Cisco Unified IP Phone 6921, 6941, 6945, and 6961 Administration Guide for Cisco Unified Communications Manager 9.0 (SCCP and SIP)

First Published: January 07, 2012

Last Modified: April 18, 2013

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

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: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco 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.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

CONTENTS

Preface

Overview

Cisco Unified IP Phone 6921, 6941, 6945, and 6961 Administration Guide for Cisco Unified Communications Manager (SCCP and 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.

Related Topics

Related documentation, on page xv

Audience

Network engineers, system administrators, and telecom engineers should review this guide to learn the steps that are required to set up Cisco Unified IP Phones. The tasks described in this document involve configuring network settings that are not intended for phone users. The tasks in this manual require a familiarity with Cisco Unified Communications Manager.

Organization

This manual is organized as follows.

Chapter	Description
Cisco Unified IP Phone, on page 1	Provides a conceptual overview and description of the Cisco Unified IP Phone 6921, 6941, 6945, and 6961.
Cisco Unified IP Phones and telephony networks, on page 47	Describes how the Cisco Unified IP Phone interacts with other key IP telephony components, and provides an overview of the tasks required before installation.
Cisco Unified IP Phone Setup, on page 61	Describes how to install and configure the Cisco Unified IP Phone on your network properly and safely.
Cisco Unified IP Phone Settings, on page 71	Describes how to configure network settings, verify status, and make global changes to the Cisco Unified IP Phone.
Features, Templates, Services, and User Setup, on page 89	Provides an overview of procedures for configuring telephony features, configuring directories, configuring phone button and softkey templates, setting up services, and adding users to Cisco Unified Communications Manager.
Cisco Unified IP Phone Customization, on page 131	Explains how to customize phone ring sounds and the phone idle display at your site.
Cisco Unified IP Phone Model Information, Status, and Statistics, on page 139	Explains how to view model information, status messages, network statistics, and firmware information from the Cisco Unified IP Phone.
Remote Monitoring, on page 153	Describes the information that you can obtain from the phone web page to remotely monitor the operation of a phone and to assist with troubleshooting.
Troubleshooting and Maintenance, on page 169	Provides tips for troubleshooting the Cisco Unified IP Phone and the Cisco Unified IP Phone Expansion Modules.
Internal support Web Site, on page 193	Provides suggestions for setting up a website to provide users with important information about their Cisco Unified IP Phones.
International User Support, on page 199	Provides information about setting up phones in non–English environments.
Technical Specifications, on page 201	Provides technical specifications of the Cisco Unified IP Phone.
Basic phone administration steps, on page 205	Provides procedures for basic administration tasks such as adding a user and phone to Cisco Unified Communications Manager and then associating the user to the phone.
Cisco Unified IP Phone 6921, 6941, 6945, and 6961 Wall Mount Kit, on page 211	Contains instructions for installing the wall mount for the Cisco Unified IP Phone.
Feature support by protocol, on page 229	Provides information about feature support for the Cisco Unified IP Phone.

Related documentation

Use the following sections to obtain related information.

Cisco Unified IP Phone 6900 Series documentation

Refer to publications that are specific to your language, phone model and Cisco Unified Communications Manager release. Navigate from the following documentation URL:

http://www.cisco.com/en/US/products/ps10326/tsd_products_support_series_home.html

Cisco Unified Communications Manager documentation

See the *Cisco Unified Communications Manager Documentation Guide* and other publications that are specific to your Cisco Unified Communications Manager release. Navigate from the following documentation URL:

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

Cisco Business Edition 3000 documentation

See the *Cisco Business Edition 3000 Documentation Guide* and other publications that are specific to your Cisco Business Edition 3000 release. Navigate from the following documentation URL:

http://www.cisco.com/en/US/products/ps11370/tsd_products_support_series_home.html

Cisco Business Edition 5000 documentation

See the *Cisco Business Edition 5000 Documentation Guide* and other publications that are specific to your Cisco Business Edition 5000 release. Navigate from the following URL:

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

Cisco Business Edition 6000 documentation

Refer to the *Cisco Business Edition 6000 Documentation Guide* and other publications that are specific to your Cisco Business Edition 6000 release. Navigate from the following URL:

http://www.cisco.com/en/US/products/ps11369/tsd_products_support_series_home.html

Documentation, support, and security guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, reviewing 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.

Guide 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.
input font	Information you must enter is in input 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:

Attention 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

CHAPTER 1

Cisco Unified IP Phone

The Cisco Unified IP Phone 6921, 6941, 6945, and 6961 provides voice communication over an 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, and call forward. In addition, because the phone is connected to your data network, it offers enhanced IP telephony features, including access to network information and services, and customizable features and services.

A Cisco Unified IP Phone, like other network devices, must be configured and managed. These phones encode G.711a, G.711u, G.729, G.729a, G.729ab, and iLBC codecs, and decode G.711a, G.711u, G.729, G.729a, G.729ab, and iLBC codecs. These phones encode and decode the codecs in similar manner.

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

This chapter includes the following topics:

Cisco Unified IP Phone 6921, 6941, 6945, and 6961

This section describes the components of the phones.

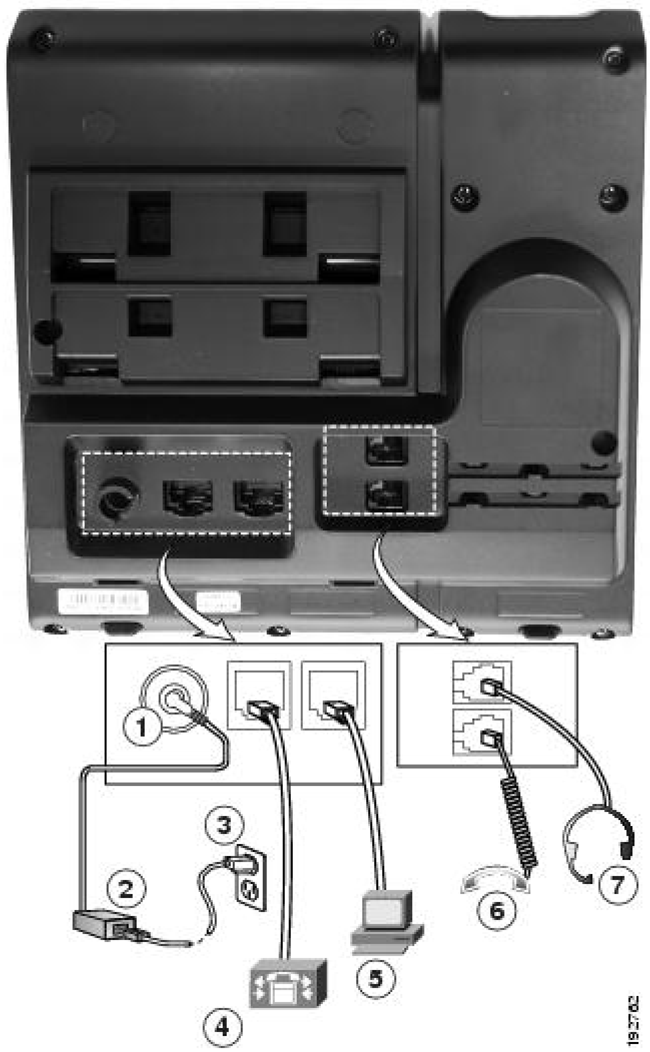
Cisco Unified IP Phone 6921

The following sections describe the features available on the Cisco Unified IP Phone 6921.

Phone Connections

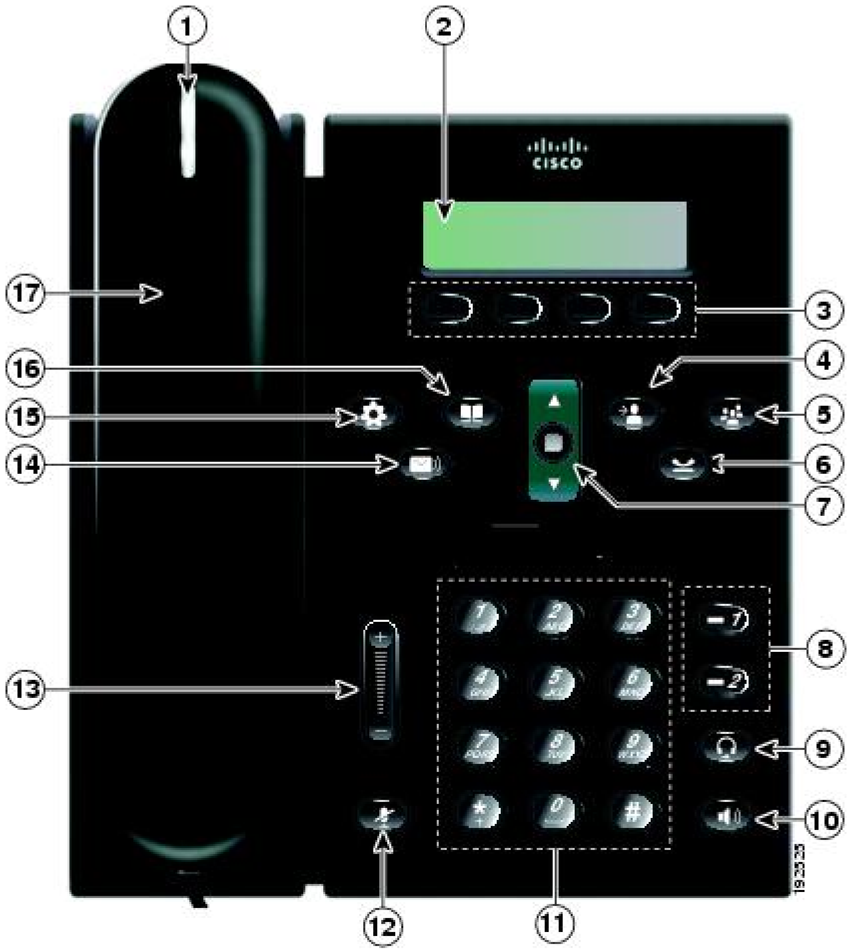
For your phone to work, it must be connected to the corporate IP telephony network.

Figure 1: Cisco IP Phone 6921 and 6941 connections



1	DC adaptor port (DC48V).	5	Access port (10/100 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 SW) connection. IEEE 802.3af power enabled.		

Buttons and hardware

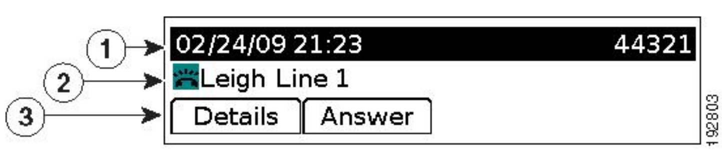


1	Handset light strip	Indicates an incoming call (flashing red) or new voice message (steady red).
2	Phone screen	Shows information about your phone such as directory number, active call and line status, softkey options, speed dials, placed calls, and phone menu listings.
3	Softkey buttons 	Depending on how your system administrator sets up the phone, enable softkey options displayed on your phone screen.
4	Transfer button 	Transfers a call.

5	Conference button 	Creates a conference call.
6	Hold button 	Places an active call on hold.
7	Navigation bar and Select button 	The Navigation bar allows you to scroll through menus and highlight items. When phone is on hook, displays phone numbers from your Placed Call listing (up arrow) or your speed dials (down arrow). The Select button (in the middle of the Navigation bar) allows you to select a highlighted item.
8	Line 1 and Line 2 buttons  	Line 1 selects the primary phone line. Depending on how your system administrator sets up the phone, Line 2 may provide access to: • Secondary phone line • Speed-dial number (speed-dial button) • Web-based service (for example, a Personal Address Book button) Buttons illuminate to indicate status: • Green, steady: Active call • Green, flashing: Held call • Amber, flashing: Incoming call or reverting call • Red, steady: Remote line in use (shared line) • Red, flashing: Remote line on hold
9	Headset button 	Toggles the headset on or off. When the headset is on, the button is lit.
10	Speakerphone button 	Toggles the speakerphone on or off. When the speakerphone is on, the button is lit.

11	Keypad	Allows you to dial phone numbers, enter letters, and select menu items (by entering the item number).
12	Mute button 	Toggles the microphone on or off. When the microphone is muted, the button is lit.
13	Volume button 	Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook). Your administrator sets a minimum ringer volume level ranging from 0 to 14. The default level is 0 (silent). You can only adjust the ringer volume to a level greater than the configured minimum ring volume value.
14	Messages button 	Autodials your voicemail system (varies by system).
15	Applications button 	Opens or closes the Applications menu. Use the Applications button to access call history, user preferences, phone settings, and phone model information.
16	Contacts button 	Opens or closes the Directories menu. Use the Contacts button to access personal and corporate directories.
17	Handset	Phone handset.

Phone Screen



1	Header	Displays date, time, and directory number.

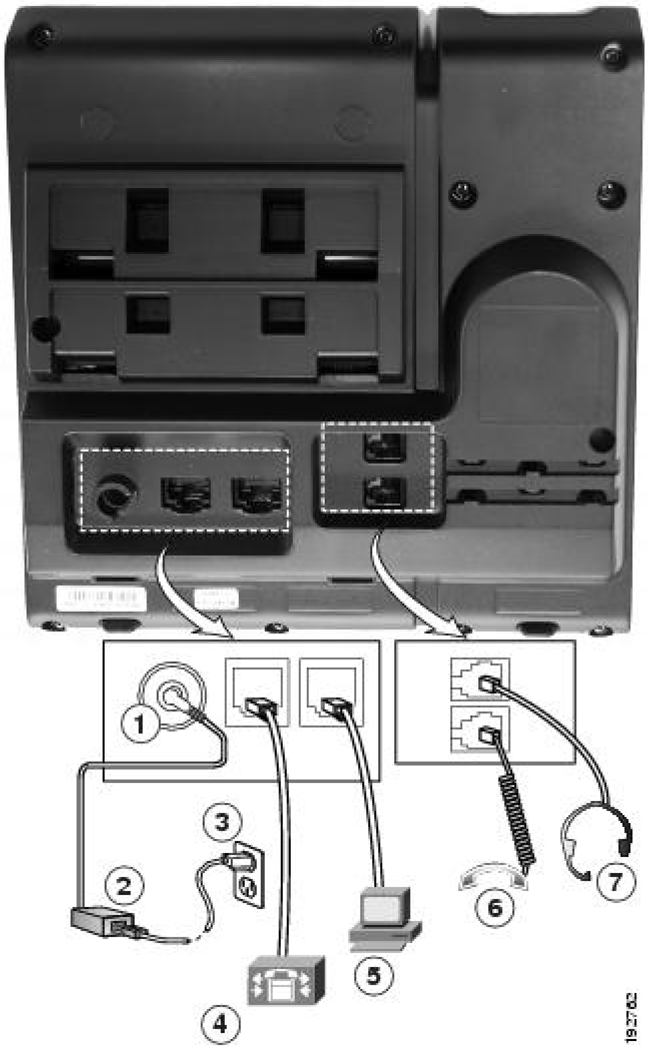
2	Line details and other phone information	During a call, displays details for the active line. If not on a call, displays line text label and other information such as placed calls, speed dials, and phone menu listings. The IP phone LCD display size limits the length of calling ID and calling number that are displayed. If the calling number is restricted, the phone displays only the calling ID. If the calling number is unrestricted and the calling ID is restricted, the phone displays the calling ID as `Unknown`. If the calling number and the calling ID are unrestricted, but the calling ID is not configured, the phone displays only the calling number.
3	Softkey labels	Display softkeys for available features or actions.

Cisco Unified IP Phone 6941

The Cisco Unified IP Phone 6941 provides the following features.

Phone Connections

For your phone to work, it must be connected to the corporate IP telephony network.



1	DC adaptor port (DC48V).	5	Access port (10/100 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 SW) connection. IEEE 802.3af power enabled.		

Buttons and hardware

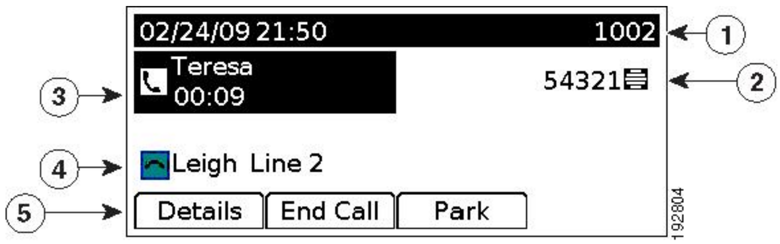
1	Handset light strip	Indicates an incoming call (flashing red) or new voice message (steady red).
2	Phone screen	Shows information about your phone such as directory number, active call and line status, softkey options, speed dials, placed calls, and phone menu listings.

3	Programmable feature buttons  	Depending on how your system administrator sets up the phone, programmable feature buttons (on each side of the phone screen) provide access to: • Phone lines and intercom lines • Speed-dial numbers (speed-dial buttons, including the Line Status speed-dial features) • Web-based services (for example, a Personal Address Book button) • Call features (for example, a Privacy button) Buttons illuminate to indicate status: • Green, steady: Active call or two-way intercom call • Green, flashing: Held call • Amber, steady: Privacy in use, one-way intercom call, DND active, or logged into Hunt Group • Amber, flashing: Incoming call or reverting call • Red, steady: Remote line in use (shared line or Line Status) • Red, flashing: Remote line on hold
4	Softkey buttons 	Depending on how your system administrator sets up the phone, enable softkey options displayed on your phone screen.
5	Transfer button 	Transfers a call.
6	Conference button 	Creates a conference call.
7	Hold button 	Places an active call on hold.

8	Navigation bar and Select button 	The Navigation bar allows you to scroll through menus and highlight items. When phone is on hook, displays phone numbers from your Placed Call listing (up arrow) or your speed dials (down arrow). The Select button (in the middle of the Navigation bar) allows you to select a highlighted item.
9	Headset button 	Toggles the headset on or off. When the headset is on, the button is lit.
10	Speakerphone button 	Toggles the speakerphone on or off. When the speakerphone is on, the button is lit.
11	Keypad	Allows you to dial phone numbers, enter letters, and select menu items (by entering the item number).
12	Mute button 	Toggles the microphone on or off. When the microphone is muted, the button is lit.
13	Volume button 	Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook). Your administrator sets a minimum ringer volume level ranging from 0 to 14. The default level is 0 (silent). You can only adjust the ringer volume to a level greater than the configured minimum ring volume value.
14	Messages button 	Autodials your voice messaging system (varies by system).
15	Applications button 	Opens or closes the Applications menu. Use the Applications button to access call history, user preferences, phone settings, and phone model information.
16	Contacts button 	Opens or closes the Directories menu. Use the Contacts button to access personal and corporate directories.

17	Handset	Phone handset.

Phone Screen



1	Header	Displays date, time, and directory number.
2	Line text label with icon	Displays text label and icon for phone or intercom line, speed-dial numbers, or services, depending on your configuration.
3	Primary line details and other phone information	Displays line label and call details for the primary line, and other phone information such as placed calls, speed dials, and phone menu listings. The IP phone LCD display size limits the length of calling ID and calling number that are displayed. If the calling number is restricted, the phone displays only the calling ID. If the calling number is unrestricted and the calling ID is restricted, the phone displays the calling ID as `Unknown`. If the calling number and the calling ID are unrestricted, but the calling ID is not configured, the phone displays only the calling number.

4	Secondary line details and other phone information	Displays line label and call details for the secondary line, and other phone information such as placed calls, speed dials, and phone menu listings. The IP phone LCD display size limits the length of calling ID and calling number that are displayed. If the calling number is restricted, the phone displays only the calling ID. If the calling number is unrestricted and the calling ID is restricted, the phone displays the calling ID as `Unknown`. If the calling number and the calling ID are unrestricted, but the calling ID is not configured, the phone displays only the calling number.
5	Softkey labels	Display softkeys for available features or actions.

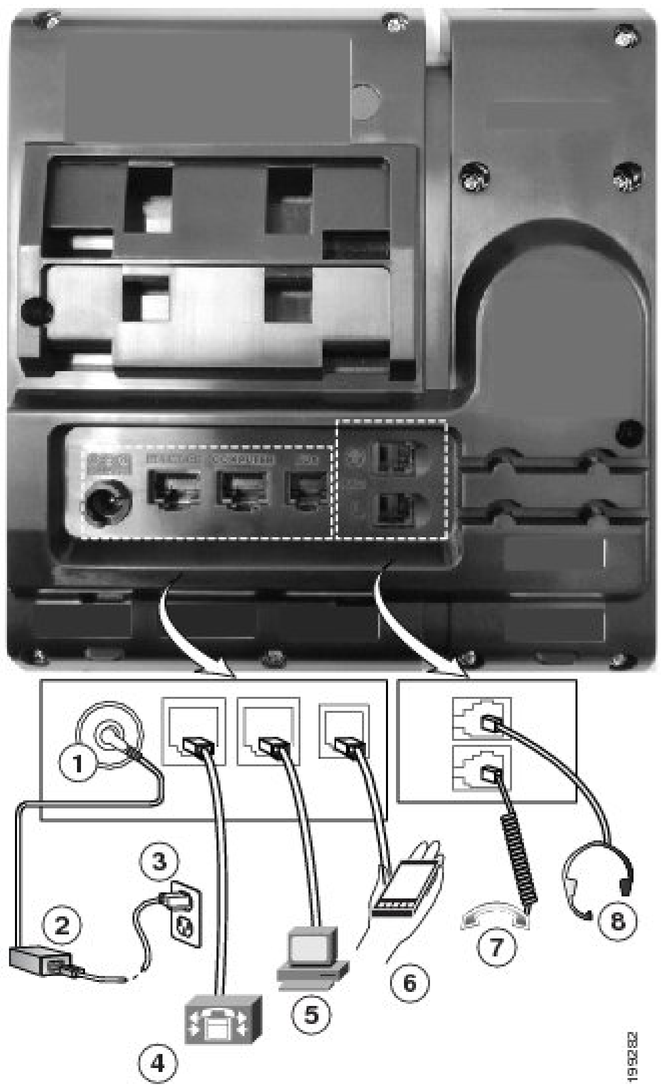
Cisco Unified IP Phone 6945

The Cisco Unified IP Phone 6945 provides the following features.

Phone Connections

For your phone to work, it must be connected to the corporate IP telephony network.

Figure 2: Cisco IP Phone 6945 connections



1	DC adaptor port (DC48V).	5	Access port (10/100/1000 PC) connection.
2	AC-to-DC power supply (optional).	6	Auxiliary port.
3	AC power wall plug (optional).	7	Handset connection.
4	Network port (10/100/1000 SW) connection. IEEE 802.3af power enabled.	8	Analog headset connection (optional).

Buttons and hardware

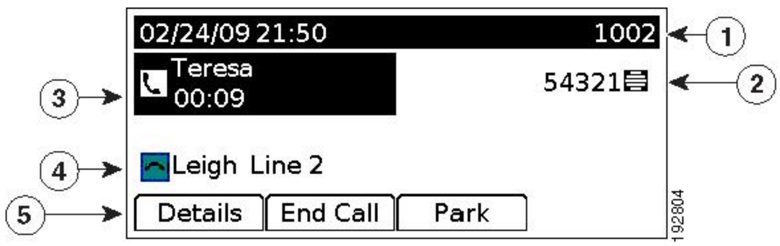
1	Handset light strip	Indicates an incoming call (flashing red) or new voice message (steady red).
2	Phone screen	Shows information about your phone such as directory number, active call and line status, softkey options, speed dials, placed calls, and phone menu listings.

3	Programmable feature buttons  	Depending on how your system administrator sets up the phone, programmable feature buttons (on each side of the phone screen) provide access to: • Phone lines and intercom lines • Speed-dial numbers (speed-dial buttons, including the Line Status speed-dial features) • Web-based services (for example, a Personal Address Book button) • Call features (for example, a Privacy button) Buttons illuminate to indicate status: • Green, steady: Active call or two-way intercom call • Green, flashing: Held call • Amber, steady: Privacy in use, one-way intercom call, DND active, or logged into Hunt Group • Amber, flashing: Incoming call or reverting call • Red, steady: Remote line in use (shared line or Line Status) • Red, flashing: Remote line on hold
4	Softkey buttons 	Depending on how your system administrator sets up the phone, enable softkey options displayed on your phone screen.
5	Transfer button 	Transfers a call.
6	Conference button 	Creates a conference call.
7	Hold button 	Places an active call on hold.

8	Navigation bar and Select button 	The Navigation bar allows you to scroll through menus and highlight items. When phone is on hook, displays phone numbers from your Placed Call listing (up arrow) or your speed dials (down arrow). The Select button (in the middle of the Navigation bar) allows you to select a highlighted item.
9	Headset button 	Toggles the headset on or off. When the headset is on, the button is lit.
10	Speakerphone  button	Toggles the speakerphone on or off. When the speakerphone is on, the button is lit.
11	Keypad	Allows you to dial phone numbers, enter letters, and select menu items (by entering the item number).
12	Mute button 	Toggles the microphone on or off. When the microphone is muted, the button is lit.
13	Volume button 	Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook). Your administrator sets a minimum ringer volume level ranging from 0 to 14. The default level is 0 (silent). You can only adjust the ringer volume to a level greater than the configured minimum ring volume value.
14	Messages button 	Autodials your voice messaging system (varies by system).
15	Applications button 	Opens or closes the Applications menu. Use the Applications button to access call history, user preferences, phone settings, and phone model information.

