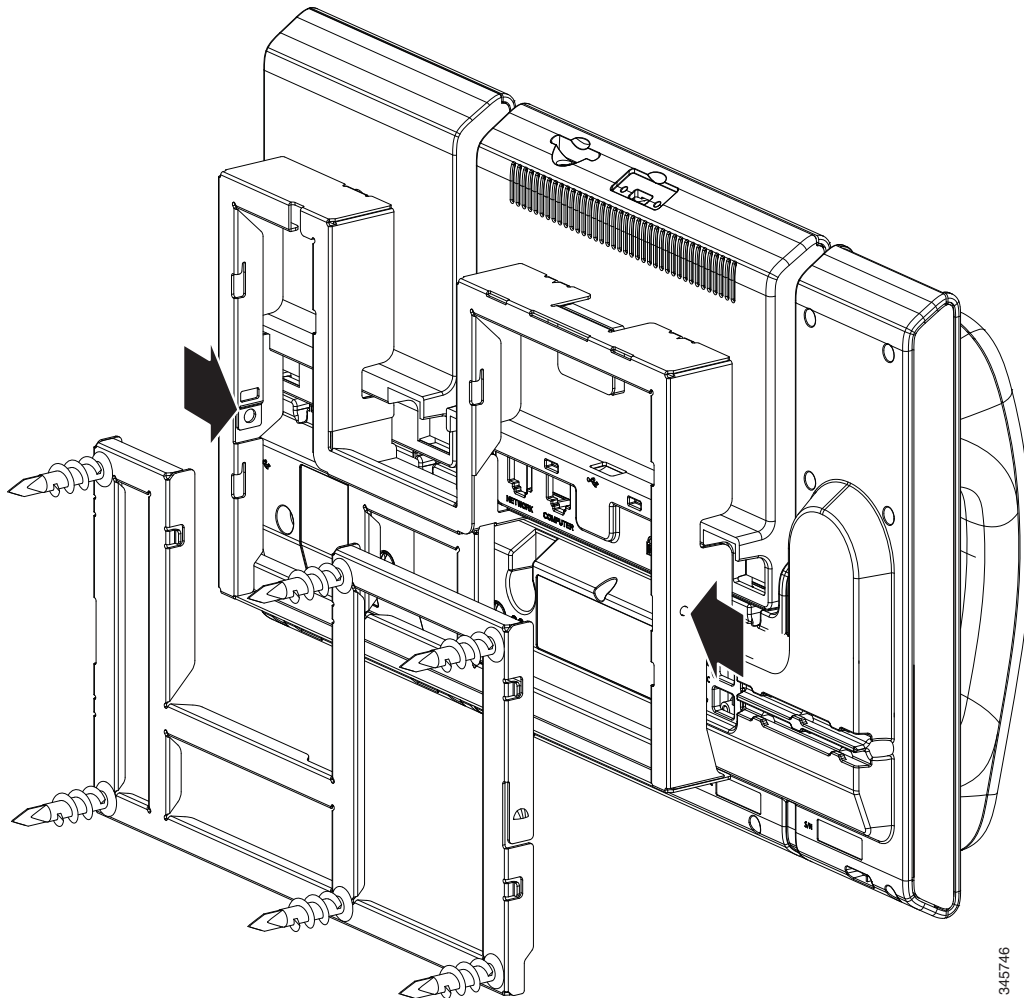
To remove the phone and mounting plate from the wall bracket, you must disengage these tabs.

Before You Begin

You require two screwdrivers or metal rods.

Step 1   Push the screw drivers into the left and right holes in the phone mounting plate until you feel resistance.

Step 2   Press firmly inwards (towards the phone) to disengage the tabs, lift up on the phone to release the phone from the wall bracket, and then pull the phone towards you.

Figure F-18   Disengage Tabs

I N D E X