16	Contacts button 	Opens or closes the Directories menu. Use the Contacts button to access personal and corporate directories.
17	Handset	Phone handset.

Phone Screen



1	Header	Displays date, time, and directory number.
2	Line text label with icon	Displays text label and icon for phone or intercom line, speed-dial numbers, or services, depending on your configuration.
3	Primary line details and other phone information	Displays line label and call details for the primary line, and other phone information such as placed calls, speed dials, and phone menu listings. The IP phone LCD display size limits the length of calling ID and calling number that are displayed. If the calling number is restricted, the phone displays only the calling ID. If the calling number is unrestricted and the calling ID is restricted, the phone displays the calling ID as `Unknown`. If the calling number and the calling ID are unrestricted, but the calling ID is not configured, the phone displays only the calling number.

4	Secondary line details and other phone information	Displays line label and call details for the secondary line, and other phone information such as placed calls, speed dials, and phone menu listings. The IP phone LCD display size limits the length of calling ID and calling number that are displayed. If the calling numbIf the calling number and the calling ID are unrestricted, but the calling ID is not configured, the phone displays only the calling number.er is restricted, the phone displays only the calling ID. If the calling number is unrestricted and the calling ID is restricted, the phone displays the calling ID as `Unknown`. If the calling number and the calling ID are unrestricted, but the calling ID is not configured, the phone displays only the calling number.
5	Softkey labels	Display softkeys for available features or actions.

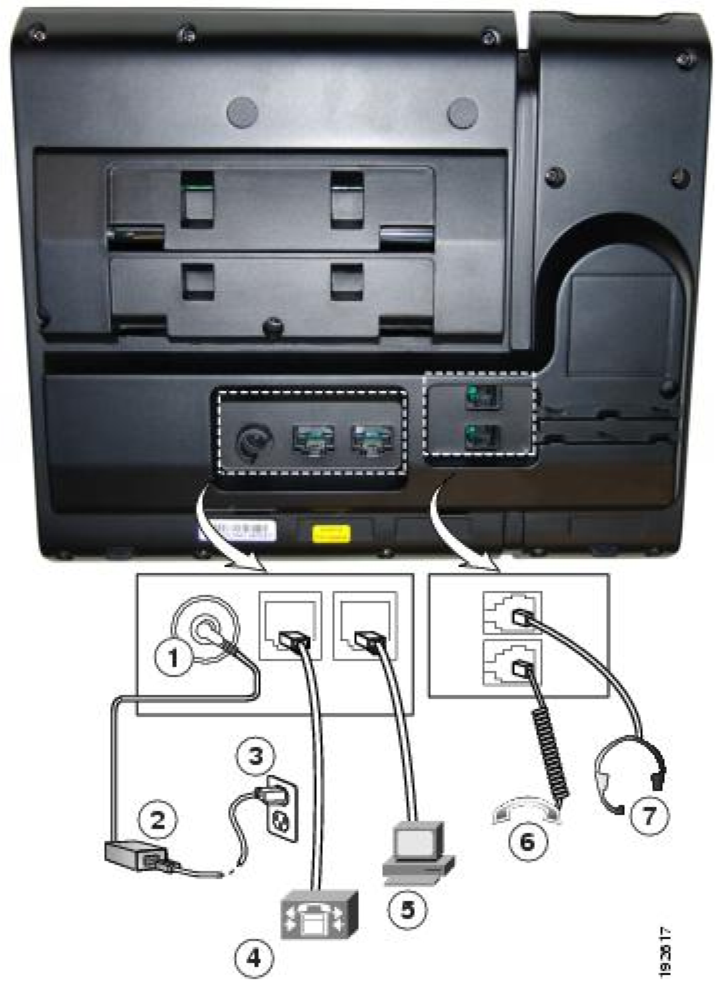
Cisco Unified IP Phone 6961

The Cisco Unified IP Phone 6961 provides the following features.

Phone Connections

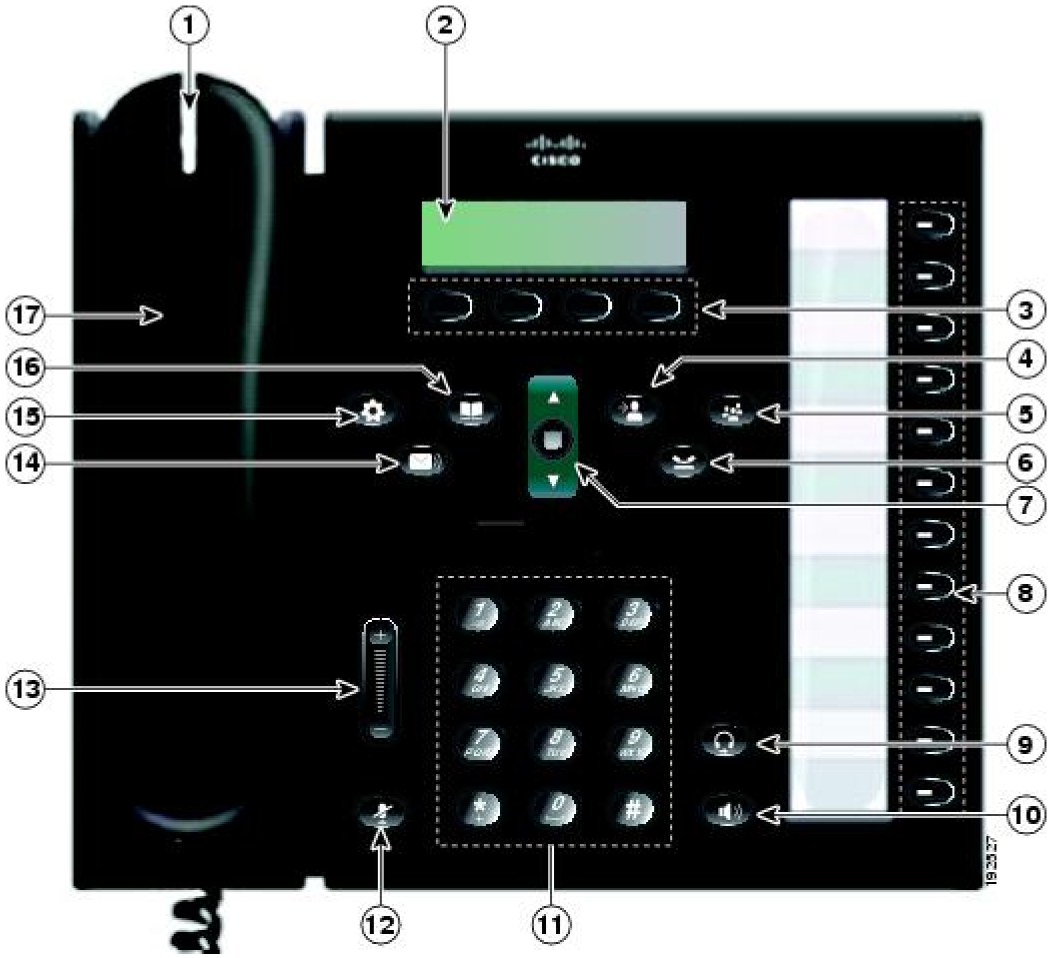
For your phone to work, it must be connected to the corporate IP telephony network.

Figure 3: Cisco IP Phone 6961 connections



1	DC adaptor port (DC48V).	5	Access port (10/100 PC) connection.
2	AC-to-DC power supply (optional).	6	Handset connection.
3	AC power wall plug (optional).	7	Headset connection (optional).
4	Network port (10/100 SW) connection. IEEE 802.3af power enabled.		

Buttons and hardware

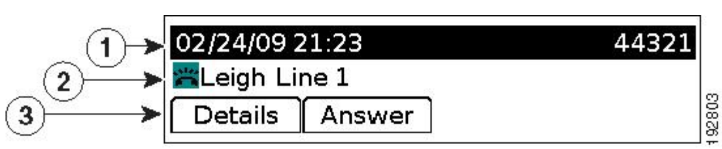


1	Handset light strip	Indicates an incoming call (flashing red) or new voice message (steady red).
2	Phone screen	Shows information about your phone such as directory number, active call and line status, softkey options, speed dials, placed calls, and phone menu listings.
3	Softkey buttons 	Depending on how your system administrator sets up the phone, enable softkey options displayed on your phone screen.
4	Transfer button 	Transfers a call.

5	Conference button 	Creates a conference call.
6	Hold button 	Places an active call on hold.
7	Navigation bar and Select button 	The Navigation bar allows you to scroll through menus and highlight items. When phone is on hook, displays phone numbers from your Placed Call listing (up arrow) or your speed dials (down arrow). The Select button allows you to select a highlighted item.
8	Programmable feature buttons 	Depending on how your system administrator sets up the phone, programmable feature buttons provide access to: • Phone lines and intercom lines • Speed-dial numbers (speed-dial buttons, including the Line Status speed-dial features) • Web-based services (for example, a Personal Address Book button) • Call features (for example, a Privacy button) Buttons illuminate to indicate status: • Green, steady: Active call or two-way intercom call • Green, flashing: Held call • Amber, steady: Privacy in use, one-way intercom call, DND active, or logged into Hunt Group • Amber, flashing: Incoming call or reverting call • Red, steady: Remote line in use (shared line or Line Status) • Red, flashing: Remote line on hold
9	Headset button 	Toggles the headset on or off. When the headset is on, the button is lit.

10	Speakerphone button 	Toggles the speakerphone on or off. When the speakerphone is on, the button is lit.
11	Keypad	Allows you to dial phone numbers, enter letters, and select menu items (by entering the item number).
12	Mute button 	Toggles the microphone on or off. When the microphone is muted, the button is lit.
13	Volume button 	Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook). Your administrator sets a minimum ringer volume level ranging from 0 to 14. The default level is 0 (silent). You can only adjust the ringer volume to a level greater than the configured minimum ring volume value.
14	Messages button 	Autodials your voice messaging system (varies by system).
15	Applications button 	Opens or closes the Applications menu. Use the Applications button to access call history, user preferences, phone settings, and phone model information.
16	Contacts button 	Opens or closes the Directories menu. Use the Contacts button to access personal and corporate directories.
17	Handset	Phone handset.

Phone Screen



1	Header	Displays date, time, and directory number.
2	Line details and other phone information	During a call, displays details for the active line. If not on a call, displays line text label and other information such as placed calls, speed dials, and phone menu listings. The IP phone LCD display size limits the length of calling ID and calling number that are displayed. If the calling number is restricted, the phone displays only the calling ID. If the calling number is unrestricted and the calling ID is restricted, the phone displays the calling ID as `Unknown`. If the calling number and the calling ID are unrestricted, but the calling ID is not configured, the phone displays only the calling number.
3	Softkey labels	Display softkeys for available features or actions.

General Phone Information

Footstand

If the phone is placed on a table or desk, the footstand can be connected to the back of your phone for a higher or lower viewing angle, depending on your preference.

1	Footstand slots for a higher viewing angle	2	Footstand slots for a lower viewing angle

Higher viewing angle

Lower viewing angle

Supported network protocols

Cisco Unified IP Phones support several industry-standard and Cisco network protocols required for voice communication. The following table provides an overview of the network protocols that the Cisco Unified IP Phone 6921, 6941, 6945, and 6961 support.

Table 1: Supported network protocols on the Cisco Unified IP Phone

Network protocol	Purpose	Usage notes
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 Tunneling (CAST)	The CAST protocol allows IP phones and associated applications behind the phone to discover and communicate with the remote endpoints without requiring changes to the traditional signaling components like Cisco Unified Communications Manager and gateways. The CAST protocol allows separate hardware devices to synchronize related media and it allows PC applications to augment nonvideo-capable phones to become video enabled using the PC as the video resource.	—
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.

Network protocol	Purpose	Usage notes
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.
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. **Note** IP phones can be HTTPS clients; they cannot be HTTPS servers.	Web applications with both HTTP and HTTPS support have two URLs configured. Cisco Unified IP Phones that support HTTPS choose the HTTPS URL. A lock icon is displayed to the user if the connection to the service is via HTTPS.
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 802.1X Authentication, on page 39 for additional information.

Network protocol	Purpose	Usage notes
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. The Cisco Unified IP Phones support IPv6 address. For more information, see "Internet Protocol Version 6 (IPv6)" in the *Cisco Unified Communications Manager Features and Services Guide*.
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.
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.

Network protocol	Purpose	Usage notes
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 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. You can configure the Cisco Unified IP Phone to use either SIP or Skinny Client Control Protocol (SCCP). Cisco Unified IP Phones do not support the SIP protocol when the phones are operating in IPv6 address mode.
Skinny Client Control Protocol (SCCP)	SCCP includes a messaging set that allows communications between call control servers and endpoint clients such as IP Phones. SCCP is proprietary to Cisco Systems.	Cisco Unified IP Phone 6921, 6941, 6945, and 6961 use SCCP, version 20 for call control.
Secure Real-Time Transfer protocol (SRTP)	SRTP is an extension of the Real-Time Protocol (RTP) Audio/Video Profile and ensures the integrity of RTP and Real-Time Control Protocol (RTCP) packets providing authentication, integrity, and encryption of media packets between two endpoints.	Cisco Unified IP Phones use SRTP for media encryption.
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.

Network protocol	Purpose	Usage notes
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	When security is implemented, Cisco Unified IP Phones use the TLS protocol when securely registering with Cisco Unified Communications Manager. For more information, see *Cisco Unified Communications Manager Security Guide*.
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 Setup menu on the phone. For more information, see "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

Interactions with Other Cisco Unified IP Telephony Products, on page 47
Phone Startup Process, on page 54
Network Setup Menu, on page 73

Cisco Unified IP Phone 6921, 6941, 6945, and 6961 Supported Features

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.

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.

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

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 coworker 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.

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.

Related Topics

Cisco Unified IP Phone Settings, on page 71
Features, Templates, Services, and User Setup, on page 89
Troubleshooting and Maintenance, on page 169
Feature support by protocol, on page 229

Telephony Feature Administration

You can modify additional settings for the Cisco Unified IP Phone from Cisco Unified Communications Manager Administration. Use Cisco Unified Communications Manager Administration 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.

For more information about Cisco Unified Communications Manager Administration, see 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 Topics

Available telephony features, on page 90
Feature support by protocol, on page 229

Cisco Unified IP Phone Network Parameters

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.

Related Topics

Cisco Unified IP Phone Settings, on page 71
Cisco Unified IP Phone Model Information, Status, and Statistics, on page 139

Feature Information for End Users

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 on the Cisco Unified IP Phone web site:

http://www.cisco.com/en/US/products/ps10326/tsd_products_support_series_home.html

From this site, you can view various user documentation.

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.

Related Topics

Internal support Web Site, on page 193

Cisco Unified IP Phone Security Features

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 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 6921, 6941, 6945, and 6961 use the Phone security profile, which defines whether the device is nonsecure or encrypted. For information on applying the security profile to the phone, see *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, see "Configuring Encrypted Phone Configuration Files" chapter in *Cisco Unified Communications Manager Security Guide*.

The following table shows where you can find additional information about security in this and other documents.

Table 2: 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	See *Troubleshooting Guide for Cisco Unified Communications Manager*
Security features supported on the Cisco Unified IP Phone	See Supported Security Features, on page 34
Restrictions regarding security features	See Security Restrictions, on page 41
Viewing a security profile name	See Security Profiles, on page 36
Identifying phone calls for which security is implemented	See Encrypted Phone Call Identification, on page 37
TLS connection	See Supported network protocols, on page 26 See Cisco Unified Communications Manager Phone Addition Methods, on page 55
Security and the phone startup process	See Phone Startup Process, on page 54
Security and phone configuration files	See Cisco Unified Communications Manager Phone Addition Methods, on page 55
Changing the TFTP Server 1 or TFTP Server 2 option on the phone when security is implemented	See IPv4 Setup Menu Options, on page 78, in Network Setup Menu, on page 73
Items on the Security Configuration menu that you access from the Device Configuration menu on the phone	See Security Setup menu, on page 84
Items on the Security Configuration menu that you access from the Settings menu on the phone	See Security Setup menu, on page 84
Applying a password to the phone so that no changes can be made to the administrative options	See Password Protection, on page 73.
Disabling access to a phone's web pages	See Control web page access, on page 155.
Troubleshooting	See Cisco Unified IP Phone Security Problems, on page 175 See *Troubleshooting Guide for Cisco Unified Communications Manager*

Topic	Reference
Deleting the CTL file from the phone	See Cisco Unified IP Phone Reset or Restore, on page 187
Resetting or restoring the phone	See Cisco Unified IP Phone Reset or Restore, on page 187
802.1X Authentication for Cisco Unified IP Phones	See these sections: • 802.1X Authentication, on page 39 • Security Setup menu, on page 84 • Status Menu, on page 141 • Cisco Unified IP Phone Security Problems, on page 175

All Cisco Unified IP Phones that support Cisco Unified Communications Manager use a security profile, which defines whether the phone is nonsecure or secure.

For information about configuring the security profile and applying the profile to the phone, see *Cisco Unified Communications Manager Security Guide*.

Supported Security Features

The following table provides an overview of the security features that the Cisco Unified IP Phone 6921, 6941, 6945, and 6961 support. For more information about these features and about Cisco Unified Communications Manager and Cisco Unified IP Phone security, see *Cisco Unified Communications Manager Security Guide*.

For information about current security settings on a phone, choose **Applications** > **Admin Settings** > **Security Setup**.

Note Most security features are available only if a certificate trust list (CTL) is installed on the phone. For more information about the CTL, see “Configuring the Cisco CTL Client” chapter in *Cisco Unified Communications Manager Security Guide*.

Table 3: Overview of Security Features

Feature	Description
Image authentication	Signed binary files (with the extension .sgn) 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.

Feature	Description
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.
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.
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.
Secure SRST reference	After you configure a SRST reference for security and then reset the dependent devices in Cisco Unified Communications Manager 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.
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.
Signaling encryption	Ensures that all SCCP signaling messages that are sent between the device and the Cisco Unified Communications Manager server are encrypted.
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.

Feature	Description
Security profiles	Defines whether the phone is nonsecure or encrypted.
Encrypted configuration files	Lets you ensure the privacy of phone configuration files.
Optional disabling of the web server functionality for a phone	You can prevent access to a phone web page, which displays a variety of operational statistics for the phone.
Phone hardening	Additional security options, which you control from Cisco Unified Communications Manager Administration: • Disabling PC port • Disabling PC Voice VLAN access • Disabling access to web pages for a phone **Note** You can view current settings for the PC Port Disabled, GARP Enabled, and Voice VLAN enabled options by looking at the phone Security Configuration menu.
802.1X Authentication	The Cisco Unified IP Phone can use 802.1X authentication to request and gain access to the network.

Related Topics

Security Profiles, on page 36
Encrypted Phone Call Identification, on page 37
802.1X Authentication, on page 39
Security Restrictions, on page 41
Cisco Unified IP Phone Security, on page 69
Security Setup menu, on page 84
Control web page access, on page 155

Security Profiles

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

Related Topics

Encrypted Phone Call Identification, on page 37
Security Restrictions, on page 41
Security Setup menu, on page 84

Encrypted Phone Call Identification

When security is implemented for a phone, you can identify encrypted phone calls by icons on the screen on the phone. 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. An encrypted 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 LCD screen changes to the lock icon: .

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 encrypted audio and video (if video is involved). If your call is connected to a non-protected phone, the security tone does not play.

Note Secured calling is supported for connections between two phones only. Some features, such as conference calling, shared lines, Cisco Extension Mobility, and Join Across Lines are not available when secured calling is configured.

Related Topics

Security Profiles, on page 36
Cisco Unified IP Phone Security Features, on page 32
Security Restrictions, on page 41

Identify Secure Conference Call

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 the 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 phones and the availability of secure conference bridges. For more information about the interactions, see Call Security Interactions and Restrictions, on page 38.

Identify Secure Phone Call

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

A protected call is established using this process:

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

Note Protected calling is supported for conversations between two phones. Some features, such as conference calling, shared lines, Cisco Extension Mobility, and Join Across Lines are not available when protected 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 security in the system. The following table provides information about changes to call security levels when using Barge.

Table 4: Call Security Interactions When Using Barge

Initiator's phone security level	Feature used	Call security level	Results of action
Nonsecure	cBarge	Encrypted call	Call barged and identified as nonsecure call
Secure	cBarge	Secure call	Call barged and identified as Secure call

The following table 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 5: Security Restrictions with Conference Calls

Initiator's phone security level	Feature used	Security level of participants	Results of action
Nonsecure	Conference	Encrypted	Nonsecure conference bridge Nonsecure conference
Secure	Conference	At least one member is nonsecure.	Secure conference bridge Nonsecure conference
Secure	Conference	All participants are encrypted.	Secure conference bridge Secure encrypted level conference
Secure	Join	Encrypted	Secure conference bridge Conference remains secure
Nonsecure	cBarge	All participants are encrypted.	Secure conference bridge Conference changes to nonsecure
Nonsecure	Meet Me	Minimum security level is encrypted.	Only nonsecure conference bridge is available and used Nonsecure conference
Secure	Meet Me	Minimum security level is nonsecure	Only secure conference bridge available and used Conference accepts all calls

802.1X Authentication

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

Related Topics

Security Restrictions, on page 41

Overview

Cisco Unified IP Phones and Cisco Catalyst switches traditionally use Cisco Discovery Protocol (CDP) to identify each other and determine parameters such as VLAN allocation and inline power requirements. CDP does not identify locally attached workstations. Cisco Unified IP Phones provide an EAPOL pass-through mechanism. This mechanism allows a workstation attached to the Cisco Unified IP Phone to pass EAPOL messages to the 802.1X authenticator at the LAN switch. The pass-through mechanism ensures that the IP phone does not act as the LAN switch to authenticate a data endpoint before accessing the network.

Cisco Unified IP Phones also provide a proxy EAPOL Logoff mechanism. In the event that the locally attached PC disconnects from the IP phone, the LAN switch does 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.

Cisco Unified IP Phones also contain an 802.1X supplicant. 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 authenticates 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. After the exchange completes, the switch 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. For more information, see the 802.1X Authentication and Status, on page 85.
- 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 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, see 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. For more information, see the Security Setup menu, on page 84. 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. For more information, see the Security Setup menu, on page 84.

- 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. For more information, see the 802.1X Authentication and Status, on page 85.

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 (fast busy) tone plays on the phone that the barge was initiated.

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.

Cisco Unified IP Phone Deployment

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, see “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.

Cisco Unified IP Phones Setup in Cisco Unified Communications Manager

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

- Autoregistration
- Cisco Unified Communications Manager Administration
- Bulk Administration Tool (BAT)
- BAT and the Tool for AutoRegistered Phones Support (TAPS)

For more information about these choices, see Cisco Unified Communications Manager Phone Addition Methods, on page 55.

For general information about configuring phones in Cisco Unified Communications Manager, see 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*

Set Up Cisco Unified IP Phone 6921, 6941, 6945, and 6961 in Cisco Unified Communications Manager

The following steps provide an overview and checklist of configuration tasks for the Cisco Unified IP Phone 6921, 6941, 6945, and 6961 in Cisco Unified Communications Manager Administration. The steps below guides you through the phone configuration process. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, see the sources in the steps.

Procedure

Step 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, softkey template, phone features, IP Phone services, or phone applications

This step provides list of configuration requirements for setting up phones and identifies preliminary configuration that you need to perform before configuring individual phones, such as phone button templates or softkey templates.

For more information, see “Cisco Unified IP Phones” chapter in the *Cisco Unified Communications Manager System Guide* and see the Available telephony features, on page 90.

Step 2 Verify that you have sufficient unit licenses for your phone. For more information, see “License Unit Report” chapter in the *Cisco Communications Manager Administration Guide*.

Step 3 Customize phone button templates (if required). Changes the number of line buttons, speed-dial buttons, Service URL buttons or adds a Privacy button to meet user needs.
For more information, see “Phone Button Template Configuration” chapter in the *Cisco Communications Manager Administration Guide* and see the Phone Button Template Modification, on page 114.

Step 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. The device with its default settings gets added to the Cisco Unified Communications Manager database.
For more information, see “Cisco Unified IP Phone Configuration” chapter in the *Cisco Communications Manager Administration Guide*.

For information about Product Specific Configuration fields, see “?” 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, see "User/Phone Add Configuration" chapter in the *Cisco Communications Manager Administration Guide*.

Step 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, see "Directory Number Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide* and see the Available telephony features, on page 90.

Step 6 Customize softkey templates. Adds, deletes, or changes order of softkey features that display on the user's phone to meet feature usage needs.
For more information, see *Cisco Unified Communications Manager Administration Guide*, "Softkey Template Configuration" and "Cisco Unified IP Phone Configuration" chapters.

Step 7 Configure speed-dial buttons and assign speed-dial numbers. Adds speed-dial buttons and numbers.

Note Users can change speed-dial settings on their phones using Cisco Unified Communications Manager User Options.

For more information, see *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter.

Step 8 Configure Cisco Unified IP Phone services and assign services. Provides IP Phone services.

Note Users can add or change services on their phones using the Cisco Unified Communications Manager User Options.

For more information, see *Cisco Communications Manager Administration Guide*, "IP Phone Services Configuration" chapter.

Step 9 Assign services to programmable buttons (optional). Provides access to an IP phone service or URL.
For more information, see *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter.

Step 10 Add user information by configuring required fields. Required fields are indicated by an asterisk (*); for example, User ID and last name. Adds user information to the global directory for Cisco Unified Communications Manager.

Note Assign a password (for User Options web pages) and PIN (for Cisco Extension Mobility and Personal Directory).

For more information, see *Cisco Unified Communications Manager Administration Guide*, "End User Configuration" chapter.

Note If your company uses 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 Corporate Directory setup, on page 113. After the Enable Synchronization from the LDAP Server field is enabled, you will not be able to add additional users from Cisco Unified Communications Manager Administration.

Note If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, see "User/Phone Add Configurations" in *Cisco Unified Communications Manager Administration Guide*.

Step 11 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.
In order for end users to access Cisco Unified Communications Manager User Options, you must add users to the standard Cisco Communications Manager End Users group.

For more information, see "End User Configuration" and "User Group Configuration" in the *Cisco Unified Communications Manager Administration Guide*.

Step 12 Associate a user with a phone. 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, see *Cisco Unified Communications Manager Administration Guide*, "End User Configuration" chapter.

Cisco Unified IP Phones Installation

After you have added the phones to the Cisco Unified Communications Manager database, you can complete the phone installation. You (or the phone user) can install the phone at the location of the user.

Note Upgrade the phone with the current firmware image before you install the phone. For information about upgrading, see the Readme file for your phone, located at:

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

For instructions on upgrading the firmware, see the Release Notes, located at:

http://www.cisco.com/en/US/products/ps10326/prod_release_notes_list.html

After the phone connects 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 autoregistration, 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.

Install Cisco Unified IP Phone 6921, 6941, 6945, and 6961

The following steps provide an overview and checklist of installation tasks for the Cisco Unified IP Phone 6921, 6941, 6945, and 6961. The steps present 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, see sources in the step.

Procedure

Step 1 Choose the power source for the phone:

- Power over Ethernet (PoE)
- External power supply

Determines how the phone receives power. See the Cisco Unified IP Phone Power, on page 50.

Step 2 Assemble the phone, adjust phone placement, and connect the network cable. Locates and installs the phone in the network.
See the Install Cisco Unified IP Phone, on page 66 and Footstand, on page 23.

Step 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 Phone Startup Verification, on page 68.

Step 4 If you are configuring the network settings on the phone, you can set up an IP address for the phone by either using DHCP or manually entering an IP address.
See the Network Settings, on page 69, Network Setup Menu, on page 73 and DHCP Usage, on page 82.

Step 5 Set up security on the phone. Provides protection against data tampering threats and identity theft of phones.
See the Cisco Unified IP Phone Security, on page 69.

Step 6 Make calls with the Cisco Unified IP Phone. Verifies that the phone and features work correctly.
For more information, see *Cisco Unified IP Phone 6921, 6941, 6945, and 6961 User Guide for Cisco Unified Communications Manager (SCCP and SIP)*.

Step 7 Provide information to 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 Internal support Web Site, on page 193

Terminology Differences

The following table highlights some of the important differences in terminology that is used in these documents:

- *Cisco Unified IP Phone 6921, 6941, 6945, and 6961 User Guide for Cisco Unified Communications Manager (SCCP and SIP)*
- *Cisco Unified IP Phone 6921, 6941, 6945, and 6961 Administration Guide for Cisco Unified Communications Manager (SCCP and SIP)*
- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager System Guide*

User Guide	Administration and System Guides
Speed Dialing (Placing a call with a speed-dial code)	Abbreviated Dialing
Conference across Lines	Join Across Lines
Conference	Join or Conference
Line Status	Busy Lamp Field (BLF)
Message Indicators	Message Waiting Indicator (MWI) or Message Waiting Lamp

User Guide	Administration and System Guides
Programmable Feature Button	Programmable Line Button or Programmable Line Key (PLK)
Voicemail System	Voice Messaging System

CHAPTER 2

Cisco Unified IP Phones and telephony networks

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 6921, 6941, 6945, and 6961 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, see the documents at this URL:

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

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

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.

Cisco Unified IP Phone and Cisco Unified Communications Manager Interaction

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: 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 using the TFTP service
- Authentication and encryption (if configured for the telephony system)
- 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 phones described in this chapter, see "Cisco Unified IP Phone Configuration" chapter in the *Cisco Communications Manager Administration Guide*.

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

For more information, see "Software Upgrades" chapter in the *Cisco Unified Communications Operating System Administration Guide*.

Related Topics

Cisco Unified IP Phone Security Features, on page 32
Available telephony features, on page 90

Cisco Unified IP Phone and VLAN Interaction

The Cisco Unified IP Phone 6921, 6941, 6945, and 6961 have an internal Ethernet switch, enabling forwarding of packets to the phone, and to the access port and the network port on the back of the phone.

If a computer is connected to the 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 (for example, auxiliary VLAN on the Cisco Catalyst 6000 series)
- Data traffic to and from the PC connected to the switch through the 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 when there are not enough IP addresses for each phone.

For more information, see 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

Phone Startup Process, on page 54
Network Setup Menu, on page 73

Cisco Unified IP Phone and Cisco Unified Communications Manager Express Interaction

When the Cisco Unified IP Phone works with the Cisco Unified Communications Manager Express (Unified CME), the phones must go into CME mode.

When a user invokes the conference feature, the tag allows the phone to use either a local or network hardware conference bridge.

The Cisco Unified IP Phones do not support the following actions:

Transfer

Only supported in the connected call transfer scenario.

Conference

Only supported in the connected call transfer scenario.

Join

Supported using the Conference button or Hookflash access.

Hold

Supported using the Hold button.

Barge

Not supported.

Direct Transfer

Not supported.

Select

Not supported.

The users cannot create conference and transfer calls across different lines.

Cisco Unified IP Phone Power

The Cisco Unified IP Phone 6921, 6941, 6945, and 6961 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.

Power Guidelines

The following table provides guidelines for powering the Cisco Unified IP Phone 6921, 6941, 6945, and 6961.

Table 6: Guidelines for Powering the Cisco Unified IP Phone 6921, 6941, 6945, and 6961

Power Type	Guidelines
External power: Provided through the CP-PWR-CUBE-3 external power supply.	The Cisco Unified IP Phone 6921, 6941, 6945, and 6961 use the CP-PWR-CUBE-3 power supply.
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.	• The Cisco Unified IP Phone 6921, 6941, 6945, and 6961 support IEEE 802.3af Class 2 power on signal pairs and spare pairs. • 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.

Power Type	Guidelines
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 6921, 6941, 6945, and 6961.

Power Outage

Your access to emergency service through the phone requires the phone to receive power. If an interruption in the power supply occurs, Service and Emergency Calling Service dialing do not function until power is restored. In the case of a power failure or disruption, you may need to reset or reconfigure equipment before you can use the Service or Emergency Calling Service dialing.

Phone Power Reduction

You can reduce the amount of energy that the Cisco Unified IP Phone consumes by using Power Save or EnergyWise (Power Save Plus) mode.

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 window on Cisco Unified Communications Administration, configure the following parameters:

Days Display Not Active

Specifies the days that the backlight remains inactive.

Display on Time

Schedules 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 after 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.

EnergyWise Mode

In addition to Power Save mode, the Cisco Unified IP Phone supports Cisco EnergyWise (Power Save Plus) mode. When your network contains an EnergyWise (EW) controller (for example, a Cisco switch with the EnergyWise feature enabled), you can configure these phones to sleep (power down) and wake (power up) on a schedule to further reduce power consumption.

Set up each phone to enable or disable the EnergyWise settings. If EnergyWise is enabled, configure a sleep and wake time, as well as other parameters. These parameters are sent to the phone as part of the phone configuration XML file. In the Phone Configuration window in Cisco Unified Communications Administration, configure the following parameters:

Enable Power Save Plus

Selects the schedule of days for which the phone powers off.

Phone On Time

Determines when the phone automatically turns on for the days that are selected in the Enable Power Save Plus field.

Phone Off Time

Determines the time of day that the phone powers down for the days that are selected in the Enable Power Save Plus field.

Phone Off Idle Timeout

Determines the length of time that the phone must be idle before the phone powers down.

Enable Audio Alert

When enabled, instructs the phone to play an audible alert starting 10 minutes before the time that the Phone Off Time field specifies.

EnergyWise Domain

Specifies the EnergyWise domain that the phone is in.

EnergyWise Secret

Specifies the security secret password that is used to communicate within the EnergyWise domain.

Allow EnergyWise Overrides

Determines whether you allow the EnergyWise domain controller policy to send power-level updates to the phones.

When a phone is sleeping, the power sourcing equipment (PSE) provides minimal power to the phone to illuminate the Select key, and the Select key can be used to wake up the phone when it is sleeping.

Additional Information About Power

The documents in the following table provide more information on the following topics:

- Cisco switches that work with Cisco Unified IP Phones
- Cisco IOS releases that support bidirectional power negotiation
- Other requirements and restrictions about 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/index.html
Cisco Catalyst Switches	http://www.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

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 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 autoregistration 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

In addition, if the device security mode in the configuration file is set to Authenticated and the CTL file on the phone has a valid certificate for Cisco Unified Communications Manager, the phone establishes a TLS connection to Cisco Unified Communications Manager. Otherwise, the phone establishes a TCP connection.

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

Note Cisco Extension Mobility Cross Cluster is an exception, in that the phone permits a TLS connection to Cisco Unified Communications Manager for secure signaling even without the CTL file.

If you configure security 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 more information, see “Configuring Encrypted Phone Configuration Files” chapter in *Cisco Unified Communications Manager Security Guide*. A phone requests a configuration file whenever it resets and registers with Cisco Unified Communications Manager.

A phone accesses a default configuration file named XmlDefault.cnf.xml only when the phone has not received a valid Trust List file containing a certificate assigned to the Cisco Unified Communications Manager and TFTP.

If auto registration is not enabled and you did not add the phone to the Cisco Unified Communications Manager database, the phone does not attempt to register with Cisco Unified Communications Manager. The phone continually displays the "Configuring IP" message until you either enable auto-registration or add the phone to the Cisco Unified Communications Manager database.

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.

For SIP phones, the TFTP server generates these SIP configuration files:

- SIP IP Phone:
    - For unsigned and unencrypted files—SEP<*mac*>.cnf.xml
    - For signed files—SEP<*mac*>.cnf.xml.sgn
    - For signed and encrypted files—SEP<*mac*>.cnf.xml.enc.sgn
        - Dial Plan—<*dialplan*>.xml
        - Softkey Template—<*softkey_template*>.xml

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.

For more information about phone configuration settings, see "Cisco Unified IP Phone Configuration" chapter in the *Cisco Communications Manager Administration Guide*.

For more information, also see *Cisco Unified Communications Manager Security Guide*.

Phone Startup Process

When connecting to the VoIP network, the Cisco Unified IP Phone 6921, 6941, 6945, and 6961 goes through a standard startup process that is described in the following procedure. Depending on your specific network setup, not all of these steps may occur on your Cisco Unified IP Phone.

Procedure

Step 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.
For more information, see Cisco Unified Communications Manager Phone Addition Methods, on page 55 and Startup Problems, on page 169.

Step 2 Load the Stored Phone Image. The Cisco Unified IP Phone has nonvolatile 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.
For more information, see Startup Problems, on page 169.

Step 3 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.
For more information, see Network Setup Menu, on page 73 and Startup Problems, on page 169.

Step 4 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.

Step 5 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.

For more information, see Network Setup Menu, on page 73 and Startup Problems, on page 169.

Step 6 Request the CTL file. The TFTP server stores the certificate trust list (CTL) file. The CTL file contains the certificates necessary for establishing a secure connection between the phone and Cisco Unified Communications Manager.
For more information, see the *Cisco Unified Communications Manager Security Guide*, “Configuring the Cisco CTL Client” chapter.

Step 7 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.
For more information, see Cisco Unified Communications Manager Phone Addition Methods, on page 55 and Startup Problems, on page 169.

Step 8 Contact Cisco Unified Communications Manager. The configuration file defines how the Cisco Unified IP Phone communicates with Cisco Unified Communications Manager 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 Communications Manager on the list.
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.

For more information, see Startup Problems, on page 169.

Cisco Unified Communications Manager Phone Addition Methods

Before installing the Cisco Unified IP Phone, you must choose a method for adding phones to the Cisco Unified Communications Manager database. Be aware that each phone type requires a fixed number of device license units and the number of unit licenses that are available on the server may impact phone registration. For more information about licensing, see “Licenses for Phones” section in the *Cisco Unified Communications Manager System Guide*.

The following table provides an overview of these methods for adding phones to the Cisco Unified Communications Manager database.

Table 7: Methods for adding phones to the Cisco Unified Communications Manager database

Method	Requires MAC address?	Notes
Autoregistration	No	Results in automatic assignment of directory numbers Not available when security or encryption is enabled **Note** Autoregistration is disabled when security is enabled on Cisco Unified Communications Manager. In this case, the phone must be manually added to the Cisco Unified Communications Manager database.
Autoregistration with TAPS	No	Requires autoregistration 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

Autoregistration Phone Addition

If you enable autoregistration 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 CM database when you physically connect the phone to your IP telephony network. During autoregistration, 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 autoregistered phones to new locations and assign them to different device pools without affecting their directory numbers.

Note Cisco recommends that you use autoregistration to add fewer than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT).

Autoregistration is disabled by default. In some cases, you might not want to use autoregistration; for example, if you want to assign a specific directory number to the phone. For information about enabling autoregistration, see “Enable autoregistration” section in the *Cisco Unified Communications Manager Administration Guide*.

Note When you configure the cluster for mixed mode through the Cisco CTL client, autoregistration is automatically disabled. When you configure the cluster for nonsecure mode through the Cisco CTL client, autoregistration is automatically enabled.

Autoregistration and TAPS Phone Addition

You can add phones with autoregistration 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 predefined configurations for phones.

Note Cisco recommends that you use autoregistration 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).

To implement TAPS, dial a TAPS directory number and follow the voice prompts. When the process completes, the phone has downloaded the directory number and other settings, and the phone is updated in Cisco Unified Communications Manager Administration with the correct MAC address.

Autoregistration 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, autoregistration is automatically disabled. When you configure the cluster for nonsecure mode through the Cisco CTL client, autoregistration is automatically enabled.

For more information, see “Bulk Administration” chapter in the *Cisco Unified Communications Manager Administration Guide* and the “Tool for Auto-Registered Phones Support” chapter in the *Cisco Unified Communications Manager Bulk Administration Guide*.

Cisco Unified Communications Manager Administration Phone Addition

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.

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, see the “Cisco Unified Communications Manager Overview” chapter in the *Cisco Unified Communications Manager System Guide*.

Related Topics

Cisco Unified IP Phone MAC Address Determination, on page 59

BAT Phone Addition

Cisco Unified Communications Manager Bulk Administration Tool (BAT) enables you to perform batch operations, including registration, on multiple phones. To access BAT, choose the Bulk Administration drop-down menu in Cisco Unified Communications Manager Administration.

To add phones using BAT only (not in conjunction with TAPS), you can use the MAC address for each phone or dummy MAC addresses if you have a large number of new phones.

For detailed instructions about using BAT, see the Bulk Administration chapter in the *Cisco Unified Communications Manager Administration Guide*.

Related Topics

Cisco Unified IP Phone MAC Address Determination, on page 59

Cisco Unified IP Phones and Different Protocols

The Cisco Unified IP Phone can operate with SCCP (Skinny Client Control Protocol) or SIP (Session Initiation Protocol). You can convert a phone that is using one protocol for use with the other protocol.

Convert New Phone from SCCP to SIP

A new, unused phone is set for SCCP by default. To convert this phone to SIP, perform these steps:

Procedure

Step 1 Take one of these actions:

- To autoregister the phone, set the Auto Registration Phone Protocol parameter in Cisco Unified Communications Manager Administration to SIP.
- To provision the phone using the Bulk Administration Tool (BAT), choose the appropriate phone model and choose SIP from the BAT.
- To provision the phone manually, make the appropriate changes for SIP on the Phone Configuration window in Cisco Unified Communications Manager Administration.

  For more information about Cisco Unified Communications Manager configuration, see *Cisco Unified Communications Manager Administration Guide*.

  For more information about using BAT, see *Cisco Unified Communications Manager Bulk Administration Guide*.

Step 2 If you are not using DHCP in your network, configure the network parameters for the phone. See Network Settings, on page 69.

Step 3 Save the configuration updates, click **Apply Config**, click **OK** when the Apply Configuration Information dialog displays, then have the user power cycle the phone.

In-Use Phone Protocol to Protocol Conversion

Phones using SCCP can be upgraded to use SIP. To change from SCCP to SIP, the phone firmware must be updated to the recommended SIP version before the phones can register. New Cisco Unified IP Phones ship from the factory with SCCP phone firmware. These new phones must be upgraded to the recommended SIP version before they can complete registration.

For information about how to convert an in-use phone from one protocol to the other, see the *Cisco Unified Communications Manager Administration Guide*, chapter “Cisco Unified IP Phone Configuration”, section “Migration Existing Phone Configuration to a Different Phone”.

Deploy Phone in SCCP and SIP Environment

To deploy Cisco Unified IP Phones in an environment that includes SCCP and SIP and in which the Cisco Unified Communications Manager autoregistration parameter specifies SCCP, perform these general steps:

Procedure

Step 1 Set the Cisco Unified Communications Manager auto_registration_protocol parameter to SCCP.

Step 2 From Cisco Unified Communications Manager, choose **System** > **Enterprise Parameters**.

Step 3 Install the phones.

Step 4 Change the Auto Registration Protocol enterprise parameter to SIP.

Step 5 Autoregister the SIP phones.

Cisco Unified IP Phone MAC Address Determination

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

- From the phone, press the **Applications** button, select **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 select **Device Information**.

  For information about accessing the web page, see the “Accessing the Web Page for a Phone” section of this document.

CHAPTER 3

Cisco Unified IP Phone Setup

This chapter helps you install the Cisco Unified IP Phone on an IP telephony network.

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 Cisco Unified IP Phones and telephony networks, on page 47

Before You Begin

Before installing the Cisco Unified IP Phone, review the requirements in this section.

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:

- 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. The time displayed on the phone can differ from the Cisco Unified Communications Manager time by up to 10 seconds. If the Cisco Unified Communications Manager server is located in a different time zone than the phones, the phones do not display the correct local time.

Cisco Unified Communications Manager Setup

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 autoregistration, 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 autoregistration, see *Cisco Unified Communications Manager Administration Guide*.

You must use Cisco Unified Communications Manager Administration to configure and assign telephony features to the Cisco Unified IP Phones.

In Cisco Unified Communications Manager Administration, you can add users to the database, add users to user groups, and associate users to specific phones. In this way, users gain access their Cisco Unified Communications Manager User Option page to configure items such as call forwarding, speed dialing, and voice messaging system options.

Related Topics

Cisco Unified Communications Manager Phone Addition Methods, on page 55
Available telephony features, on page 90
Cisco Unified Communications Manager user addition, on page 121

Cisco Unified IP Phone 6921, 6941, 6945, and 6961 Components

The Cisco Unified IP Phone 6921, 6941, 6945, and 6961 include these components on the phone or as accessories for the phone:

Network and Access Ports

The back of the Cisco Unified IP Phone 6921, 6941, 6945, and 6961 includes these ports:

- Network port: Labeled network
- Access port: Labeled computer

Each port supports 10/100 Mbps half- or full-duplex connections to external devices. Cisco Unified IP Phone 6945 also supports 1000 Mbps full-duplex connections to external devices. You can use either Category 3, 5, or 5e cabling for 10-Mbps connections, but you must use Category 5 or 5e for 100 or 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.

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

Related Topics

Cisco Unified Communications Manager Phone Addition Methods, on page 55

Handset

The Cisco Unified IP Phone uses a handset that is designed especially for the phone. The handset includes a light strip to indicate incoming calls and voice messages waiting.

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

Disable Speakerphone

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

You can disable the speakerphone by using Cisco Unified Communications Manager Administration.

Procedure

Step 1 Select **Device** > **Phone**.

Step 2 Select the phone you want to modify.

Step 3 In the Phone Configuration window for the phone, check the **Disable Speakerphone** check box.

Headsets

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

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 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. For more information, see External device use, on page 65.

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.

Note The Cisco Unified IP Phone 6945 supports wideband headsets.

Audio Quality

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.

For additional information, see the Headsets for Cisco Unified IP Phones and Desktop Clients page on Cisco.com.

Wired Headsets

You can use the wired headset with all 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.

Connect to Wired Headset

To connect a wired headset to the Cisco Unified IP Phone, perform these steps:

Procedure

Step 1 Plug the headset into the Headset port on the back of the phone.

Step 2 Press the **Headset** button on the phone to place and answer calls using the headset.

Disable Wired Headset

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

Procedure

Step 1 To disable the headset from Cisco Unified Communications Manager Administration, choose **Device** > **Phone** and locate the phone that you want to modify.

Step 2 In the Phone Configuration window (Product Specific Configuration layout portion), select the **Disable Speakerphone and Headset** check box.

External device use

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 performs adequately when suitable devices are attached with 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].

Wireless Headset Using Auxiliary Port

The Cisco Unified IP Phone 6945 supports a wireless analog headset. To use a wireless headset, users connect a base station to the auxiliary port. The base station communicates with the wireless headset.

The Electronic Hookswitch feature enables users to remotely control basic IP phone functionality from the wireless headset. Basic IP phone functionality includes off-hook and on-hook, ring indication, audio volume control, and mute.

Enable Electronic Hookswitch

The Electronic Hookswitch feature supports the following headset devices:

- Jabra

- PRO9400 and GO6400 series
- Straight cable (Jabra Link14201-22)
- PRO920, GN9300 series and GN9120 the adapter cable Link 14201-16

For more information about wireless headsets that work in conjunction with the Electronic Hookswitch feature, go to the following URL:

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

To enable or disable the Electronic Hookswitch feature for a Cisco Unified IP Phone 6945, perform these steps:

Procedure

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

Step 2 Scroll to the Wireless Headset Hookswitch Control section.

Step 3 To enable Electronic Hookswitch, choose **Enabled**.

Step 4 To disable Electronic Hookswitch, choose **Disabled**.

Install Cisco Unified IP Phone

You must connect the Cisco Unified IP Phone to the network and to a power source before using it. Figure 1: Cisco IP Phone 6921 and 6941 connections, on page 2 shows the connections for Cisco Unified IP Phones 6921 and 6941. Figure 2: Cisco IP Phone 6945 connections, on page 13 shows the connections for a Cisco Unified IP Phone 6945. Figure 3: Cisco IP Phone 6961 connections, on page 19 shows the connections for a Cisco Unified IP Phone 6961.

Note Before you install a phone, even if it is new, upgrade the phone to the current firmware image. Before using external devices, see the Readme file for safety and performance information.

To install a Cisco Unified IP Phone, perform these tasks.

Procedure

Step 1 Connect the handset to the Handset port.

Step 2 Connect a headset to the Headset port. You can add a headset later if you do not connect one now. See the Headsets, on page 63 for supported headsets.

Step 3 Connect the power supply to the Cisco DC Adapter port. See the Cisco Unified Communications Manager Phone Addition Methods, on page 55 for guidelines.

Step 4 Connect a straight-through Ethernet cable from the switch to the network port labeled Network on the Cisco Unified IP Phone 6921, 6941, 6945, and 6961.Each Cisco Unified IP Phone ships with one Ethernet cable in the box.

You can use either Category 3, 5, or 5e cabling for 10-Mbps connections, but you must use Category 5 or 5e for 100 Mbps connections.

See the Network and Access Ports, on page 62 for guidelines.

Step 5 Connect a straight-through Ethernet cable from another network device, such as a desktop computer, to the access port labeled Computer on the Cisco Unified IP Phone 6921, 6941, 6945, and 6961. You can connect another network device later if you do not connect one now.
You can use either Category 3, 5, or 5e cabling for 10-Mbps connections, but you must use Category 5 or 5e for 100 Mbps connections.

See the Network and Access Ports, on page 62 for guidelines.

Related Topics

Phone Startup Verification, on page 68
Network Settings, on page 69

Cisco Unified IP Phone 6921 Installation

Use the diagram and table in Phone Connections, on page 2 to attach cables to the phone.

Cisco Unified IP Phone 6941 Installation

Use the diagram and table in Phone Connections, on page 6 to attach cables to the phone.

Cisco Unified IP Phone 6945 installation

Use the diagram and table in Phone Connections, on page 13 to attach cables to the phone.

Cisco Unified IP Phone 6961 Installation

Use the diagram and table in Phone Connections, on page 13 to attach cables to the phone.

Phone wall mount

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.

Note Wall mount kits are ordered separately from the phone.

Related Topics

Cisco Unified IP Phone 6921, 6941, 6945, and 6961 Wall Mount Kit, on page 211
Cisco Unified IP Phone Non-Lockable Wall Mount, on page 219

Phone Startup Verification

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 following LED buttons flash on and off during the various stages of boot up as the phone checks its hardware. See the following table for a list of the hardware test and the LED diagnostic status.

Table 8: LED Diagnostic Status

Hardware Test	MWI	Hold	Mute	Speaker
Power is Ready	On	On	On	On
Flash is Accessible	—	On	On	On
RAM Test Successful	—	—	On	On
Ethernet Test Successful	—	—	—	On

2. The screen displays the Cisco Systems, Inc., logo screen.
3. This message appears as the phone starts up.
    - Phone not registered
4. The home screen displays:
    - Current date and time
    - Primary directory number
    - Additional directory numbers and speed dial numbers, if configured (Only on Cisco Unified IP Phone 6961)
    - Softkeys

If the phone successfully passes through these stages, it has started up properly. If the phone does not start up properly, see the Startup Problems, on page 169.

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
- IPv6 addresses
- 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 Cisco Unified IP Phone Settings, on page 71

Cisco Unified IP Phone Security

The security features protect against several threats, including threats to the identity of the phone and to data. These features establish and maintain secure communication streams between the phone and the Cisco Unified Communications Manager server, and digitally sign files before they are delivered.

For more information about the security features, see the related topics and *Cisco Unified Communications Manager Security Guide*.

Related Topics

Cisco Unified IP Phone Security Features, on page 32

Set Up Locally Significant Certificate

You can initiate the installation of a Locally Significant Certificate (LSC) from the Security Configuration 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 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.

For more information, see *Cisco Unified Communications Manager Security Guide*.

To manually 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, choose **Applications** > **Admin Settings** > **Security Configuration**.

Note You can control access to the Administrator 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 To unlock settings, see the Password Protection, on page 73.

Step 4 Scroll to LSC and press **Update**.
The phone prompts for an authentication string.

Step 5 Enter the authentication code and press **Submit**.
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.

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 Configuration menu. Settings must be unlocked before you can press this softkey.

You can verify that an LSC is installed on the phone by choosing **Admin Settings** > **Phone Information** and ensuring that the LSC setting shows Installed.

CHAPTER 4

Cisco Unified IP Phone Settings

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:

Cisco Unified IP Phone configuration menus

The Cisco Unified IP Phone includes the following configuration menus:

- Network Setup: Provides options for viewing and making a variety of network settings.
- IPv4 Configuration: A submenu of the Network Setup menu, the IPv4 menu items provide additional network options for viewing and setting.
- IPv6 Configuration: A submenu of the Network Setup menu, the IPv6 menu items provide additional network options for viewing and setting.

Before you can change option settings on the Network Setup menu, you must unlock options for editing.

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.

Related Topics

IPv4 Setup Menu Options, on page 78
IPv6 Setup Menu Options, on page 83
Network Setup Menu, on page 73

Security Setup menu, on page 84

Display Configuration Menu

You can control whether a phone has access to the Settings menu or to options on this menu by using the Settings Access field in the Cisco Unified Communications Manager Administration Phone Configuration window. The Settings Access field accepts these values:

- **Enabled**: Allows access to the Settings menu.
- **Disabled**: Prevents access to the Settings menu.
- **Restricted**: Allows access to the User Preferences menu and allows volume changes to be saved. Prevents access to other options on the Settings menu.

If you cannot access an option on the Administrator Settings menu, check the Settings Access field.

To display a configuration menu, perform these steps:

Procedure

Step 1 Press **Applications**.

Step 2 Select **Admin Settings**.

Note For information about the Status menu, see Cisco Unified IP Phone Model Information, Status, and Statistics, on page 139 For information about the Reset Settings menu, see Troubleshooting and Maintenance, on page 169

Step 3 Enter the password and then press **Select**. The Admin Settings password is configured in the Local Phone Unlock Password parameter in the Common Phone Profile Configuration on Cisco Unified Communications Manager Administration.

Note Users can access the Admin Settings without entering a password when the Local Phone Unlock Password parameter is not configured

Step 4 Perform one of these actions to display the desired menu:

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

Step 5 To display a submenu, repeat Step 4.

Step 6 To exit a menu, press **Exit**.

Related Topics

Password Protection, on page 73
Edit Values, on page 73
Network Setup Menu, on page 73
IPv4 Setup Menu Options, on page 78
IPv6 Setup Menu Options, on page 83

Password Protection

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

Apply Phone Password

To apply a password to the phone, perform these steps:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, navigate to the Common Phone Profile Configuration window using **Device** > **Device Settings** > **Common Phone Profile**.

Step 2 Enter a password in the Local Phone Unlock Password option.

Step 3 Apply the password to the common phone profile that the phone uses.

Edit Values

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

- 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 **2** 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.
- To enter a period (for example, in an IP address), press * on the keypad.
- Press the up arrow on the navigation bar to move the cursor to the left most character, and press the down arrow on the navigation bar to move the cursor to the right most character.
- Press if you make a mistake. This softkey deletes the character to the left of the cursor.
- Press **Cancel** before pressing **Save** to discard any changes that you have made.

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 Cisco Unified IP Phone Reset or Restore, on page 187.

Network Setup Menu

The Network Setup menu provides options for viewing and making a variety of network settings. The following table describes these options and, where applicable, explains how to change them.

For information about how to access the Network Setup menu, see the Display Configuration Menu, on page 72.

For information about the keys you can use to edit options, see the Edit Values, on page 73.

Table 9: Network Setup Menu Options

Option	Description	To Change
IPv4 Setup	In the IPv4 Setup 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, see IPv4 Setup Menu Options, on page 78.	Scroll to IPv4 Setup and press **Select**.
IPv6 Setup	In the IPv6 Setup submenu, you can do the following: • Enable or disable the phone to use the IPv6 address that is assign by the DHCPv6 server. • Manually set the IPv6 Address, Subnet Prefix Length, IPv6 DNS Server, and IPv6 TFTP Servers. For more information on the IPv6 address fields, see IPv6 Setup Menu Options, on page 83.	Scroll to IPv6 Setup and press **Select**.
Host Name	Unique host name that the DHCP server assigned to the phone.	Display only—Cannot configure.
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.	Set Domain Name Field, on page 76

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 defaults to a VLAN ID of 4095.	Display only—Cannot configure. The phone obtains its Operational VLAN ID via Cisco Discovery Protocol (CDP) 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.	Set Admin VLAN ID Field, on page 77
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.	Set PC VLAN Field, on page 77
SW Port Setup	Speed and duplex of the network port. Valid values: • Auto Negotiate • 1000 Full: 1000-BaseT/full duplex (Supported only for Cisco Unified IP Phone 6945.) • 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.	Set SW Port Configuration Field, on page 77

Option	Description	To Change
PC Port Setup	Speed and duplex of the access port. Valid values: • Auto Negotiate • 1000 Full: 1000-BaseT/full duplex (Supported only for Cisco Unified IP Phone 6945.) • 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 autonegotiate. If you change the setting of this option, you must change the SW Port Configuration option to the same setting.	Set PC Port Configuration Field, on page 78
LLDP-MED: Switch Port	Enables and disables Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) on the switch port. Use this setting to force the phone to use a specific discovery protocol, which should match the protocol supported by the switch. Settings include: • Enabled: default • Disabled	From Cisco Unified Communications Manager Administration, choose **Device** > **Phone** > **Phone Configuration**.

Set Domain Name Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.

Step 2 Scroll to the Domain Name option, press **Edit**, and then enter a new domain name.

Step 3 Press **Apply**, and then press **Save**.

Set Admin VLAN ID Field

Procedure

Step 1 Scroll to the Admin. VLAN ID option, press **Edit** , and then enter a new Admin VLAN setting.

Step 2 Press **Apply**, and then press **Save**.

Set PC VLAN Field

Procedure

Step 1 Make sure the Admin VLAN ID option is set.

Step 2 Scroll to the PC VLAN option, press **Edit**, and then enter a new PC VLAN setting.

Step 3 Press **Apply**, and then press **Save**.

Set SW Port Configuration Field

Procedure

Step 1 Unlock network setup options.

Step 2 Scroll to the SW Port Setup option and then press **Edit**.

Step 3 Scroll to the setting that you want and then press **Select**.

Step 4 To configure the setting on multiple phones simultaneously, enable the Switch Port Remote Configuration in the Enterprise Phone Configuration (**System** > **Enterprise Phone Configuration**).

Note If the ports are configured for Switch Port Remote Configuration in Unified Communications Manager, the data cannot be changed on the phone.

Set PC Port Configuration Field

Procedure

Step 1 Unlock network setup options.

Step 2 Scroll to the PC Port Setup option and then press **Edit**.

Step 3 Scroll to the setting that you want and then press **Select**.

Step 4 To configure the setting on multiple phones simultaneously, enable the PC Port Remote Configuration in the Enterprise Phone Configuration (**System** > **Enterprise Phone Configuration**).

Note If the ports are configured for PC Port Remote Configuration in Unified Communications Manager, the data cannot be changed on the phone.

IPv4 Setup Menu Options

The IPv4 Setup menu is a submenu of the Network Setup menu. To reach the IPv4 Setup menu, select the IPv4 option on the Network Setup menu.

The following table describes the IPv4 Setup menu options.

For information about the keys you can use to edit options, see the Edit Values, on page 73.

Table 10: IPv4 Setup Menu Options

Option	Description	To Change
DHCP	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. For more information, see DHCP Usage, on page 82.	Set DHCP Field, on page 79
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.	Set IP Address Field, on page 80
Subnet Mask	Subnet mask used by the phone.	Set Subnet Mask Field, on page 80

Option	Description	To Change
Default Router 1	Default router used by the phone (Default Router 1).	Set Default Router Field, on page 80
DNS Server 1	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) used by the phone.	Set DNS Server Field, on page 80
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.	Set Alternate TFTP Field, on page 81
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 nonzero value for the TFTP Server 1 option.	Set TFTP Server 1 Field, on page 81
TFTP Server 2	Optional backup TFTP server that the phone uses if the primary TFTP server is unavailable.	Set TFTP Server 2 Field, on page 81
DHCP Address Released	Releases the IP address assigned by DHCP.	Release DHCP Address, on page 82

Set DHCP Field

Procedure

Step 1 Scroll to the DHCP option.

Step 2 Press **Edit**.

Step 3 Press either **No** to disable DHCP, or press **Yes** to enable DHCP.

Set IP Address Field

Procedure

Step 1 Set the DHCP option to **No**.
Step 2 Scroll to the IP Address option, press **Edit**, and then enter a new IP Address.
Step 3 Press **Apply**, then press **Save**.

Set Subnet Mask Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the Subnet Mask option, press **Edit**, and then enter a new subnet mask.
Step 3 Press **Apply**, then press **Save**.

Set Default Router Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the appropriate Default Router option, press **Edit**, and then enter a new router IP address.
Step 3 Press **Apply**, then press **Save**.

Set DNS Server Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the appropriate DNS Server option, press **Edit**, and then enter a new DNS server IP address.
Step 3 Press **Apply**, then press **Save**.

Set Alternate TFTP Field

Procedure

Step 1 Scroll to the Alternate TFTP option.

Step 2 Press **Yes** if the phone should use an alternative TFTP server; press **No** if the phone should not use an alternative TFTP server.

Set TFTP Server 1 Field

Procedure

Step 1 If DHCP is enabled, set the Alternate TFTP option to **Yes**.

Step 2 Scroll to the TFTP Server 1 option, press **Edit**, and then enter a new TFTP server IP address.

Step 3 Press **Apply**, then press **Save**.

Set TFTP Server 2 Field

Procedure

Step 1 Enter an IP address for the TFTP Server 1 option.

Step 2 Scroll to the TFTP Server 2 option, press **Edit**, and then enter a new backup TFTP server IP address.

Step 3 Press **Apply**, and then press **Save**.

Release DHCP Address

Procedure

Step 1 Scroll to the DHCP Address Released option.

Step 2 Press **Edit**.

Step 3 Press **Yes** to release the DHCP Address.

DHCP Usage

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.

Note You must also enter the domain name for the phone in the Ethernet Setup page.

Set Up Phone To Use 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, perform these steps:

Procedure

Step 1 Press **Applications** and choose **Administrator Settings** > **Network Setup** > **Ethernet Setup** > **IPv4 Setup**.

Step 2 To enable DHCP, set DHCP Enabled to **Yes**. DHCP is enabled by default.

Step 3 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 that DHCP assigns.

Step 4 Press **Apply**,

Set Up Phone To Not Use DHCP

When not using DHCP, you must configure the IP address, subnet mask, TFTP server, and default router locally on the phone.

Procedure

Step 1 Press **Applications** and choose **Administrator Settings** > **Network Setup** > **Ethernet Setup** > **IPv4 Setup**.

Step 2 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.

Step 3 Press **Apply**.

IPv6 Setup Menu Options

The IPv6 Setup menu is a submenu of the Network Setup menu. To reach the IPv6 Setup menu, select the IPv6 option on the Network Setup menu.

The following table describes the IPv6 Setup menu options.

Table 11: IPv6 Setup Menu Options

Option	Description
DHCPv6	Indicates whether the phone has DHCPv6 enabled or disabled. When DHCPv6 is enabled, the DHCPv6 server assigns the phone an IPv6 address. When DHCP v6 is disabled, the administrator must manually assign an IPv6 address to the phone.
IPv6 Address	Internet Protocol version 6 (IPv6) address of the phone. The IPv6 address is a 128 bit address. If you assign an IP address with this option, you must also assign the IPv6 prefix length and default router.
IPv6 Prefix Length	Subnet prefix length that is used by the phone. The subnet prefix length is a decimal value from 1-128, that specifies the portion of the IPv6 address that comprises the subnet.
IPv6 Default Router 1	Default router used by the phone (Default Router 1).
IPv6 DNS Server 1	Primary Domain Name System (DNS) server (DNS Server 1) used by the phone.
IPv6 Address Released	The phone has been configured to release its IPv6 address.
IPv6 Alternate TFTP	Indicates whether the phone is using the IPv6 Alternate TFTP server.

Option	Description
IPv6 TFTP Server 1 (SCCP phones only)	Primary IPv6 Trivial File Transfer Protocol (TFTP) server used by the phone.
IPv6 TFTP Server 2 (SCCP phones only)	Optional backup IPv6 TFTP server that the phone uses if the primary IPv6 TFTP server is unavailable.

Related Topics

Display Configuration Menu, on page 72
Password Protection, on page 73
Edit Values, on page 73

Security Setup menu

The Security Configuration menu provides information about various security settings. It provides access to the Trust List File screen and the 802.1x authentication.

The following table describes the options in this menu.

Table 12: 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**.
LSC	Indicates if a locally significant certificate (used for the security features) is installed on the phone (Installed) or is not installed on the phone (Not Installed).	For information about how to manage the LSC for your phone, see “Using the Certificate Authority Proxy Function” chapter in *Cisco Unified Communications Manager Security Guide*.
Trust List	The Trust List provides submenus for CTL signature and Call Manager/TFTP Server.	For more information, see the Trust List menu, on page 84.
802.1X Authentication	Displays the device authentication, EAP/MD5, and transaction status.	See 802.1X Authentication and Status, on page 85.

Trust List menu

The Trust List menu displays information about all the servers that the phone trusts and includes the options described in the following table.

To exit the Trust List menu, press **Back**.

Table 13: Trust List menu settings

Option	Description	To change
CTL File	Displays the MD5 hash of the CTL file.	For more information about this file, see “Configuring the Cisco CTL Client” chapter in the *Cisco Unified Communications Manager Security Guide*.
ITL File	Displays a submenu of options. Select an option to view its ITL setting information: • ITL Signature: MD5 hash of the ITL file • Unified CM/TFTP Server • CAPF Server • TVS	For more information about this file, see “Configuring the Cisco ITL Client” chapter in the *Cisco Unified Communications Manager Security Guide*.
Configuration (signed)	Displays the SRST router.	

802.1X Authentication and Status

The 802.1X Authentication and 802.1X Authentication Status menus allow you to enable 802.1X authentication and view transaction status. These options are described in the following table.

To exit these menus, press Exit.

Table 14: 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.	Set Device Authentication Field, on page 86

Option	Description	To Change
EAP-MD5	Device ID: A derivative of the phone model number and unique MAC address displayed in this format: CP-<model>-SEP-<MAC>	Set EAP-MD5 Device ID Field, on page 87
	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 of the phone, the shared secret is deleted.	Set EAP-MD5 Shared Secret Field, on page 87
	Realm: Indicates the user network domain, always set as Network.	Set EAP-MD5 Realm Field, on page 87
Transaction Status	Displays the transaction status of your 802.1X Authentication.	To view the transaction status of your 802.1X Authentication, choose **Applications** > **Admin Settings** > **Security Configuration** > **802.1X Authentication Status**.

Set Device Authentication Field

Procedure

Step 1 Choose **Applications** > **Admin Settings** > **Security Config** > **802.1X Authentication** > **Device Authentication**.

Step 2 Press **Edit**.

Step 3 Set the Device Authentication option to Enabled or Disabled.

Step 4 Press **Save**.

Set EAP-MD5 Device ID Field

Procedure

Step 1 Choose **Applications** > **Admin Settings** > **Security Config** > **802.1X Authentication** > **EAP-MD5** > **Device ID**.

Step 2 Press **Edit**.

Step 3 Set the Device ID.

Step 4 Press **Save**.

Set EAP-MD5 Shared Secret Field

Procedure

Step 1 Choose **Applications** > **Admin Settings** > **Security Config** > **802.1X Authentication** > **EAP-MD5** > **Shared Secret**.

Step 2 Press **Edit**.

Step 3 Enter the shared secret.

Step 4 Press **Save**.
See the Cisco Unified IP Phone Security Problems, on page 175 for assistance in recovering from a deleted shared secret.

Set EAP-MD5 Realm Field

Procedure

Step 1 Choose **Applications** > **Admin Settings** > **Security Config** > **802.1X Authentication** > **EAP-MD5** > **Realm**.

Step 2 Press **Edit**.

Step 3 Enter the Network.

Step 4 Press **Save**.

CHAPTER 5

Features, Templates, Services, and User Setup

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. The Cisco Unified Communications Manager documentation provides detailed instructions for these procedures.

To list supported features for all phones or for a particular phone model on your Cisco Unified Communications Manager, you can generate a Unified Communications Manager Phone Feature List report on Cisco Unified Reporting.

For suggestions about how to provide users with information about features, and what information to provide, see Internal support Web Site, on page 193.

For information about setting up phones in non-English environments, see International User Support, on page 199.

This chapter includes following topics:

Available telephony features

After you add Cisco Unified IP Phones to Cisco Unified Communications Manager, you can add functionality to the phones. The following table 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, see the *Cisco Unified IP Phone 6921, 6941, 6945, and 6961 User Guide for Cisco Unified Communications Manager (SCCP and SIP)*.

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, see the *Cisco Unified Communications Manager Administration Guide*.

For more information on the functions of a service, select the name of the parameter or the question mark help button in the Service Parameter Configuration window.

Table 15: Telephony features for the Cisco Unified IP Phone

Feature	Description	Configuration reference
Abbreviated Dialing	Allows users to speed dial a phone number by entering an assigned index code (1-99) on the phone keypad. **Note** You can use Abbreviated Dialing while on-hook or off-hook. Users assign index codes from the User Options web pages.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, “Cisco Unified IP Phone Configuration” • *Cisco Unified Communications Manager System Guide*, “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 greetings as needed. When a customer calls, both the agent and the customer 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 Communications Manager Administration application, choose **Device** > **Phone**, locate the 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 Communications Manager 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 Phone”
Any Call Pickup	Allows users to pick up a call on any line in their call pickup group, regardless of how the call was routed to the phone.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, “Call Pickup Configuration” chapter.
Assisted Directed Call Park (SIP only)	Enables users to park a call by pressing only one button using the Direct Park feature. Administrators must configure a Busy Lamp Field (BLF) Assisted Directed Call Park button. When users press an idle BLF Assisted Directed Call Park button for an active call, the active call is parked at the Direct Park slot associated with the Assisted Directed Call Park button.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, “Assisted Directed Call Park” chapter.
Audible Message Waiting Indicator (AMWI)	A stutter tone from the handset, headset, or speakerphone indicates that a user has one or more new voice messages on a line. **Note** The stutter tone is line-specific. You hear it only when using the line with the waiting messages.	For more information, see the *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phone” chapter.
Auto Answer	Connects incoming calls automatically after a ring or two. Auto Answer works with either the speakerphone or the headset.	For more information, see the *Cisco Unified Communications Manager Administration Guide*, “Directory Number Configuration” chapter.

Feature	Description	Configuration reference
Automatic Port Synchronization	When the Cisco Unified Communications Manager 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.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 Communications Manager, if the phone is powered by PoE.	To configure the parameter in the Cisco Unified Communications Manager 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 either the Enterprise Phone Configuration (**System** > **Enterprise Phone Configuration**) or the Common Phone Profile Configuration (**Device** > **Device Settings** > **Common Phone Profile**).
Auto Pickup	Allows a user to use one-touch pickup functionality for call pickup features.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" chapter.
Block External to External Transfer	Prevents users from transferring an external call to another external number.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, "External Call Transfer Restrictions" chapter.
Busy Lamp Field (BLF)	Allows a user to monitor the call state of a directory number associated with a speed-dial button on the phone.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, "Presence" chapter.
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, see the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" chapter.

Feature	Description	Configuration reference
Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available.	For more information, see: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" • *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Call Back"
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, see: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans" • *Cisco Unified Communications Manager Features and Services Guide*, "Call Display Restrictions"
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.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" • Customize User Options Web Page Display, on page 123
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, see the *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter.
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, see the *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter.

Feature	Description	Configuration reference
Call Forward Configurable Display	Allows you to specify information that appears on a phone when a call is forwarded. This information can include the caller name, caller number, redirected number, and original dialed number.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone"
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, see the *Cisco Unified Communications Manager System Guide*, "Understanding Directory Numbers" chapter.
Call Forward Notification	Allows you to configure the information that the user sees when receiving a forwarded call.	For more information, see Call Forward Notification Setup, on page 126.
Call History for Shared Line	Allows you to view shared line activity in the phone Call History. This feature will: • Log missed calls for a shared line • Log all answered and placed calls for a shared line	For more information, see Enable Call History for Shared Line, on page 119.
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, see the *Cisco Unified Communications Manager Features and Services Guide*, "Call Park and Directed Call Park" chapter.
Call Pickup	Allows users to redirect a call that is ringing on another phone within their pickup group to their phone. You can configure an audio and 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, see the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" chapter.

Feature	Description	Configuration reference
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. **Note** 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, see the *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. Incoming call information appears on the phone display.	For more information, see: • *Cisco Unified Communications Manager System Guide*, "Understanding Directory Numbers" • Phone Call Waiting Setup, on page 124
Call Waiting Ring	Provides Call Waiting users with the option of an audible ring instead of the standard beep. Options are Ring and Ring Once.	For more information, see the *Cisco Unified Communications Manager System Guide*, "Directory Numbers".
Caller ID	Caller identification such as a phone number, name, or other descriptive text appear on the phone display.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans" • *Cisco Unified Communications Manager Features and Services Guide*, "Call Display Restrictions" • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration".

Feature	Description	Configuration reference
Caller ID Blocking	Allows a user to block their phone number or email address from phones that have caller identification enabled.	For more information, see: • *Cisco Unified Communications Manager System Guide*, “Understanding Route Plans” • *Cisco Unified Communications Manager Administration Guide*, “Directory Number Configuration”
Calling Party Normalization	Calling party normalization presents phone calls to the user with a dialable phone number. Any escape codes are added to the number so that the user can easily connect to the caller again. The dialable number is saved in the call history and can be saved in the Personal Address Book.	For more information, see Calling Party Normalization, on page 128
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*.
cBarge	Allows a user to join a nonprivate call on a shared phone line. cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, “Cisco Unified IP Phone Configuration” • *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phone” • *Cisco Unified Communications Manager Features and Services Guide*, “Barge and Privacy”
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 when they log 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, see the *Cisco Unified Communications Manager Features and Services Guide*, “Cisco Extension Mobility” chapter.

Feature	Description	Configuration reference
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. **Note** Configure Cisco Extension Mobility on Cisco Unified IP Phones before you configure EMCC.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Extension Mobility Cross Cluster" chapter.
Cisco Unified Communications Manager Express (Unified CME) Version Negotiation	The Cisco Unified Communication Manager Express uses a special tag in the information sent to the phone to identify itself. This tag enables the phone to provide services to the user that the switch supports.	For more information, see: • *Cisco Unified Communications Manager Express System Administrator Guide* • Cisco Unified IP Phone and Cisco Unified Communications Manager Express Interaction, on page 49
Cisco Unified Video Advantage (CUVA)	Allows users to make video calls by using your Cisco Unified IP Phone, your personal computer, and an external video camera. **Note** Configure the Video Capabilities parameter in the Product Specific Configuration Layout section in Phone Configuration.	For more information, see the Cisco Unified Video Advantage documentation.
Cisco WebDialer	Allows users to make calls from web and desktop applications.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, "Cisco WebDialer" chapter.
Classic Ringtone	Supports 29 ringtones: 2 embedded in the phone firmware and 27 downloaded from the Cisco Unified Communications Manager. The feature makes the available ringtones common with other Cisco Unified IP Phones.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" • Custom Phone Rings, on page 132
Client Matter Code (CMC)	Enables a user to specify that a call relates to a specific client matter.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, "Client Matter Codes and Forced Authorization Codes" chapter.

Feature	Description	Configuration reference
Conference	• Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference and Meet Me. • Allows a noninitiator in a standard (ad hoc) conference to add or remove participants; also allows any conference participant to join together two standard conferences on the same line.	The Advance Adhoc Conference service parameter, disabled by default in Cisco Unified Communications Manager Administration, allows you to enable these features. For information on conferences, see the *Cisco Unified Communications Manager System Guide*, "Conference Bridges" chapter. For more information, see *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter. **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, see *Cisco Unified Communications Manager Administration Guide*, "CTI Route Point Configuration" chapter.
Debug Phone	Provides an additional menu on the phone for debugging phone problems. For more information, see Troubleshoot Using Debug Menu, on page 184	No configuration required.
Device Invoked Recording	Provides end users with the ability to record their telephone calls via a softkey. In addition administrators may continue to record telephone calls via the CTI User Interface.	For more information, see Enable Device Invoked Recording, on page 119
Direct Transfer	Allows users to connect two calls to each other without remaining on the line.	For more information, see the *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter.
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. **Note** If you implement Directed Call Park, avoid configuring the Park softkey. This prevents users from confusing the two Call Park features.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, "Call Park and Directed Call Park" chapter.

Feature	Description	Configuration reference
Directed Call Pickup	Allows a user to answer a call that is ringing on a particular directory number.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, “Call Pickup” chapter.
Disable Single Button Barge	The softkeys are controlled by configuration in the Cisco Unified Communications Manager. The Line Key Barge parameter in the Administration window has the following options: • Default: The Barge and cBarge buttons are always available for use by the user. • Off: The Barge and cBarge buttons are never available by use by the user • Turn on softkey: The Barge and cBarge buttons are displayed, if configured in the phone profile.	For more information, see the *Cisco Unified Communications Manager Administration Guide*.
Distinctive Ring	Users can customize how their phone indicates an incoming call and a new voice mail message.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, “Call Pickup” chapter.
Divert	Allows a user to transfer a ringing, connected, or held call directly to a voice-messaging system. When a call is diverted, the line becomes available to make or receive new calls.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, “Immediate Divert” chapter.

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, see the *Cisco Unified Communications Manager Features and Services Guide*, “Do Not Disturb” chapter.
Electronic Hookswitch	Enables users to remotely control basic IP phone functionality from a wireless analog headset connected to the phone auxiliary port. Basic IP phone functionality includes off-hook/on-hook, ring indication, audio volume control, and mute/unmute. **Note** This feature applies to the Cisco Unified IP Phone 6945 only.	For more information, see Enable Electronic Hookswitch, on page 65.
EnergyWise	Enables an IP Phone to sleep (power down) and wake (power up) at predetermined times, to promote energy savings.	For more information, see EnergyWise on the Cisco Unified IP Phone Setup, on page 135.
Enhanced Secure Extension Mobility Cross Cluster (EMCC)	Improves the Secure Extension Mobility Cross Cluster (EMCC) feature by preserving the network and security configurations on the login phone. By so doing, security policies are maintained, network bandwidth is preserved and network failure is avoided within the visiting cluster (VC).	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, “Cisco Extension Mobility Cross Cluster” 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, see Modify Phone Button Template for PAB or Fast Dial, on page 116.

Feature	Description	Configuration reference
Forced Authorization Code (FAC)	Controls the types of calls that certain users can place.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, “Client Matter Codes and Forced Authorization Codes” chapter.
Headset Sidetone Control	Allows an administrator to set the sidetone level of a wired headset. Available sidetone levels are: • Normal • Low • Very Low • Off	For more information, see the *Cisco Unified Communications Manager Administration Guide*, “Cisco Unified IP Phone Configuration” chapter.
Group Call Pickup	Allows a user to answer a call that is ringing on a directory number in another group.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, “Call Pickup” chapter.
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. You can configure call focus priority to favor incoming or reverting calls.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, “Hold Reversion” chapter.
Hold Status	Enables phones with a shared line to distinguish between the local and remote lines that placed a call on hold.	No configuration required.
Hold/Resume	Allows the user to move a connected call from an active state to a held state.	• No configuration required unless you want to use Music On Hold. See “Music On Hold” in this table for information. • See “Hold Reversion” in this table.
HTTP Download	Enhances the file download process to the phone to use HTTP by default. If the HTTP download fails, the phone reverts to using the TFTP download.	No configuration required.

Feature	Description	Configuration reference
HTTPS for Phone Services	Increases security by requiring communication using HTTPS. Enable the HTTPS Service parameter using **Device** > **Phone** or **System** > **Enterprise Phone Configuration**. **Note** IP Phones can be HTTPS clients; they cannot be HTTPS servers.	For more information, see the Cisco Unified Communications Manager documentation.
Hunt Group	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 the first directory number in the hunt group is busy, the system hunts in a predetermined sequence for the next available directory number in the group and directs the call to that phone.	For more information, see: • *Cisco Communications Manager Administration Guide*, "Hunt Group Configuration" • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans"
Incoming Call Toast Timer	Allows you to set the length of time that an incoming call toast (notification) appears on the phone screen.	For more information, see Incoming Call Toast Timer Setup, on page 128.
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.	For more information, see the *Cisco Unified Communications Manager Feature and Services Guide*, "Intercom" chapter.
Jitter Buffer	The Jitter Buffer feature handles jitter from 10 milliseconds (ms) to 1000 ms for both audio and video streams.	No configuration required.

Feature	Description	Configuration reference
Join Across Lines	Allows users to combine calls that are on multiple phone lines to create a conference call.	Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco Unified IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines. For more information, see Join and Direct Transfer Policy, on page 112. For more information, see the *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter.
Join	Allows users to combine two calls that are on one line to create a conference call and remain on the call.	Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco Unified IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines. For more information, see Join and Direct Transfer Policy, on page 112. For more information, see: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" • *Cisco Unified IP Phone 6921, 6941, 6945, and 6961 User Guide for Cisco Unified Communications Manager (SCCP and SIP)*
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 nonhunt group calls from ringing their phone.	For more information, see: • See Softkey Template Setup, on page 116 • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans"

Feature	Description	Configuration reference
Line Status for Call Lists	Allows the user to see the Line Status availability status of monitored line numbers in the Call History list. The Line Status states are • Unknown • Idle • Busy • DND	For more information, see Enable Line Status for Call Lists, on page 129.
Malicious Caller Identification (MCID)	Allows users to notify the system administrator about suspicious calls that are received.	For more information, see: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" • *Cisco Unified Communications Manager Features and Services Guide*, "Malicious Call Identification"
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, see the *Cisco Unified Communications Manager Administration Guide*, "Meet Me Number/Pattern Configuration" chapter.
Message Waiting	Defines directory numbers for message waiting on and off indicators. A directly-connected voice-message 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, see: • *Cisco Unified Communications Manager Administration Guide*, "Message Waiting Configuration" • *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager"
Message Waiting Indicator	A light on the handset that indicates that a user has one or more new voice messages.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Message Waiting Configuration" • *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager"

Feature	Description	Configuration reference
Minimum Ring Volume	Sets a minimum ringer volume level for an IP phone. The minimum ringer volume level can range from 0 to 14. The default is 0 (silent).	For more information, see Set Minimum Ring Volume , on page 129.
Missed Call Logging	Allows a user to specify whether missed calls will be logged in the missed calls directory for a given line appearance.	For more information, see the *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter.
Mobile Connect	Enables users to manage business calls using a single phone number and pick up in-progress calls on the desk 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.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Unified Mobility" chapter.
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, see the *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Unified Mobility" chapter.
Multilevel Precedence and Preemption (MLPP) (SCCP phones only)	Provides a method of prioritizing calls within your phone system. Use this feature when users work in an environment where they need to make and receive urgent or critical calls.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, "Multilevel Precedence and Preemption" chapter.
Multiple Calls Per Line Appearance	Each line can support multiple calls. By default, your phone supports two active calls per line, and a maximum of six active calls per line. Only one call can be connected at any time; other calls are automatically placed on hold. The system allows you to configure maximum calls/busy trigger not more than 6/6 both for SCCP and SIP. Any configuration more than 6/6 is not officially supported. For SCCP, you must upgrade to Cisco Unified Communications Manager 8.6 or above to support multiple calls per line.	For more information, see the *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter.
Music On Hold	Plays music while callers are on hold.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, "Music On Hold" chapter.
Mute	Mutes the microphone from the handset or headset.	No configuration required.
No Alert Name	Makes it easier for end users to identify transferred calls by displaying the original caller's phone number. The call appears as an Alert Call followed by the caller's telephone number.	No configuration required.

Feature	Description	Configuration reference
Onhook Dialing	Allows a user to dial a number without going off hook. The user can then either pick up the handset or press Dial.	For more information, see the *Cisco Unified IP Phone 6921, 6941, 6945, and 6961 User Guide for Cisco Unified Communications Manager (SCCP and SIP)*.
Other Group Pickup	Allows a user to answer a call ringing on a phone in another group that is associated with the user's group.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, “Call Pickup” chapter.
Phone Display Message for Extension Mobility Users	This feature enhances the phone interface for the Extension Mobility user by providing friendly messages.	No configuration required.
PLK Support for Queue Statistics	The PLK Support for Queue Statistics feature enables the users to query the call queue statistics for hunt pilots and the information appears on phone screen.	For more information, see Softkey Template Setup, on page 116.
Plus Dialing	Allows the user to dial E.164 numbers prefixed with a plus (+) sign. To dial the + sign, the user needs to press and hold the star (*) key for at least 1 second. This applies to dialing the first digit for an on-hook (including edit mode) or off-hook call.	No configuration required.
Privacy	Prevents users who share a line from adding themselves to a call and from viewing information on their phone display about the call of the other user.	For more information, see: • *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, see the *Cisco Unified Communications Manager Administration Guide*, “Directory Number Configuration” chapter.

Feature	Description	Configuration reference
Programmable Feature Buttons	You can assign features, such as New Call, Call Back, and Forward All to line buttons.	For more information, see: • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter • *Cisco Unified Communications Manager Administration Guide*, "Phone Button Template Configuration" chapter
Quality Reporting Tool (QRT)	Allows users to submit information about problem phone calls by pressing a button. QRT can be configured for either of two user modes, depending upon the amount of user interaction desired with QRT.	For more information, see: • *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 a button or the Redial softkey.	No configuration required.
Reroute Direct Calls to Remote Destination to Enterprise Number	Reroutes a direct call to a user's mobile phone to the enterprise number (desk phone). For an incoming call to remote destination (mobile phone), only remote destination rings; desk phone does not ring. When the call is answered on their mobile phone, the desk phone displays a Remote In Use message. During these calls, users can make use of various features of their mobile phone.	For more information, see the *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Unified Mobility" chapter.

Feature	Description	Configuration reference
Remote Port Configuration	Allows the administrator to configure the speed and duplex function of the phone Ethernet ports remotely by using Cisco Unified Communications Manager 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 Communications Manager, the data cannot be changed on the phone.	To configure the parameter in the Cisco Unified Communications Manager Administration application, choose **Device** > **Phone**, select the appropriate IP phone, 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 configuration in either Enterprise Phone Configuration (**System** > **Enterprise Phone Configuration**) or Common Phone Profile Configuration (**Device** > **Device Settings** > **Common Phone Profile**. (Switch Port Remote Configuration or PC Port Remote Configuration)
Ringtone Setting	Identifies ring type used for a line when a phone has another active call.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter • Custom Phone Rings, on page 132
RTCP Hold For SIP	Ensures that held calls are not dropped by the gateway. The gateway checks the status of the RTCP port to determine if a call is active or not. By keeping the phone port open, the gateway will not end held calls.	No configuration required.
Secure Conference	• Allows secure phones to place conference calls using a secured conference bridge. • As new participants are added by using Confrn, Join, cBarge, 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 nonsecure participants from the Conference List. Noninitiators can add or remove conference participants if the Advanced Adhoc Conference Enabled parameter is set.)	For more information about security, see the Supported Security Features, on page 34. For additional information, see: • *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*

Feature	Description	Configuration reference
Secure EMCC	Improves the EMCC feature by providing enhanced security for a user logging into their phone from a remote office.	No configuration required.
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, see the following: • *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	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.	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
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, see the *Cisco Unified Communications Manager System Guide*, "Understanding Directory Numbers" chapter.
Show Calling ID and Calling Number	The phones can display both the calling ID and calling number for incoming calls. The IP phone LCD display size limits the length of the calling ID and the calling number that display. The Show Calling ID and Calling Number feature applies to the incoming call alert only and does not change the function of the Call Forward and Hunt Group features.	For more information, see "Caller ID" in this table.

Feature	Description	Configuration reference
Monitoring and Recording	Allows a supervisor to silently monitor an active call. The supervisor cannot be heard by either party on the call. The user might hear a monitoring audible alert tone during a call when it is being monitored. 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 monitored. **Note** When an active call is being monitored or recorded, the use can receive or place intercom calls; however, if the user 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, see the *Cisco Unified Communications Manager Features and Services Guide*, “Monitoring and Recording” chapter.
Speed Dial	Dials a specified number that has been previously stored.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, “Cisco Unified IP Phone Configuration” • *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phone”
SSH Access	Allows the administrator to enable or disable the SSH Access setting using Cisco Unified Communications Manager Administration. This option indicates whether the phone supports the SSH Access. Settings include: • Enabled • Disabled—Default Enabling the SSH server allows the phone to accept the SSH connections. Disabling the SSH server functionality of the phone blocks the SSH access to the phone.	For more information, see Set Up SSH Access, on page 127

Feature	Description	Configuration reference
Time-of-Day Routing	Restricts access to specified telephony features by time period.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, "Time Period Configuration" • *Cisco Unified Communications Manager System Guide*, "Time-of-Day Routing"
Time Zone Update	Updates the Cisco Unified IP Phone with time zone changes.	For more information, see 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.	Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco Unified IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines. For more information, see the Join and Direct Transfer Policy, on page 112.
Transfer - Direct Transfer	Transfer: The first invocation of Transfer will always initiate a new call by using the same directory number, after putting the active call on hold. Direct Transfer: This transfer joins two established calls (call is in hold or in connected state) into one call and drops the feature initiator from the call. Direct Transfer does not initiate a consultation call and does not put the active call on hold.	Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco Unified IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines. For more information, see the Join and Direct Transfer Policy, on page 112. For more information, see the *Cisco Unified Communications Manager System Guide*, "Understanding Directory Numbers" chapter.

Feature	Description	Configuration reference
TVS	Trust Verification Services (TVS) enables phones to authenticate signed configurations and authenticate other servers or peers without increasing the size of the Certificate Trust List (CTL) or requiring the downloading of an updated CTL file to the phone. TVS is enabled by default. TVS details can be viewed from the **Applications** > **Admin Settings** > **Security Settings** > **Trust List** menu of the phone.	No configuration required.
UCR 2008 (SCCP only)	The Cisco Unified IP Phones using SCCP support Unified Capabilities Requirements (UCR) 2008 by providing the following functions: • Support for Federal Information Processing Standard (FIPS) 140-2 • Support for 80-bit SRTCP Tagging As an IP Phone administrator, you must set up specific parameters in Cisco Unified Communications Manager Administration.	For more information, see UCR 2008 Setup, on page 124.
Voice Message System	Enables callers to leave messages if calls are unanswered.	For more information, see: • *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
Web Access Disabled by Default	Enhances security by disabling access to all web services, such as HTTP. Users can only access web services if the administrator enables web access.	For more information, see UCR 2008 Setup, on page 124.

Join and Direct Transfer Policy

Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco Unified IP Phone. In order for these applications to control and monitor these phones, you must configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines. You can configure the Join and Direct Transfer Policy for the following:

- To configure the policy for all phones on the system, choose **System** > **Enterprise Phone Configurations** from Cisco Unified Communications Manager Administration.
- To configure the policy to a group of phones, choose **Device** > **Device Settings** > **Common Phone Profile** from Cisco Unified Communications Manager Administration.
- To configure the policy on an individual phone, configure the Join and Direct Transfer Policy in the Phone Configuration for the specific phone.

Because this parameter can be configured in three different windows, 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

When you change the setting of the Join and Direct Transfer Policy Parameter, you must check the Override Common Settings box for the setting to take effect. The default policy is to have Same line, across line enabled for join and direct transfer.

To determine the proper setting for this parameter, refer to the documentation of the JTAPI/TAPI application.

Corporate and Personal Directory setup

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 coworkers. To support this feature, you must configure corporate directories.

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.

Corporate Directory setup

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 user rights to access the system. Authorization identifies the telephony resources that a user is permitted to use, such as a specific phone extension.

For more information, see “Understanding Directory Numbers” in the *Cisco Unified Communications Manager System Guide*.

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

Personal Directory Setup

Personal Directory consists of the following features:

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

Users can use these methods to access Personal Directory features:

- 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 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 WAB. TabSync can then be used to synchronize the WAB with Personal Directory. For instructions about TABSync, see Obtain Cisco Unified IP Phone Address Book Synchronizer, on page 195 and Cisco Unified IP Phone Address Book Synchronizer Deployment, on page 195.

To ensure that Cisco IP Phone Address Book Synchronizer users access only their end-user data, 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 sign-in information.

Phone Button Template Modification

Phone button templates let you assign speed dials and call-handling features to programmable line buttons. Call-handling features that can be assigned to buttons include call forward, hold, and conference.

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. For more information, see *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide*.

- The default Cisco Unified IP Phone 6921 template that ships with the phone uses buttons 1 and 2 for lines.
- The default Cisco Unified IP Phone 6941 template that ships with the phone uses buttons 1 through 4 for lines.
- The default Cisco Unified IP Phone 6945 template that ships with the phone uses buttons 1 through 4 for lines.

- The default Cisco Unified IP Phone 6961 template that ships with the phone uses buttons 1 through 12 for lines.

To avoid confusion for users, do not assign a feature to a button and a softkey at the same time.

Related Topics

Softkey Template Setup, on page 116

Set Up PAB or Speed Dial as 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>* (Depends on the protocol that the Cisco Unified IP Phone supports.)

Step 4 Select **Save**.

You can add, update, or delete service parameters 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; otherwise, users must resubscribe to the service to rebuild the correct URL.

Modify Phone Button Template for PAB or Fast Dial

For more information about IP Phone services, see "Cisco Unified IP Phone Services Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*. For more information about configuring line buttons, see "Cisco Unified IP Phone Configuration" chapter and "Configuring Speed-Dial Buttons" section in the *Cisco Unified Communications Manager Administration Guide*.

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 Select **Copy**, enter a name for the new template, and then select **Save**.
The Phone Button Template Configuration window opens.

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

Step 6 Select **Save** to create a new phone button template that uses 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.

Step 9 Select **Save** to store the change and then select **Reset** to implement the change.
The phone user can now access the User Options web pages and associate the service with a button on the phone.

Softkey Template Setup

Using Cisco Unified Communications Manager Administration, you can associate up to 18 softkeys with applications that are supported by the Cisco Unified IP Phone 6921, 6941, 6945, and 6961.
Cisco Unified Communications Manager support the Standard User and Standard Feature softkey template.

An application that supports softkeys can have one or more standard softkey templates associated with it. You can modify a standard softkey template by making a copy of it, giving it a new name, and making updates to that copied softkey template. You can also modify a nonstandard softkey template.

To configure softkey templates, select **Device** > **Device Settings** > **Softkey Template** from Cisco Unified Communications Manager Administration. To assign a softkey template to a phone, use the Softkey Template field in the Cisco Unified Communications Manager Administration Phone Configuration page. For more information, see *Cisco Unified Communications Manager Administration Guide*, "Softkey Template Configuration" and the *Cisco Unified Communications Manager System Guide*, "Softkey Template".

The Cisco Unified IP Phone 6921, 6941, 6945, and 6961 do not support all the softkeys that are configurable in Softkey Template Configuration on Cisco Unified Communications Manager Administration. The following table lists the features, softkeys that can be configured on a softkey template, and note whether it is supported on the Cisco Unified IP Phone 6921, 6941, 6945, and 6961.

Note Cisco Unified Communications Manager allows you to configure any softkey in a softkey template, but unsupported softkeys do not display on the phone.

Table 16: Configurable Softkeys

Feature	Configurable softkeys in the Softkey Template configuration	Supported as a softkey on Cisco Unified IP Phone 6921, 6941, 6945, and 6961	Notes
Answer	Answer (Answer)	Yes	—
Barge	Barge (Barge)	No	Configure as a programmable line button or as a softkey.
Call Back	Call Back (CallBack)	Yes	—
Call Forward All	Forward All (cfwdAll)	Yes	Phone displays **Fwd ALL** or **Fwd Off**.
Call Park	Call Park (Park)	Yes	—
Call Pickup	Pick Up (Pickup)	Yes	Configure as a programmable line button or as a softkey.
cBarge	Conference Barge (cBarge)	Yes	Configure as a programmable line button or as a softkey.
Conference	Conference (Confrn)	No	Conference is a dedicated button.
Conference List	Conference List (ConfList)	No	Phone displays **Detail**.
Divert	Immediate Divert (iDivert)	Yes	Phone displays **Divert**.
Do Not Disturb	Toggle Do Not Disturb (DND)	Yes	Configure Do Not Disturb as a programmable line button or softkey.

Feature	Configurable softkeys in the Softkey Template configuration	Supported as a softkey on Cisco Unified IP Phone 6921, 6941, 6945, and 6961	Notes
End Call	End Call (EndCall)	Yes	Phone displays **Cancel** if the call is not answered.
Group Pickup	Group Pick Up (GPickUp)	Yes	Configure as a programmable line button or as a softkey.
Hold	Hold (Hold)	No	Hold is a dedicated button.
Hunt Group	HLog (HLog)	Yes	Configure Hunt Group as a programmable feature button.
Join	Join (Join)	No	—
Malicious Call Identification	Toggle Malicious Call Identification (MCID)	Yes	Configure Malicious Call Identification as a programmable feature button or softkey.
Meet Me	Meet Me (MeetMe)	Yes	Configure as a programmable line button or as a softkey.
Mobile Connect	Mobility (Mobility)	Yes	Configure Mobile Connect as a programmable feature button or softkey.
New Call	New Call (NewCall)	Yes	Phone displays **New Call**.
Other Pickup	Other Pickup (oPickup)	Yes	Configure as a programmable line button or as a softkey.
PLK Support for Queue Statistics	Queue Status	Yes	—
Quality Reporting Tool	Quality Reporting Tool (QRT)	Yes	Configure Quality Reporting Tool as a programmable feature button or softkey.
Redial	Redial (Redial)	Yes	—
Remove Last Conference Participant	Remove Last Conference Participant (Remove)	Yes	Phone displays **Remove** when a participant is selected.
Resume	Resume (Resume)	Yes	—

Feature	Configurable softkeys in the Softkey Template configuration	Supported as a softkey on Cisco Unified IP Phone 6921, 6941, 6945, and 6961	Notes
Speed Dial	Abbreviated Dial (AbbrDial)	Yes	Phone displays **SpeedDial**.
Transfer	Direct Transfer (DirTrfr)	No	Transfer is a dedicated button. Configure transfer (Direct Transfer policy) in the Product Specific Configuration Layout section in Phone Configuration.
Video Mode Command	Video Mode Command (VidMode)	No	—

Enable Device Invoked Recording

Configure the Device Invoked Recording feature from Cisco Unified Communications Manager. To enable this feature, perform the following steps.

Procedure

Step 1 Set the IP phone Built In Bridge to **On**.

Step 2 Set Recording Option to **Selective Call Recording Enabled**.

Step 3 Select the appropriate Recording Profile.

Enable Call History for Shared Line

For more information, see *Cisco Unified Communications Manager Administration Guide*.

Procedure

Step 1 Go to Cisco Unified CM Administration and choose **Device** > **Phone**.

Step 2 Find your phone from the list of phones associated with the Cisco Unified CM.

Step 3 Click on the Device Name of the phone.
The Phone Configuration window appears.

Step 4 Go to Product Specific Configuration Layout area and from the Logging Display drop-down list box, choose the applicable profile.

The Disabled option is selected by default.

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 as well, 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

Services Setup

You can give users access to Cisco Unified IP Phone Services on the Cisco Unified IP Phone 6921, 6941, 6945, and 6961. You can also assign a button or a softkey to different phone services. These services comprise XML applications that enable the display of interactive content with text and graphics on the phone. 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 available services.
- 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, user configuration of IP Phone applications.

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.

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

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.

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

Related Topics

Phone Features User Subscription and Setup, on page 194

Cisco Unified Communications Manager user addition

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, see *Cisco Unified Communications Manager Administration Guide*, "End User Configuration".

- 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, see the *Cisco Unified Communications Manager Administration Guide*, "Bulk Administration".

- To add users from your corporate LDAP directory, choose **System** > **LDAP** > **LDAP System** from Cisco Unified Communications Manager Administration.

  Note After the Enable Synchronization from the LDAP Server is enabled, you will not be able to add additional users from Cisco Unified Communications Manager Administration.

  For more information on LDAP, see the *Cisco Unified Communications Manager System Guide*, "Understanding the Directory".

- To add a user and phone at the same time, choose **User Management** > **User/Phone Add** from Cisco Unified Communications Manager.

User Options Web Pages Management

From the User Options web pages, users can customize and control several phone features and settings. For detailed information about the User Options web pages, see the user guide.

Set Up Access to 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.

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

- The URL for accessing the application. This URL is: **http:**//<*server_name:portnumber*>/**ccmuser**/, where *server_name* is the host on which the web server is installed and *portnumber* is the port number on that host.
- A user ID and default password for accessing the application. These settings correspond to the values that you entered when you added the user to Cisco Unified Communications Manager.

For more information, see:

- *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

Add User to End User Group

To add a user to the Cisco Unified Communications Manager Standard End User group, perform 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 Select the **Standard CCM End Users** link. The User Group Configuration window for the Standard CCM End Users appears.

Step 4 Select **Add End Users to Group**. The Find and List Users window appears.

Step 5 Use the Find User drop-down list boxes to find the users that you want to add and click **Find**. A list of users that matches your search criteria appears.

Step 6 In the list of records that appear, click the check box next to the users that you want to add to this user group. If the list is long, use the links at the bottom to see more results.

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

Step 7 Choose **Add Selected**.

Associate Phones with Users

You associate phones with users from the Cisco Unified Communications Manager End User window.

Procedure

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

The Find and List Users window appears.

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

Step 3 In the list of records that appear, select the link for the user.

Step 4 Select **Device Association**.
The User Device Association window appears.

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

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

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

Step 8 From the Related Links drop-down list in the upper, right corner of the window, select **Back to User**, and click **Go**.
The End User Configuration window appears and the associated devices that you chose display in the Controlled Devices pane.

Step 9 Choose **Save Selected/Changes**.

Customize User Options Web Page Display

Most options that display on the User Options web pages appear by default. However, the system administrator must set the following options 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, perform 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 displays on the User Options web pages by choosing one of these values from the Parameter Value drop-down list 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.

Phone Call Waiting Setup

The Cisco Unified IP Phones 6921, 6951, 6945, and 6961 support multiple calls per line. With multiple calls per line, setting up call waiting is simplified on the Cisco Unified Communications Manager. For more information, see the "Understanding Directory Numbers" chapter in the *Cisco Unified Communications Manager System Guide*.

UCR 2008 Setup

The parameters that support UCR 2008 reside in Cisco Unified Communications Manager Administration. The following table describes the parameters and indicates the procedure to change the setting.

Table 17: UCR 2008 Parameter Location

Parameter	Administration Path	Procedure
FIPS Mode	**Device** > **Device Settings** > **Common Phone Profile**	Set Up UCR 2008 in Common Phone Profile, on page 125
	System > **Enterprise Phone Configuration**	Set Up UCR 2008 in Enterprise Phone Configuration, on page 126
SSH Access	**Device** > **Phone**	Set Up UCR 2008 in Phone, on page 125
	Device > **Device Settings** > **Common Phone Profile**	Set Up UCR 2008 in Common Phone Profile, on page 125
Web Access	**Device** > **Phone**	Set Up UCR 2008 in Phone, on page 125
80-bit SRTCP	**Device** > **Device Settings** > **Common Phone Profile**	Set Up UCR 2008 in Common Phone Profile, on page 125
	System > **Enterprise Phone Configuration**	Set Up UCR 2008 in Enterprise Phone Configuration, on page 126
IP Addressing Mode	**Device** > **Device Settings** > **Common Device Configuration**	Set Up UCR 2008 in Common Device Configuration, on page 126

Parameter	Administration Path	Procedure
IP Addressing Mode Preference for Signaling	**Device** > **Device Settings** > **Common Device Configuration**	Set Up UCR 2008 in Common Device Configuration, on page 126

Set Up UCR 2008 in Phone

Use this procedure to set the following UCR 2008 parameters:

- SSH Access
- Web Access

Procedure

Step 1 Choose **Device** > **Phone**.
Step 2 Set the SSH Access parameter to **Disabled**.
Step 3 Set the Web Access parameter to **Disabled**.
Step 4 Select **Save**.

Set Up UCR 2008 in Common Phone Profile

Use this procedure to set the following UCR 2008 parameters:

- FIPS Mode
- SSH Access
- 80-bit SRTCP

Procedure

Step 1 Choose **Device** > **Device Settings** > **Common Phone Profile**.
Step 2 Set the FIPS Mode parameter to **Enabled**.
Step 3 Set the SSH Access parameter to **Disabled**.
Step 4 Set the 80-bit SRTCP parameter to **Enabled**.
Step 5 Select **Save**.

Set Up UCR 2008 in Enterprise Phone Configuration

Use this procedure to set the following UCR 2008 parameters:

- FIPS Mode
- 80-bit SRTCP

Procedure

Step 1 Choose **System** > **Enterprise Phone Configuration**.
Step 2 Set the FIPS Mode parameter to **Enabled**.
Step 3 Set the 80-bit SRTCP parameter to **Enabled**.
Step 4 Select **Save**.

Set Up UCR 2008 in Common Device Configuration

Use this procedure to set the following UCR 2008 parameters:

- IP Addressing Mode
- IP Addressing Mode Preference for Signaling

Procedure

Step 1 Choose **Device** > **Device Settings** > **Common Device Configuration**.
Step 2 Set the IP Addressing Mode parameter.
Step 3 Set the IP Addressing Mode Preference for Signaling parameter.
Step 4 Select **Save**.

Call Forward Notification Setup

You set up the information that the user sees from Cisco Unified Communications Manager Administration in the Device Configuration window (**Device** > **Phone**). The following table describes the Call Forward Notification fields.

Table 18: Call Forward Notification Fields

Field	Description
Caller Name	When this check box is checked, the caller name displays in the notification window. By default, this check box is checked.
Caller Number	When this check box is checked, the caller number displays in the notification window. By default, this check box is not checked.
Redirected Number	When this check box is checked, the information about the caller who last forwarded the call displays in the notification window. Example: If Caller A calls B, but B has forwarded all calls to C and C has forwarded all calls to D, the notification box that D sees contains the phone information for caller C. By default, this check box is not checked
Dialed Number	When this check box is checked, the information about the original recipient of the call displays in the notification window. Example: If Caller A calls B, but B has forwarded all calls to C and C has forwarded all calls to D, then the notification box that D sees contains the phone information for caller B. By default, this check box is checked.

Set Up SSH Access

The SSH Access is disabled by default.

If you set the same parameter in the Common Phone Profile window (**Device** > **Device Settings** > **Common Phone Profile**), the setting that takes precedence is determined in the following order:

1. Phone Configuration window settings
2. Common Phone Profile window settings

Procedure

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

Step 2 Select the appropriate phones.

Step 3 Scroll to the Product Specific Configuration Layout pane and select **Enable** from the SSH Access drop-down list box.

Calling Party Normalization

In line with E.164 standards, calling party normalization enhances the dialing capabilities of some phones and improves call back functionality when a call is routed to multiple geographical locations. That is, the feature ensures that the called party can return a call without having to modify the directory number in the call log directories on the phone. Additionally, calling party normalization allows the user to globalize and localize phone numbers, so the appropriate calling number presentation displays on the phone.

The SCCP and SIP phones support the following functions:

- For the final presentation of the calling number to the user, the phone screen displays the calling number based on the international, national, or local subscriber numbers.
    - If the call is an intracity call, the calling number presented on the phone is presented in the subscriber number format (without the area or city code).
    - For intercity calls, the calling number is presented in a national number format.
    - If the call is an international call, the calling number is presented with the E.164 format, with the plus (+) prefix digit.
- The call logs directories record the calling number in the received and missed call logs with the appropriate escape codes (9/0, 0/1, +). The user can go into directories, and select and dial one of these entries with the escape code without having to edit the number.

Configuring calling party normalization alleviates issues with toll bypass where the call is routed to multiple locations over the IP WAN. In addition, it allows Cisco Unified Communications Manager to distinguish the origin of the call to globalize or localize the calling party number for the phone user.

The phone itself can localize the calling party number. For the phone to localize the calling party number, you must configure the Calling Party Transformation CSS or the Use Device Pool Device Calling Party Transformation CSS setting in the Phone Configuration window.

For information on how to configure this feature for your phone, see “Calling Party Normalization” in the *Cisco Unified Communications Manager Features and Services Guide*.

Depending on your configuration for globalizing and localizing the calling party number, the phone user may see a localized number, a globalized number with access codes and prefixes, or the international escape character, +, in the calling party number. If a phone supports calling party normalization, the phone can show the localized calling party number on the phone screen and the globalized number in the call log directories on the phone.

In addition, these phones show both the globalized and localized calling party number in the Call Details. If a phone does not support calling party normalization, the phone shows the localized calling party on the phone screen and in the call log directories on the phone.

Incoming Call Toast Timer Setup

You can set the time that the Incoming Call Toast (incoming call notification window) displays on the user phone. You set up the feature from one of the following Cisco Unified Communications Manager windows:

- Enterprise Phone Configuration (**System** > **Enterprise Phone**)
- Common Phone Profile Configuration (**Device** > **Device Settings** > **Common Phone Profile**)

- Phone Configuration (**Device** > **Phone**)

The following table describes the Incoming Call Toast Timer.

Table 19: Incoming Call Toast Timer Field

Field	Description
Incoming Call Toast Timer	Gives the time, in seconds, that the toast displays. The time includes the fade-in and fade-out times for the window. The possible values are 3, 4, 5, 6, 7, 8, 9, 10, 15, 30, and 60. The default is 5.

Enable Line Status for Call Lists

To enable the Line Status for Call Lists, perform the following procedure:

Procedure

Step 1 Go to Cisco Unified CM Administration and choose System > Enterprise Parameters.
The Enterprise Parameters Configuration window appears.

Step 2 From the Line Status for Call Lists drop-down list box, choose the applicable profile.
The Disabled option is selected by default.

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 as well, 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

Set Minimum Ring Volume

The minimum ring volume is set to 0 (silent) for each phone by default.

Procedure

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

Step 2 Find a phone from the list of phones.

Step 3 Select **Minimum Ring Volume**.

Step 4 Choose a value between 0 and 14.

Step 5 Click **Save**.

CHAPTER 6

Cisco Unified IP Phone Customization

This chapter explains how you customize configuration files and phone ring sounds, and how to disable the phone screen to conserve power. Ring sounds play when the phone receives a call.

This chapter includes these topics:

Customization and Modification of Configuration Files

You can modify configuration files (for example, edit the xml files) and add customized files (for example, custom ring tones and, 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. For information on how to upload files to the TFTP folder on a Cisco Unified Communications Manager server, see *Cisco Unified Communications Operating System Administration Guide*.

You can obtain a copy of the Ringlist.xml and List.xml files from the system by using the following administration command line interface (CLI) *file* commands. For exact syntax, see *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

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*.

Ringlist.xml File Format Requirements

The Ringlist.xml file defines an XML object that contains a list of phone ring types. This file includes 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 appears 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 specifies the name of the custom ring for the associated PCM file that displays 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 in length.

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
- Mu-law compression
- Maximum ring size = 16080 samples
- Minimum ring size = 240 samples
- Number of samples in the ring = multiple of 240.
- Ring start and end at zero crossing.

To create PCM files for custom phone rings, use any standard audio editing package that supports these file format requirements.

Set Up Custom Phone Ring

To create custom phone rings for the Cisco Unified IP Phone, perform 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 PCM File Requirements for Custom Ring Types, on page 133.

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 a text editor to edit the Ringlist.xml file. See Ringlist.xml File Format Requirements, on page 132 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 reenable the “Enable Caching of Constant and Bin Files at Startup” TFTP service parameter (that is found in the Advanced Service Parameters area.)

Idle Display Setup

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 is idle (not in use) for a designated period and no feature menu is open.

For detailed instructions about creating and displaying the idle display, see *Creating Idle URL Graphics on Cisco Unified IP Phone* at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801c0764.shtml

In addition, see the *Cisco Unified Communications Manager Administration Guide* or the *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 in the Phone Configuration window in Cisco Unified Communications Manager Administration.
    - For multiple phones simultaneously: URL Idle field in the 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 in the Phone configuration window in Cisco Unified Communications Manager Administration.
    - For multiple phones simultaneously: URL Idle Time field in the 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.

Cisco Unified IP Phone Display Automatic Disable

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.

You can take any of these actions to turn on the display any time it is off:

- Press any button on the phone.

  The phone takes the action designated by that button in addition to turning on the display.
- Lift the handset.

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.

The following table 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 20: Backlight 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.
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.
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 a user (by pressing a button on the phone or lifting the handset). 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 a user turns the display on, enter **1:30**. The default value is 0:30.

EnergyWise on the Cisco Unified IP Phone Setup

To reduce power consumption, configure the phone to sleep (power down) and wake (power up) if your system includes an EnergyWise controller.

You configure settings in Cisco Unified Communications Manager Administration to enable EnergyWise and configure sleep and wake times. These parameters are closely tied to the phone display configuration parameters.

When EnergyWise is enabled and a sleep time is set, the phone sends a request to the switch to wake it up at the configured time. The switch returns either an acceptance or a rejection of the request. If the switch rejects the request or if the switch does not reply, the phone does not power down. If the switch accepts the request, the idle phone goes to sleep, thus reducing the power consumption to a predetermined level. A phone that is not idle sets an idle timer and goes to sleep after the timer expires.

To wake up the phone press **Select**. At the scheduled wake time, the system restores power to the phone, waking it up.

The following table explains the Cisco Unified Communications Manager Administration fields that control the EnergyWise settings. You configure these fields in Cisco Unified Communications Manager Administration in the Product Specific Configuration area of the Phone Configuration window **Device** > **Phone**.

Table 21: EnergyWise Configuration Fields

Field	Description
Enable Power Save Plus	Selects the schedule of days for which the phone powers off. Select multiple days by pressing and holding the Control key while clicking on the days for the schedule. By default, no days are selected. When Enable Power Save Plus is checked, you receive a message that warns about emergency (e911) concerns. **Caution** While Power Save Plus Mode (the "Mode") is in effect, endpoints that are configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: (i) You take full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect; (ii) Cisco has no liability in connection with your selection of the mode and all liability in connection with enabling the mode is your responsibility; and (iii) You fully inform users of the effects of the mode on calls, calling and otherwise. **Note** To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box. Leaving the Allow EnergyWise Overrides checked with no days selected in the Enable Power Save Plus field does not disable Power Save Plus.
Phone On Time	Determines when the phone automatically turns on for the days that are in the Enable Power Save Plus field. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power up the phone at 7:00 a.m. (0700), enter 7:00. To power up the phone at 2:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. **Note** The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 7:00, the Phone On Time must be no earlier than 7:20.

Field	Description
Phone Off Time	The time of day that the phone powers down for the days that are selected in the Enable Power Save Plus field. If the Phone On Time and the Phone Off Time fields contain the same value, the phone does not power down. Enter the time in this field in 24-hour format, where 00:00 is midnight. For example, to automatically power down the phone at 7:00 a.m. (0700), enter 7:00. To power down the phone at 2:00 p.m. (1400), enter 14:00. The default value is blank, which means 00:00. **Note** The Phone On Time must be at least 20 minutes later than the Phone Off Time. For example, if the Phone Off Time is 7:00, the Phone On Time must be no earlier than 7:20.
Phone Off Idle Timeout	The length of time that the phone must be idle before the phone powers down. The timeout occurs under the following conditions: • When the phone was in Power Save Plus mode, as scheduled, and was taken out of Power Save Plus mode because the phone user pressed the **Select** key. • When the phone is repowered by the attached switch. • When the Phone Off Time is reached but the phone is in use. The range of the field is 20 to 1440 minutes. The default value is 60 minutes.
Enable Audible Alert	When enabled, instructs the phone to play an audible alert starting 10 minutes before the time that the Phone Off Time field specifies. The audible alert uses the phone ringtone, which briefly plays at specific times during the 10-minute alerting period. The alerting ringtone plays at the user-designated volume level. The audible alert schedule is: • At 10 minutes before power down, play the ringtone four times. • At 7 minutes before power down, play the ringtone four times. • At 4 minutes before power down, play the ringtone four times. • At 30 seconds before power down, play the ringtone 15 times or until the phone powers off. This check box applies only if the Enable Power Save Plus list box has one or more days selected.
EnergyWise Domain	The EnergyWise domain that the phone is in. The maximum length of this field is 127 characters.
EnergyWise Secret	The security secret password that is used to communicate with the endpoints in the EnergyWise domain. The maximum length of this field is 127 characters.

Field	Description
Allow EnergyWise Overrides	This check box determines whether you allow the EnergyWise domain controller policy to send power level updates to the phones. The following conditions apply: **1** One or more days must be selected in the Enable Power Save Plus field. **2** The settings in Cisco Unified Communications Manager Administration take effect on schedule even if EnergyWise sends an override. For example, assuming the Phone Off Time is set to 22:00 (10:00 p.m.), the value in the Phone On Time field is 06:00 (6:00 a.m.), and the Enable Power Save Plus has one or more days selected. • If EnergyWise directs the phone to turn off at 20:00 (8:00 p.m.), that directive remains in effect (assuming no phone user intervention occurs) until the configured Phone On Time at 6:00 a.m. • At 6:00 a.m., the phone turns on and resumes receiving the power level changes from the settings in Unified Communications Manager Administration. • To change the power level on the phone again, EnergyWise must reissue a new power level change command. **Note** To disable Power Save Plus, you must uncheck the Allow EnergyWise Overrides check box checked. Leaving the Allow EnergyWise Overrides checked with no days selected in the Enable Power Save Plus field does not disable Power Save Plus.

CHAPTER 7

Cisco Unified IP Phone Model Information, Status, and Statistics

This chapter describes how to use the following menus on the Cisco Unified IP Phone 6921, 6941, 6945, and 6961 to view model information, status messages, and network statistics for the phone:

- Model Information screen: Displays hardware and software information about the phone.
- Status menu: Provides access to screens that display the status messages, network statistics, and statistics for the current call.

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 web page. For more information, see Remote Monitoring, on page 153.

For more information about troubleshooting the Cisco Unified IP Phone 6921, 6941, 6945, and 6961, see Troubleshooting and Maintenance, on page 169.

This chapter includes these topics:

Display Model Information Screen

To display the Model Information screen, perform the following steps:

Procedure

Step 1 Press **Applications** and then select **Phone Information**.
If the user is connected to a secure or authenticated server, a corresponding icon (lock or certificate) displays 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 appears.

The Model Information screen includes the options described in Model Information Settings Fields, on page 140.

Step 2 To exit the Model Information screen, press **Exit**.

Model Information Settings Fields

The Model Information screen includes the options described in the following table.

Table 22: Model Information Settings for the Cisco Unified IP Phone 6900 Series

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.
MAC Address	MAC address of the phone.	Display only—cannot configure.
Unified Video Advantage	Indicates if video call is enabled or disabled.	Display only—cannot configure.
Active Load	Version of firmware currently installed on the phone.	Display only—cannot configure.
Inactive Load	Version of firmware installed on the phone, but not currently running. The “Inactive Load” label also displays the status of the load, such as “Upgrade in Progress” or “Upgrade Failed.”	Display only—cannot configure.
Last Upgrade	Date of the most recent firmware upgrade.	Display only—cannot configure.
Active Server	IP address or name of the server to which the phone is registered.	Display only—cannot configure.
Stand-by Server	IP address or name of the standby server.	Display only—cannot configure.
Backlight On Time	Time of day the backlight is to automatically turn itself on for days listed in the off schedule.	Display only—cannot configure.
Backlight On Duration	Amount of time the backlight is to be active for when it is turned on by the programmed schedule.	Display only—cannot configure.

Option	Description	To Change
Backlight Idle Timeout	Time duration how long to wait before the backlight is turned off when it was turned on by user activity.	Display only—cannot configure.
Days Backlight Not Active	Days that the backlight is to remain off by default.	Display only—cannot configure.

Status Menu

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.
- Network Statistics—Displays the Network Statistics screen, which shows Ethernet traffic statistics.
- Call Statistics—Displays counters and statistics for the current call.

Display Status Menu

To display the Status menu, perform these steps:

Procedure

Step 1 To display the Status menu, press **Applications**.

Step 2 Select **Administrator Settings** > **Status**.

Step 3 To exit the Status menu, press **Exit**.

Status Messages Screen

The Status Messages screen displays the 10 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. Status Messages, on page 142 describes the status messages that might appear. This table also includes actions you can take to address errors.

Display Status Messages Screen

To display the Status Messages screen, perform these steps:

Procedure

Procedure

Step 1 Press **Applications**.
Step 2 Select **Admin Settings**.
Step 3 Select **Status**.
Step 4 Select **Status Messages**.
Step 5 To remove current status messages, press **Clear**.
Step 6 To exit the Status Messages screen, press **Back**.

Status Messages

The following table describes the status messages that display on the Status Messages screen.

Table 23: Status Messages on the Cisco Unified IP Phone 6900 Series

Message	Description	Possible Explanation and Action
CFG file not found	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 Cisco Unified Communications Manager Administration Phone Addition, on page 57 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 Network Setup Menu, on page 73 for details on assigning a TFTP server.
CFG TFTP Size Error	The configuration file is too large for file system on the phone.	Power cycle the phone.

Message	Description	Possible Explanation and Action
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.
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 Network Setup Menu, on page 73 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 Network Setup Menu, on page 73 section for details. • If you are using DHCP, check the DHCP server configuration.

Message	Description	Possible Explanation and Action
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
File not found	The phone cannot locate, on the TFTP server, the phone load file that is specified in the phone configuration file.	From Cisco Unified Operating System Administration, make sure that the phone load file is on the TFTP server, and that the entry in the configuration file is correct.
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 Network Setup Menu, on page 73 for details.
Load ID incorrect	Load ID of the software file is of the wrong type.	Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose **Device** > **Phone**). Verify that the load ID is entered correctly.
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 Network Setup Menu, on page 73 section for details. • If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.

Message	Description	Possible Explanation and Action
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 Network Setup Menu, on page 73 section for details. • If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.
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 Network Setup Menu, on page 73 for details on assigning a TFTP server.
TFTP file not found	The requested load file (.bin) was not found in the TFTPPath directory.	Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose **Device** > **Phone**). Verify that the TFTPPath directory contains a .bin file with this load ID as the name.
TFTP error	The phone does not recognize an error code provided by the TFTP server.	Contact the Cisco TAC.
TFTP server not authorized	The specified TFTP server could not be found in the phone's CTL.	• The DHCP server has the wrong configuration file for the TFTP server. In this case, update the TFTP server configuration to specify the correct TFTP server. The CTL file was made and then the TFTP server address changed. In this case, regenerate the CTL file. • If the phone is using a static IP address, the phone may be configured with the wrong TFTP server address. In this case, enter the correct TFTP server address in the Network Setup menu on the phone. • If the TFTP server address is correct, there may be a problem with the CTL file. In this case, run the CTL client and update the CTL file, making sure that the proper TFTP servers are included in this file.

Message	Description	Possible Explanation and Action
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.
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.

Network Statistics Screen

The Network Statistics screen displays information about the phone and network performance. Network Statistics Fields, on page 147 describes the information that appears in this screen.

Display Network Statistics Screen

To display the Network Statistics screen, perform these steps:

Procedure

Step 1 Press **Applications**.

Step 2 Select **Admin Settings**.

Step 3 Select **Status**.

Step 4 Select **Status** > **Network Statistics**. Network Statistics Fields, on page 147 describes the information that appears in this screen.

Step 5 To reset the Rx Frames, Tx Frames, and Rx Broadcasts statistics to 0, press **Clear**.

Step 6 To exit the Network Statistics screen, press **Back**.

Network Statistics Fields

The following table describes the information in the Network Statistics screen.

Table 24: Cisco Unified IP Phone 6900 Series Network Statistics Fields

Item	Description
Tx Frames	Number of packets sent by the phone
Tx Broadcasts	Number of broadcast packets sent by the phone
Tx Unicast	Total number of unicast packets transmitted by the phone
Rx Frames	Number of packets received by the phone
Rx Broadcasts	Number of broadcast packets received by the phone
Rx Unicast	Total number of unicast packets received by the phone
Neighbor Device ID: • Neighbor IP Address • Neighbor Port	Identifier of a device connected to this port discovered by CDP protocol.
Restart Cause: One of these values: • Hardware Reset (Power-on reset) • Software Reset (memory controller also reset) • Software Reset (memory controller not reset) • Watchdog Reset • Unknown	Cause of the last reset of the phone
Port 1	Link state and connection of the PC port (for example, Auto 100 Mb Full-Duplex means that the PC port is in a link-up state and has auto-negotiated a full-duplex, 100-Mbps connection)
Port 2	Link state and connection of the Network port

Item	Description
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

Display Call Statistics Screen

You can access the Call Statistics screen 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 Remote Monitoring, on page 153

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, perform these steps:

Procedure

Step 1 Press **Applications**.

Step 2 Select **Admin Settings**.

Step 3 Select **Status**.

Step 4 Select **Call Statistics**. The fields in the window are described in Call Statistics Fields, on page 149.

Step 5 To exit the Call statistics screen, press **Exit**.

Call Statistics Fields

The Call Statistics screen displays these items:

Table 25: Call Statistics Items for the Cisco Unified Phone 6900 Series

Item	Description
Rcvr Codec	Type of voice stream received (RTP streaming audio from codec): G.729, G.711 u-law, G.711 A-law, G.722 (only on 6945 phone).
Sender Codec	Type of voice stream transmitted (RTP streaming audio from codec): G.729, G.711 u-law, G.711 A-law, G.722 (only on 6945 phone).
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.
Avg Jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network) observed since the receiving voice stream was opened.
Max Jitter	Maximum jitter 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.

Item	Description
Rcvr Lost Packets	Missing RTP packets (lost in transit).
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 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).
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.
MOS LQK	Objective estimate of the Mean Opinion Score (MOS) for Listening Quality (LQK) that ranks audio quality from 5 (excellent) to 1 (bad). This score is based on audible-concealment events due to a frame loss in the preceding 8 seconds of the voice stream. **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 for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score from the start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score from the start of the voice stream. The following codecs provide the corresponding maximum MOS LQK scores under normal conditions with no frame loss: • G.711: 4.5 • G.722: 4.5 • G.728/iLBC: 3.9 • G729A/AB: 3.7
MOS LQK Version	Version of the Cisco-proprietary algorithm used to calculate the MOS LQK scores.

Display Security Configuration

You can view information about the security on the phone. For more information, refer Cisco Unified IP Phone Security, on page 69.

To display the Security Configuration screen, follow these steps.

Procedure

Step 1 Press **Applications**.

Step 2 Select **Admin Settings**.

Step 3 Select **Security**. For information on the fields displayed, see Security Configuration Fields, on page 151.

Step 4 To exit, press **Exit**.

Security Configuration Fields

The Security Configuration screen displays these items.

Table 26: Security Configuration Items for the Cisco Unified Phone 6900 Series

Item	Description
Security Mode	Displays the security mode that is set for the phone.
LSC	Indicates whether a locally significant certificate (used for the security features) is installed on the phone or is not installed on the phone.
Trust List	The Trust List is a top-level menu that provides submenus for the CTL Signature and Call manager/TFTP Server.
802.1x Authentication	Allows you to enable 802.1X authentication for the phone.

CHAPTER 8

Remote Monitoring

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 Cisco Unified IP Phone Model Information, Status, and Statistics, on page 139

For more information about troubleshooting the Cisco Unified IP Phone, Troubleshooting and Maintenance, on page 169

This chapter includes these topics:

Access Web Page for Phone

To access the web page for a Cisco Unified IP Phone, perform these steps.

If you cannot access the web page, it may be disabled. See Control web page access, on page 155 for more information.

Procedure

Step 1 Obtain the IP address of the Cisco Unified IP Phone using one of these methods:

a) Search for the phone in Cisco Unified Communications Manager 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.
b) On the Cisco Unified IP Phone, press **Applications**, choose **Administrator Settings** > **Network 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

Cisco Unified IP Phone Web Page Information

The web page for a Cisco Unified IP Phone includes these topics:

- **Device Information**: Displays device settings and related information for the phone.
- **Network Setup**: Displays network setup information and information about other phone settings.
- **Network Statistics**: Includes the following hyperlinks, which provide information about network traffic:
    - **Ethernet Information**: Displays information about Ethernet traffic.
    - **Network (Port)**: Displays information about network traffic to and from the network port on the phone.
    - **Debug Display**: Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting.
- **Device Logs**: Includes the following hyperlinks, which provide information that you can use for troubleshooting:
    - **Console Logs**: Includes hyperlinks to individual log files.
    - **Core Dumps**: Includes hyperlinks to individual dump files.
    - **Status Messages**: Displays up to the 10 most recent status messages that the phone has generated since it was last powered up.
    - **Debug Display**: Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting.

- **Streaming Statistics**: Includes the following hyperlink:
    - **Stream 1**: Displays a variety of streaming statistics.

Related Topics

Device Information Area, on page 155
Network Setup, on page 157
Network Statistics, on page 162
Device Logs, on page 164
Streaming Statistics, on page 165

Control web page access

For security purposes, access to the web pages for a phone is disabled by default. This practice prevents access to the web pages that are described in this chapter and to the Cisco Unified Communications Manager User Options web pages.

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 enable or disable access to the web pages for a phone, perform these steps from Cisco Unified Communications Manager Administration:

Procedure

Step 1 Choose **Device** > **Phone**.
Step 2 Specify the criteria to find the phone and select **Find**, or select **Find** to display a list of all phones.
Step 3 Select the device name to open the Phone Configuration window for the device.
Step 4 Scroll to the Product Specific Configuration area.
Step 5 To enable access, from the Web Access drop-down list, choose **Enabled**.
Step 6 To disable access, from the Web Access drop-down list, choose **Disabled**.
Step 7 Select **Apply Config**.

Device Information Area

The Device Information area on a phone web page displays device settings and related information for the phone. The following table describes these items.

To display the Device Information area, access the web page for the phone as described in the Access Web Page for Phone, on page 154, and then click the **Device Information** hyperlink.

Table 27: 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
App Load ID	Identifier of the firmware running on the phone
Boot Load ID	Identifier of the factory-installed load running on the phone
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 • Version Identifier: Represents the hardware version of the phone • Serial Number: Displays the unique serial number of the phone.
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
FIPS Mode Enabled	Indicates whether the FIPS Mode parameter is enabled.

Network Setup

The Network Setup on a phone web page displays network setup information and information about other phone settings. The following table describes these items.

You can view and set many of these items from the Network Setup Menu and the Phone Information Menu on the Cisco Unified IP Phone. For more information, see Cisco Unified IP Phone Settings, on page 71.

To display the Network Setup area, access the web page for the phone as described in the Access Web Page for Phone, on page 154, and then click the **Network Setup** hyperlink.

Table 28: Network Setup Area Items

Item	Description
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address.
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	Default router used by the phone.
DNS Server	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) 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.

Item	Description
Unified CM 1 to 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 Network Setup 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.

Item	Description
Proxy Server URL	URL of proxy server, which makes HTTP requests to nonlocal host addresses on behalf of the phone HTTP client and provides responses from the nonlocal host to the phone HTTP client.
Authentication URL	URL that the phone uses to validate requests made to the phone web server.
Automatic Port Synchronization	Indicates if the phone is enabled to synchronize the PC and SW ports to the same speed and to duplex mode.
SW Port Remote Configuration	Indicates if remote port configuration of the speed and duplex mode for the switch port is enabled or disabled.
PC Port Remote Configuration	Indicates if remote port configuration of the speed and duplex mode for the PC port is enabled or disabled.
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 (Supported only for Cisco Unified IP Phone 6945.) • No Link: No connection to the switch port
PC Port Setup	Speed and duplex of the PC 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 (Supported only for Cisco Unified IP Phone 6945.) • No Link: No connection to the PC port
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.

Item	Description
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 PC.
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.
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.
LLDP-MED: Switch Port	Indicates whether Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is enabled on the switch port.

Item	Description
LLDP Power Priority	Advertises the phone 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.
CDP: PC Port	Indicates whether CDP is supported on the PC port (default is enabled). Enable CDP on the PC port when Cisco VT Advantage/Unified Video Advantage (CVTA) is connected to the PC port. CVTA does not work without CDP interaction with the phone. 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: 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.
SSH Access Enabled	Indicates whether the phone accepts or blocks the SSH connections.
EnergyWise Level	Indicates the EnergyWise Level.
EnergyWise Domain	The EnergyWise domain that the phone is in.
FIPS Mode Enabled	Indicates whether the FIPS Mode parameter is enabled.
IP Addressing Mode	Displays the IP addressing mode that is available on the phone.
IP Preference Mode Control	Indicates the IP address version that the phone uses during signaling with Cisco Unified Communications Manager when both IPv4 and IPv6 are both available on the phone.
IPv6 Auto Configuration	Displays whether the autoconfiguration is enabled or disabled on the phone.

Item	Description
IPv6 CAPF Server	Common Name (from the Cisco Unified Communications Manager Certificate) of the CAPF used by the phone.
DHCPv6	Dynamic Host Configuration Protocol (DHCP) automatically assigns IPv6 address to devices when you connect them to the network. Cisco Unified IP Phones enable DHCP by default.
IPv6 Address Released	The phone has been configured to release its IPv6 address.
IPv6 Default Router 1	Default router used by the phone (Default Router 1).
IPv6 Address	IPv6 address of the phone. The IPv6 address is a 128 bit address.
IPv6 Prefix Length	Subnet prefix length that is used by the phone. The subnet prefix length is a decimal value from 1 to 128, that specifies the portion of the IPv6 address that comprises the subnet.
IPv6 DNS Server 1	Primary Domain Name System (DNS) server (DNS Server 1) used by the phone.
IPv6 Alternate TFTP	Indicates whether the phone is using the IPv6 Alternate TFTP server.
IPv6 TFTP Server 1	Primary IPv6 Trivial File Transfer Protocol (TFTP) server used by the phone.
IPv6 TFTP Server 2	Optional backup IPv6 TFTP server that the phone uses if the primary IPv6 TFTP server is unavailable.

Network Statistics

The following Network Statistics hyperlinks on a phone 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 Access Web Page for Phone, on page 154.

- Ethernet Information: Displays information about Ethernet traffic.
- Network: Displays information about network traffic to and from the network port (10/100 SW) on the phone.

Ethernet Information

The following table describes the fields in the Ethernet screen.

Table 29: 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 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 unicast	Total number of unicast packets received by the phone

Access Area and Network Information

The following table describes the fields in the Access Area and Network screens.

Table 30: Access Area and Network Items

Item	Description
Tx Frames	Number of packets transmitted by the phone
Tx broadcast	Number of broadcast packets transmitted by the phone
Tx Unicast	Number of unicast packets transmitted by the phone
Rx Frames	Number of packets received by the phone
Rx broadcast	Number of broadcast packets received by the phone
Rx unicast	Number of unicast packets received by the phone
LLDP FramesOutTotal	Number of LLDP frames sent out from the phone
LLDP AgeoutsTotal	Number of LLDP frames that have been time out in cache
LLDP FramesDiscardedTotal	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	Number of LLDP frames that received with one or more detectable errors.
LLDP FramesInTotal	Number of LLDP frames received on the phone.
LLDP TLVDiscardedTotal	Number of LLDP TLVs that are discarded.

Item	Description
LLDP TLVUnrecognizedTotal	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.
Restart Cause	Cause of the last reset of the phone. • Hardware Reset (Power-on reset) • Software Reset (memory controller also reset) • Software Reset (memory controller not reset) • Watchdog Reset • Unknown
Port Information	Speed and duplex information.
IPv4	Information on the DHCP status.

Device Logs

The following device logs hyperlinks on a phone 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 Access Web Page for Phone, on page 154.

- 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. Status Messages, on page 142 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.

- Restart Cause: Displays the cause for the restart.

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 call or running a service that sends or receives audio or data.

The streaming statistics areas on a phone web page provide information about the streams. Cisco Unified IP Phones 6900 Series use only Stream 1.

To display a Streaming Statistics area, access the web page for the phone as described in the Access Web Page for Phone, on page 154, and then select the **Stream 1** hyperlink.

The following table describes the items in the Streaming Statistics areas.

Table 31: 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 (see note)	Number of times the RTCP Sender Report have been sent.
Sender Report Time Sent (see note)	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.

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 (see note)	Number of times the RTCP Receiver Reports have been sent.
Rcvr Report Time Sent (see note)	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 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 5 percent concealment events (lost frames) from the start of the voice stream.
Latency (see note)	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 (see note)	Number of times RTCP Sender Reports have been received.

Item	Description
Sender Report Time Received (see note)	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 (see note)	Number of times RTCP Receiver Reports have been received.
Rcvr Report Time Received (see note)	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 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).
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.
MOS LQK	Objective estimate of the Mean Opinion Score (MOS) for Listening Quality (LQK) that ranks audio quality from 5 (excellent) to 1 (bad). This score is based on audible-concealment events due to a frame loss in the preceding 8 seconds of the voice stream. **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 for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score from the start of the voice stream.

Item	Description
Max MOS LQK	Baseline or highest MOS LQK score from the start of the voice stream. The following codecs provide the corresponding maximum MOS LQK scores under normal conditions with no frame loss: • G.711: 4.5 • G.722: 4.5 • G.728/iLBC: 3.9 • G729A/AB: 3.7
MOS LQK Version	Version of the Cisco-proprietary algorithm used to calculate the MOS LQK scores.

Note When the RTP Control Protocol is disabled, no data generates for this field and thus displays as 0.

Related Topics

Cisco Unified IP Phone Settings, on page 71

CHAPTER 9

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 Documentation, support, and security guidelines, on page xv.

Troubleshooting

Use the following sections to troubleshoot problems with the phones.

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 Phone Startup Verification, on page 68. If the phone does not start up properly, see the following sections for troubleshooting information:

Cisco Unified IP Phone Does Not Go Through 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 Phone Startup Verification, on page 68 and the LCD 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:

- 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.

- 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.

- 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.
- If the phone still does not start up properly, perform a factory reset of the phone. For instructions, see the Factory Reset, on page 188.

If after attempting these solutions, the LCD 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.

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 LCD 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.

Related Topics

Cisco Unified IP Phone Security Problems, on page 175

Phone Displays Error Messages

Problem

Phone status messages display errors during startup.

Solution

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, on page 141 for instructions about accessing status messages and for a list of potential errors, their explanations, and their solutions.

Phone Cannot Connect to TFTP Server or to Cisco Unified Communications Manager

Problem

If the network is down between the phone and either the TFTP server or Cisco Unified Communications Manager, the phone cannot start up properly.

Solution

Ensure that the network is currently running.

TFTP Server Settings

Problem

The TFTP server settings may not be correct.

Solution

Check the TFTP settings. See Check TFTP Settings, on page 180.

IP Addressing and Routing

Problem

The IP addressing and routing fields may not be correctly configured.

Solution

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. See Check DHCP Settings, on page 181.

DNS settings

Problem

The DNS settings may be incorrect.

Solution

If you use DNS to access the TFTP server or Cisco Unified Communications Manager, you must ensure that you specify a DNS server. Check your DNS settings.

Cisco CallManager and TFTP Services Are Not Running

Problem

If the Cisco CallManager or TFTP services are not running, phones may not be able to start up properly. In such a situation, it is likely that you are experiencing a systemwide failure, and other phones and devices are unable to start up properly.

Solution

If the Cisco CallManager service is not running, all devices on the network that rely on it to make phone calls are affected. If the TFTP service is not running, many devices cannot start up successfully. For more information, see Start Service, on page 183.

Configuration file corruption

Problem

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.

Solution

Create a new phone configuration file. See Create New Phone Configuration File, on page 181

Cisco Unified Communications Manager Phone Registration

Problem

The phone is not registered with the Cisco Unified Communications Manager.

Solution

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 and if there are sufficient number of unit licenses. Review Cisco Unified Communications Manager Phone Addition Methods, on page 55 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 the MAC Address. For information about determining a MAC address, see Cisco Unified IP Phone MAC Address Determination, on page 59.

If the phone is already in the Cisco Unified Communications Manager database, its configuration file may be damaged. See Configuration file corruption, on page 172 for assistance

For more information on licensing go to the “Licenses for Phones” section in the *Cisco Unified Communications Manager System Guide*.

Cisco Unified IP Phone Cannot Obtain IP Address

Problem

If a phone cannot obtain an IP address when it starts up, the phone may not be on the same network or VLAN as the DHCP server, or the switch port to which the phone connects may be disabled.

Solution

Ensure that the network or VLAN to which the phone connects has access to the DHCP server, and ensure 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.

Physical Connection Problems

Problem

The physical connection to the LAN may be broken.

Solution

Verify that the Ethernet connection to which the Cisco Unified IP Phone connects is up. For example, check whether the particular port or switch to which the phone connects is down and that the switch is not rebooting. Also ensure that no cable breaks exist.

Intermittent network outages

Problem

Your network may be experiencing intermittent outages.

Solution

Intermittent network outages affect data and voice traffic differently. Your network might be 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 to the network. Contact the system administrator for information on known problems in the voice network.

DHCP Setting Errors

Problem

The DHCP settings may be incorrect.

Solution

Verify that you have properly configured the phone to use DHCP. See Network Setup Menu, on page 73 for more information. Verify that the DHCP server has been set up properly. Verify the DHCP lease duration. Cisco recommends that you set it to 8 days.

Static IP Address Settings Errors

Problem

The static IP address assigned to the phone may be incorrect.

Solution

If the phone has been assigned a static IP address, verify that you have entered the correct settings. See Network Setup Menu, on page 73 for more information.

Voice VLAN Setup Errors

Problem

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.

Solution

Isolating the phones on a separate auxiliary VLAN increases the quality of the voice traffic. See Cisco Unified IP Phone and VLAN Interaction, on page 48 for more information.

DNS or Other Connectivity Errors

Problem

The phone reset continues and you suspect DNS or other connectivity issues.

Solution

If the phone continues to reset, eliminate DNS or other connectivity errors with Determine DNS or Connectivity Issues, on page 182.

Phones Have Not Been Intentionally Reset

Problem

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.

Solution

You can check if a Cisco Unified IP Phone received a command from Cisco Unified Communications Manager to reset by pressing **Applications** on the phone and choosing **Administrator Settings** > **Status** > **Network Statistics**.

- If the Restart Cause field displays `Reset-Reset`, the phone receives a Reset/Reset from Cisco Unified Communications Manager Administration.
- If the Restart Cause field displays `Reset-Restart`, the phone closed because it received a Reset/Restart from Cisco Unified Communications Manager Administration.

Power Connection Problems

Problem

The phone does not appear to be powered up.

Solution

In most cases, a phone restarts 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 connects to an external power supply.

Cisco Unified IP Phone Security Problems

The following sections 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 and encryption, refer to *Cisco Unified Communications Manager Security Guide*.

CTL File Problems

The following sections describe problems with the CTL file.

Authentication Error, Phone Cannot Authenticate CTL File

Problem

A device authentication error occurs.

Cause

CTL file does not have a Cisco Unified Communications Manager certificate or has an incorrect certificate.

Solution

Install a correct certificate.

Phone Cannot Authenticate CTL File

Problem

Phone cannot authenticate the CTL file.

Cause

The security token that signed the updated CTL file does not exist in the CTL file on the phone.

Solution

Change the security token in the CTL file and install the new file on the phone.

CTL File Authenticates but Other Configuration Files Do Not Authenticate

Problem

Phone cannot authenticate any configuration files other than the CTL file.

Cause

A bad TFTP record exists, or the configuration file may not be signed by the corresponding certificate in the phone Trust List.

Solution

Check the TFTP record and the certificate in the Trust List.

TFTP Authorization Fails

Problem

Phone reports TFTP authorization failure.

Cause

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.

Solution

Check the configuration of the TFTP address in the phone CTL file.

Signed Configuration Files Are Not Requested

Problem

Phone does not request signed configuration files.

Cause

The CTL file does not contain any TFTP entries with certificates.

Solution

Configure TFTP entries with certificates in the CTL file.

802.1X Authentication Problems

802.1X authentication problems can be broken down into the categories described in the following table.

Table 32: Identifying 802.1X Authentication Problems

Is all the following conditions apply,	See
• Phone cannot obtain a DHCP-assigned IP address • Phone does not register with Cisco Unified Communications Manager • Phone status display as "Configuring IP" or "Registering" • 802.1X Authentication Status displays as "Held" • Status menu displays 802.1x status as "Failed"	802.1X is Enabled on Phone but Phone Does Not Authenticate, on page 177
• Phone cannot obtain a DHCP-assigned IP address • 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	802.1X is Not Enabled, on page 178
• Phone cannot obtain a DHCP-assigned IP address • Phone does not register with Cisco Unified Communications Manager • Phone status display as "Configuring IP" or "Registering" • Cannot access phone menus to verify 802.1X status	Factory Reset of the Phone Has Deleted 802.1X Shared Secret, on page 178

802.1X is Enabled on Phone but Phone Does Not Authenticate

Problem

The phone cannot authenticate.

Cause

These errors typically indicate that 802.1X authentication is enabled on the phone, but the phone is unable to authenticate.

Solution

To resolve this problem, you need to check the 802.1X and shared secret configuration. See Identify 802.1X Authentication Problems, on page 183.

802.1X is Not Enabled

Problem

The phone does not have 802.1X configured.

Cause

These errors typically indicate that 802.1X authentication is not enabled on the phone.

Solution

These errors typically indicate that 802.1X is not enabled on the phone. To enable it, see the Security Setup menu, on page 84 for information on enabling 802.1X on the phone.

Factory Reset of the Phone Has Deleted 802.1X Shared Secret

Problem

After a reset, the phone does not authenticate.

Cause

These errors typically indicate that the phone has completed a factory reset while 802.1X was enabled. A factory reset deletes the shared secret, which is required for 802.1X authentication and network access.

Solution

To resolve this, you have two options:

- Temporarily disable 802.1X on the switch.
- Temporarily move the phone to a network environment that is not using 802.1X authentication.

After the phone starts up normally in one of these conditions, you can access the 802.1X configuration menus and re-enter the shared secret.

Audio and Video Problems

The following sections describe how to resolve audio and video problems.

Phone Display is Wavy

Problem

The display appears to have rolling lines or a wavy pattern.

Cause

The phone might be interacting with certain types of older fluorescent lights in the building.

Solution

Move the phone away from the lights or replace the lights to resolve the problem.

No Speech Path

Problem

One or more people on a call do not hear any audio.

Solution

When at least one person in a call does not receive audio, IP connectivity between phones is not established. Check the configuration of routers and switches to ensure that IP connectivity is properly configured.

Choppy Speech

Problem

A user complains of choppy speech on a call

Cause

There may be a mismatch in the jitter configuration

Solution

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 Display Call Statistics Screen, on page 148 for information about displaying these statistics.

General Telephone Call Problems

The following sections help troubleshoot general telephone call problem.

Phone Call Cannot Be Established

Problem

A user complains about not being able to make a call.

Cause

The phone does not have a DHCP IP address, is unable to register to Cisco Unified Communications Manager. Phones with an LCD display show the message `Configuring IP` or `Registering`. Phones without an LCD display play the reorder tone (instead of dial tone) in the handset when the user attempts to make a call.

Solution

1. Verify the following:
    a. The Ethernet cable is attached.
    b. The Cisco CallManager service is running on the Cisco Unified Communications Manager server.
    c. Both phones are registered to the same Cisco Unified Communications Manager.
2. Audio server debug and capture logs are enabled for both phones. If needed, enable Java debug.

Phone Does Not Recognize DTMF Digits or Digits Are Delayed

Problem

The user complains that numbers are missed or delayed when the keypad is used.

Cause

Pressing the keys too quickly can result in missed or delayed digits.

Solution

Keys should not be pressed rapidly.

Troubleshooting Procedures

These procedures can be used to identify and correct problems.

Check TFTP Settings

Procedure

Step 1 You can determine the IP address of the TFTP server used by the phone by pressing **Applications**, then selecting **Administrator Settings** > **Network Setup** > **IPv4** > **TFTP Server 1**.

Step 2 If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option.

Step 3 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.

Step 4 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 Network Setup Menu, on page 73 for more information.

Check DHCP Settings

Procedure

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

Step 2 Select **Administrator Settings** > **Network Setup** > **IPv4**, and look at the following options:

- Boot/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/ps708/prod_tech_notes_list.html

- 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 Network Setup Menu, on page 73 for instructions.

Step 3 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

Verify DNS Settings

Procedure

Step 1 Press **Applications**.

Step 2 Select **Administrator Settings** > **Network Setup** > **IPv4** > **DNS Server 1**.

Step 3 Verify that there is a CNAME entry in the DNS server for the TFTP server and for the Cisco Unified Communications Manager system.

Step 4 Verify that DNS is configured to do reverse look-ups.

Create New Phone 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.

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 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. For more information, see the *Cisco Unified Communications Manager Administration Guide*.
- 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.

To create a new configuration file, perform 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 Cisco Unified Communications Manager Phone Addition Methods, on page 55 for details.

Step 4 Power cycle the phone.

Determine DNS or Connectivity Issues

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 Cisco Unified IP Phone Reset or Restore, on page 187 for details.

Step 2 Modify DHCP and IP settings:

a) Disable DHCP. See the Network Setup Menu, on page 73 for instructions.
b) Assign static IP values to the phone. See the Network Setup Menu, on page 73 for instructions. Use the same default router setting used for other functioning Cisco Unified IP Phones.

c) Assign a TFTP server. See the Network Setup Menu, on page 73 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 Cisco Unified IP Phone MAC Address Determination, on page 59.

Step 6 Power cycle the phone.

Identify 802.1X Authentication Problems

Procedure

Step 1 Verify that you have properly configured the required components 802.1X Authentication, on page 39.

Step 2 Confirm that the shared secret is configured on the phone (see the Security Setup menu, on page 84 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.

Start Service

Note A service must be activated before it can be started or stopped. To activate a service, choose **Tools** > **Service Activation**.

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 the corresponding radio button and then click **Start**.
The Service Status symbol changes from a square to an arrow.

Troubleshoot Using Debug Menu

On the phone, the **Admin Settings** > **Debug Phone** menu enables you to troubleshoot phone problems.

Note When the debug level is set to Debug, the phone may experience degradation of service due to the amount of information that is collected. Use this level for the least amount of time necessary.

To debug a phone, you connect a computer to the PC port of the phone and start the debugging program. The computer requires a debugging program to be already installed. After changing the debug setting, the phone sends debug information to the debugging program on the computer.

For more information about debugging programs, contact Cisco TAC.

You can also connect to the phone using SSH (if enabled) to view the debug information. Limited debug information is available through the Phone web page, with the amount of information limited by the amount of available flash memory in the phone.

The debug setting persists when the phone restarts, resets, or power cycles. The debug settings reset when the phone is restored to the Factory Defaults, or when **Reset Settings** > **All** is selected.

Before You Begin

- Computer with a phone debugging program installed.
- Cisco Unified Communications Manager must have the Settings Access parameter set to Enabled (default).
- Cisco Unified Communications Manager must have the Display Logging parameter set to PC Controlled (default) or Enabled.
    - PC Controlled means that the phone sends logs only when the debugging program is active on the computer and the computer is plugged into the PC port of the phone.
    - Enabled means that the logs are always sent to the PC port.

Procedure

Step 1 Access the debug information using one of the following methods:

- Connect a computer to the PC port of the phone that is experiencing problems. Launch the debugging program
- Connect to the phone using SSH (when enabled) to view the debug information.

- Check the phone web page. Note that the amount of information in the web page is limited by the amount of available flash memory on the phone.

Step 2 On the phone that is experiencing problems, choose **Admin Settings** > **Debug Phone**.

Step 3 Choose one of the following entries:

- **MMI** to troubleshoot user interface problems
- **Network** to troubleshoot network problems
- **CallControl** to troubleshoot problems with phone calls
- **Signaling** to troubleshoot communication problems
- **Security** to troubleshoot security problems

Step 4 Choose one of the following debug levels:

- **Errors** to only log error messages. This setting is the phone default.
- **Warnings** to log error messages and warning messages.
- **Details** to log error and warning messages, as well as other details to assist troubleshooting.
- **Debug** to create a large amount of information, including error and warning messages.

Step 5 Recreate the problem on the phone.

Step 6 After you recreate the phone problem, navigate to **Admin Settings** > **Debug Phone** and set the debug level to **Errors**.

Step 7 Use the captured debug information in the computer to diagnose the problem. For information on using the captured information, see the debugging program documentation.

General Troubleshooting Information

The following table provides general troubleshooting information for the Cisco Unified IP Phone.

Table 33: 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 when calling digital cell phones using the G.729 protocol.	In Cisco Unified Communications Manager, you can configure the network to use the G.729 protocol (the default is G.711). When using G.729, calls between an IP phone and a digital cellular phone will have poor voice quality. Use G.729 only when absolutely necessary.

Summary	Explanation
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.
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 setup options are locked to prevent users from making changes that could impact their network connectivity. You must unlock the network setup options before you can configure them. See the Password Protection, on page 73 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.
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 Display Call Statistics Screen, on page 148 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 Display Call Statistics Screen, on page 148 for information about displaying these statistics.

Summary	Explanation
Loopback condition.	A loopback condition can occur when the following conditions are met: • The SW Port Configuration option in the Network Setup 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.

Additional Troubleshooting Information

If you have additional questions about troubleshooting the Cisco Unified IP Phones, several Cisco.com web sites can provide you with more tips. Choose from the sites available for your access level.

- Cisco Unified IP Phone Troubleshooting Resources:

  http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_troubleshoot_and_alerts.html

- Cisco Products and Services (Technical Support and Documentation):

  http://www.cisco.com/en/US/products/ps10326/tsd_products_support_series_home.html

Maintenance

The following sections describe voice and phone maintenance.

Cisco Unified IP Phone Reset or Restore

There are two general methods for resetting or restoring the Cisco Unified IP Phone.

The debug settings (set in **Admin Settings** > **Debug Phone**) persist when the phone restarts, resets, or power cycles. The debug settings reset when the phone is restored to the Factory Defaults, or when **Reset Settings** > **All** is selected.

Basic Reset

Performing a basic 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.

The following table describes the ways to perform a basic reset. 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 34: Basic Reset Methods

Operation	Performing	Explanation
Restart phone	Press **Services, Applications, or Directories** and then press **#**.	Resets any user and network setup changes that you have made, but that the phone has not written to its Flash memory, to previously saved settings, then restarts the phone.
Reset Settings	To reset settings, press **Applications** and choose **Admin Settings** > **Reset Settings** > **Network**.	Resets user and network setup settings to their default values, and restarts the phone.
	To reset the CTL file, press **Applications** and choose **Admin Settings** > **Reset Settings** > **Security**.	Resets the CTL file.

Factory Reset

When you perform a factory reset of the Cisco Unified IP Phone, the following information is erased or reset to its default value:

- User configuration settings: Reset to default values
- Network setup settings: Reset to default values
- Call histories: Erased
- Locale information: Reset to default values

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.

Perform Factory Reset from Phone Reset Settings Menu

To perform a factory reset of a phone,

Procedure

Step 1 Press **Applications**.

Step 2 Choose **Admin Settings** > **Reset Settings** > **All**.

Perform Factory Reset from Phone Keypad

Use these steps to reset the phone to factory default settings using the phone keypad.

Procedure

Step 1 While powering up the phone, press and hold #.

Step 2 When the light on the Mute button and handset light strip turns off and all other lights (Line button, Headset button, Speakerphone button and Select button) stay green, press **123456789*0#** in sequence.
When you press **1**, the lights on the line buttons turn red. The light on the Select button flashes when a button is pressed.

If you press the buttons out of sequence, the lights on the line button, headset button, speakerphone button, and Select button turn green. You need to start over and press **123456789*0#** in sequence again.

After you press these buttons, the phone goes through the factory reset process.

Caution Do not power down the phone until it completes the factory reset process, and the main screen appears.

Voice Quality Monitoring

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.
- Mean Opinion Score (MOS) for Listening Quality (LQK) Voice Metrics: Uses a numeric score to estimate the relative voice-listening quality. The Cisco Unified IP Phones calculate the MOS LQK based audible-concealment events due to a frame loss in the preceding 8 seconds and includes weighting factors such as codec type and frame size.

  MOS LQK scores are produced by a Cisco-proprietary algorithm, the Cisco Voice Transmission Quality (CVTQ) index. Depending on the MOS LQK version number, these scores may comply with the International Telecommunications Union (ITU) standard P.564. This standard defines evaluation methods and performance accuracy targets that predict listening quality scores based on observation of actual network impairment.

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 using the Call Statistics screen or remotely by using Streaming Statistics.

Related Topics

Display Call Statistics Screen, on page 148
Remote Monitoring, on page 153

Voice Quality Metrics

When using the metrics for monitoring voice quality, note the typical scores under normal conditions of zero packet loss and use the metrics as a baseline for comparison.

It is also important to distinguish significant changes from random changes in metrics. Significant changes are scores that change about 0.2 MOS or more and persist in calls that last longer than 30 seconds. Conceal ratio changes indicate a frame loss greater than 3 percent.

The MOS LQK scores can vary based on the codec that the Cisco Unified IP Phone uses. The following codecs provide these corresponding maximum MOS LQK scores under normal conditions with zero frame loss for Cisco Unified Phones 6901 and 6911:

- G.711: 4.5 MOS LQK
- G.722: 4.5 MOS LQK
- G.728/iLBC: 3.9 MOS LQK
- G729A/AB: 3.7 MOS LQK

Cisco Voice Transmission Quality (CVTQ) does not support wideband (7 kHz) speech codecs, because ITU has not defined the extension of the technique to wideband. Therefore, MOS LQK scores that correspond to G.711 performance are reported for G.722 calls to allow basic quality monitoring, rather than not reporting an MOS score.

- Reporting G.711-scale MOS scores for wideband calls through the use of CVTQ allows basic-quality classifications to be indicated as good/normal or bad/abnormal. Calls with high scores (approximately 4.5) indicate high quality or a low packet loss, and lower scores (approximately 3.5) indicate low quality or a high packet loss.
- Unlike MOS, the conceal ratio and concealed seconds metrics remain valid and useful for both wideband and narrowband calls.

A conceal ratio of zero indicates that the IP network is delivering frames and packets on time with no loss.

Voice Quality Troubleshooting Tips

When you observe significant and persistent changes to metrics, use the following table for general troubleshooting information.

Table 35: Changes to Voice Quality Metrics

Metric change	Condition
Conceal Ratio and Conceal Seconds increase significantly	Network impairment from packet loss or high jitter.

Metric change	Condition
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.
MOS LQK scores decrease significantly	Network impairment from packet loss or high jitter levels: • Average MOS LQK decreases may indicate widespread and uniform impairment. • Individual MOS LQK decreases may indicate bursty impairment. Cross-check the conceal ratio and conceal seconds for evidence of packet loss and jitter.
MOS LQK scores increase significantly	• Check to see if the phone is using a different codec than expected (RxType and TxType). • Check to see if the MOS LQK version changed after a firmware upgrade.

Note Voice quality metrics do not account for noise or distortion, only frame loss.

Cisco Unified IP Phone Cleaning

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 to the phone. As with all nonweatherproof electronics, liquids and powders can damage the components and cause failures.

When the phone is in sleep mode, the touchscreen is blank and the **Select** button is not lit. When the phone is in this condition, you can clean the screen, as long as you know that the phone will remain asleep until after you finish cleaning. If the phone is likely to wake up during cleaning, wake it up or wait until it is awake before following the preceding cleaning instructions.

APPENDIX A

Internal support Web Site

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:

Cisco Unified IP Phone User Support

To successfully use some of the features on the Cisco Unified IP Phone (including Speed Dial, Services, and voice message system options), users must receive information from you or from your network team or must be able to contact you for assistance. Make sure to provide users with the names of people to contact for assistance and with instructions for contacting those people.

User Options Web Pages Access

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 more information, see:

- "User Group Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*
- "Role Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*

Phone Features User Subscription and Setup

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 Cisco Unified Communications Manager user addition, on page 121).

- 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.

User Voice Messaging System Access

Cisco Unified Communications Manager lets you integrate with 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.

User Personal Directory Entries Setup

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 Phone Features User Subscription and Setup, on page 194 for details.
- Cisco Unified IP Phone Address Book Synchronizer: Make sure to provide users with the installer for this application.

Obtain Cisco Unified IP Phone Address Book Synchronizer

To download a copy of the synchronizer to send to your users, follow these steps:

Procedure

Step 1 To obtain the installer, choose **Application** > **Plugins** from Cisco Unified Communications Manager Administration.

Step 2 Select **Download**, which is located next to the Cisco Unified IP Phone Address Book Synchronizer plugin name.

Step 3 When the file download dialog box displays, select **Save**.

Step 4 Send the TabSyncInstall.exe file and the instructions in Cisco Unified IP Phone Address Book Synchronizer Deployment, on page 195 to all users who require this application.

Cisco Unified IP Phone Address Book Synchronizer Deployment

The Cisco Unified IP Phone Address Book Synchronizer synchronizes data that is stored in your Microsoft Windows address book with the Cisco Unified Communications Manager directory and the User Options Personal Address Book.

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 you perform the following procedures.

Install Synchronizer

To install the Cisco Unified IP Phone Address Book Synchronizer, follow these steps:

Procedure

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 that your administrator provided.
The publisher dialog box displays.

Step 3 Select **Run**.

The Welcome to the InstallShield Wizard for Cisco Unified CallManager Personal Address Book Synchronizer window displays.

Step 4 Select **Next**.
The License Agreement window displays.

Step 5 Read the license agreement information, and select the **I Accept**. Select **Next**.
The Destination Location window displays.

Step 6 Choose the directory in which you want to install the application and select **Next**.
The Ready to Install window displays.

Step 7 Select **Install**.
The installation wizard installs the application to your computer. When the installation is complete, the InstallShield Wizard Complete window displays.

Step 8 Select **Finish**.

Step 9 To complete the process, follow the steps in Set Up Synchronizer, on page 196.

Set Up Synchronizer

To configure the Cisco Unified IP Phone Address Book Synchronizer, perform these steps:

Procedure

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, select **User**.
The Cisco Unified CallManager User Information window displays.

Step 3 Enter the Cisco Unified IP Phone user name and password and select **OK**.

Step 4 To configure Cisco Unified Communications Manager server information, select **Server**.
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 select **OK**.
If you do not have this information, contact your system administrator.

Step 6 To start the directory synchronization process, select **Synchronize**.
The Synchronization Status window provides 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.

Step 7 Choose the entry that you want to include in your Personal Address Book and select **OK**.

Step 8 When synchronization is complete, select **Exit** to close the Cisco Unified CallManager Address Book Synchronizer.

Step 9 To verify whether the synchronization worked, sign in to your User Options web pages and choose **Personal Address Book**. The users from your Windows address book should be listed.

APPENDIX B

International User Support

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.

For information on changing the language that is displayed on the User Options web page or the phone, see the *Cisco Unified IP Phone 6921, 6941, 6945, and 6961 User Guide for Cisco Unified Communications Manager (SCCP and SIP)*.

Cisco Unified Communications Manager Locale Installer Installation

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 that are 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, see 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.

International Call Logging Support

If your phone system is configured for international call logging (calling party normalization), the call logs, redial, or call directory entries may display a plus (+) 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.

APPENDIX C

Technical Specifications

The following sections describe the technical specifications for the Cisco Unified IP Phone 6921, 6941, 6945, and 6961.

Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the Cisco Unified IP Phone 6921, 6941, 6945, and 6961.

Table 36: Physical and Operating Specifications

Specification	Value or Range
Operating temperature	23° to 113°F (–5° to 45°C)
Operating relative humidity	10% to 90% (noncondensing)
Storage temperature	–13° to 176°F (–25° to 80°C)
Height	7.3 in. (18.57 cm)
Width	5.8 in. (14.79 cm)
Depth	7.1 in. (18.05 cm)
Weight	2.2 lb (1.0 kg)

Specification	Value or Range
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
Cables	Category 3/5/5e for 10-Mbps cables with 4 pairsCategory 5/5e for 100-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 100 meters (330 feet).

Cable Specifications

- RJ-9 jack (4-conductor) for handset and headset connection.
- RJ-45 jack for the LAN 10/100BaseT connection (labeled 10/100 SW on the Cisco Unified IP Phone 6921, 6941, 6945, and 6961).
- RJ-45 jack for a second 10/100BaseT compliant connection (labeled 10/100 PC on the Cisco Unified IP Phone 6921, 6941, 6945, and 6961).
- 48-volt power connector.

Network, access, and auxiliary port pinouts

Although both the network and access ports are used for network connectivity, they serve different purposes and have different port pinouts.

- The network port is labeled `network` on the Cisco Unified IP Phone.
- The access port is labeled `Computer` on the Cisco Unified IP Phone.
- The auxiliary port is labeled `AUX` on the Cisco Unified IP Phone 6945. Cisco Unified IP Phones 6921, 6941, and 6961 do not provide an auxiliary port.

Network Port Connector

The following table describes the network port connector pinouts.

Table 37: 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 bidirectional, while DA, DB, DC and DD stand for Data A, Data B, Data C and Data D respectively.	

Computer Port Connector

The following table describes the computer port connector pinouts.

Table 38: 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 bidirectional, while DA, DB, DC and DD stand for Data A, Data B, Data C and Data D respectively.	

Auxiliary Port Connector

The following table describes the auxiliary port connector pinouts for the Cisco Unified IP Phone 6945.

Table 39: Auxiliary Port Connector Pinouts

Pin number	Function
1	PWR_OUT+ (48V)
2	RS232_TXD
3	GND
4	RS232_RXD
5	GND
6	PWR_OUT- (RTN)

APPENDIX D

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

In the procedures that follow, examples are given when possible to illustrate some of the steps. Example user and phone information used throughout these procedures includes:

- User's Name: John Doe
- User ID: johndoe
- MAC address listed on phone: 00127F576611
- Five-digit internal telephone number: 26640

Cisco Unified Communications Manager user addition

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.

Add user from 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 Select on the LDAP directory name.

Step 5 Select **Perform Full Sync Now**.
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 Identify phone, on page 207.

Add 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:

Procedure

Step 1 Choose **User Management** > **End User**, then select **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 Select **Save**.

Step 4 Proceed to the section Identify phone, on page 207.

Identify phone

To configure the phone, you must first identify the phone and then configure it using the following procedures.

Identify phone

To identify the user phone model and protocol, follow these steps:

Procedure

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

Step 2 Select **Add New**.

Step 3 Select the user phone model from the Phone Type drop-down list, and select **Next**.
The Phone Configuration window appears. On the Phone Configuration window, you can use the default values for most of the fields.

Set up phone fields

To configure the required fields and some key additional fields, perform 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.

  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 fields in conjunction with the **Find** button to find all configured phone button templates and their current settings.

- Softkey Template: Choose the appropriate softkey template. The softkey template determines the configuration of the softkeys on Cisco Unified IP Phones. Leave this field blank if the common device configuration contains the assigned softkey template.

  Softkey templates are defined on the Softkey Template Configuration window of Cisco Unified Communications Manager Administration (**Device** > **Device Settings** > **Softkey Template**). You can use the search fields in conjunction with the **Find** button to find all configured softkey 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.

  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 fields 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.

  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 fields 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 nonsecure profile.

To identify the settings that are contained in the profile, choose **System** > **Security Profile** > **Phone Security Profile**.

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) Select **Save**.

Step 2 Configure line settings:

a) On the Phone Configuration window, select 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.
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 (for example, 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 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 numbers 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 select the **Propagate Selected** button. (The check box at right displays only if other devices share this directory number.)

g) Select **Save**.
h) Select **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 choose **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) Select **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 (for example, *doe* for the last name).
- Select the user ID (for example, *johndoe*). The End User Configuration window appears.
- Select **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 choose **Save Selected/Changes**. The user is now associated with the device.
- Click **Go** next to the "Back to User" Related link in the upper-right corner of the screen.

Step 3 Proceed to Perform final end user configuration steps, on page 210.

Perform final end user configuration steps

If you are not already jn the End User Configuration window, choose **User Management** > **End User** to perform some final configuration tasks. Use the Search fields and **Find** to locate the user (for example, 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, follow these steps:

Procedure

Step 1 In the Directory Number Associations area of the screen, set the primary extension from the drop-down list.

Step 2 In the Mobility Information area, check the Enable Mobility box.

Step 3 In the Permissions Information area, 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 is defined as a Standard CCM End User Group.

Step 4 To view all configured user groups, choose **User Management** > **User Group**.

Step 5 In the Extension Mobility area, check the Enable Extension Mobility Cross Cluster box if the user is allowed for Extension Mobility Cross Cluster service.

Step 6 Select **Save**.

APPENDIX **E**

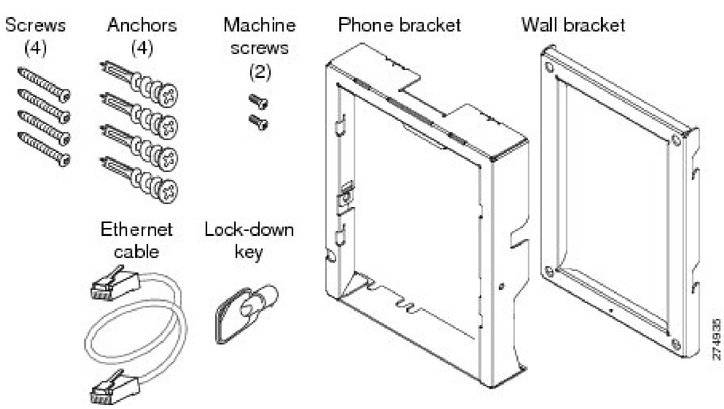
Cisco Unified IP Phone 6921, 6941, 6945, and 6961 Wall Mount Kit

This appendix contains information on installing the wall mount for use with the Cisco Unified IP Phone 6921, 6941, 6945, and 6961.

Wall Mount Kit Components

The following figure shows the contents of the Wall Mount kit.

Figure 4: Wall Mount Kit



The package includes these items:

- One phone bracket

- One wall bracket
- Four #10-12x1-inch Phillips-head screws with 4 anchors
- Two #4-40x1/4-inch machine screws
- One 6-inch Ethernet cable
- One 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 Cisco Unified IP Phone Setup, on page 61 chapter.

Install Bracket

To install the phone on the wall, perform the following steps:

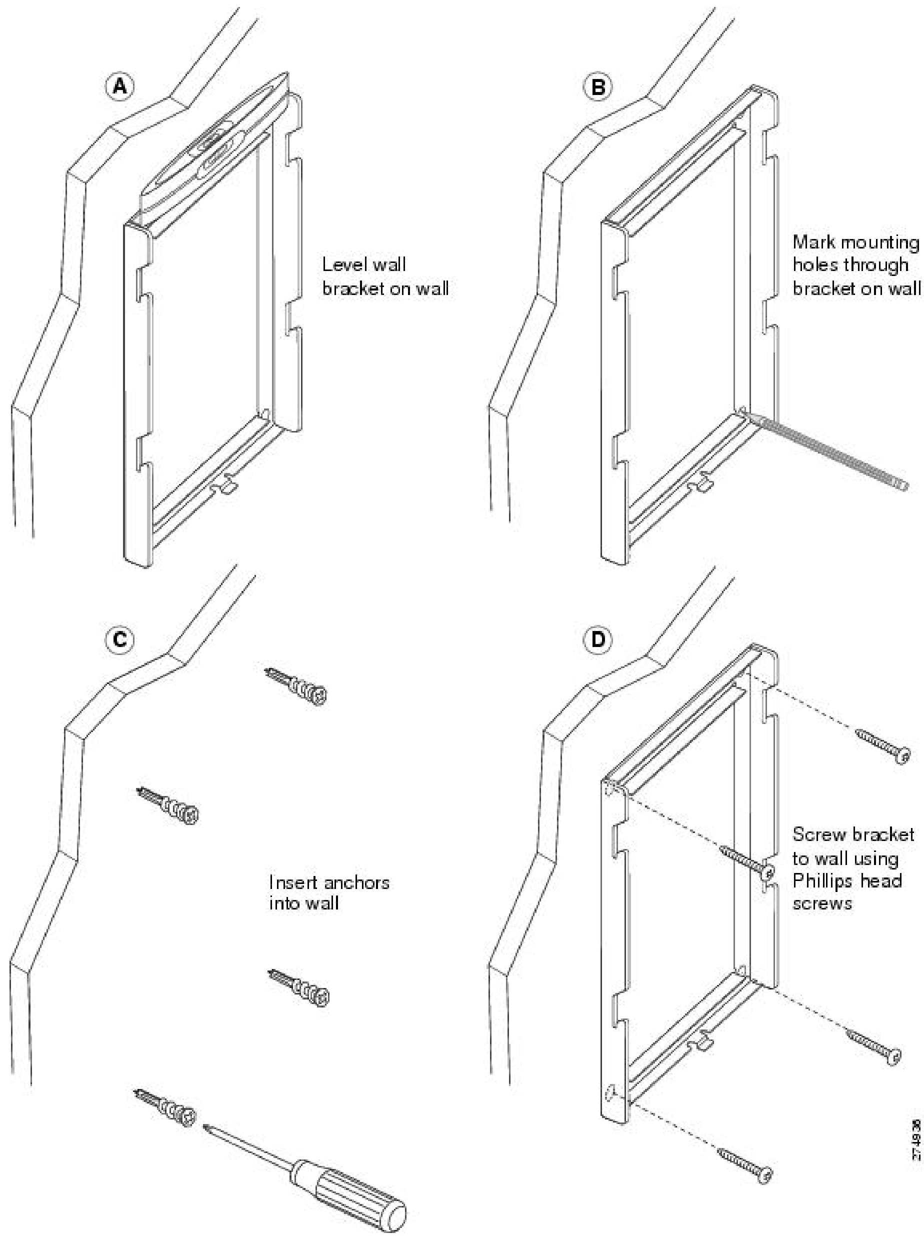
Procedure

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.

a) Use the level to ensure the bracket is level, then use a pencil to mark the screw holes.
b) Use a #2 Phillips-head screwdriver to 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 5: Mounting the Wall Bracket

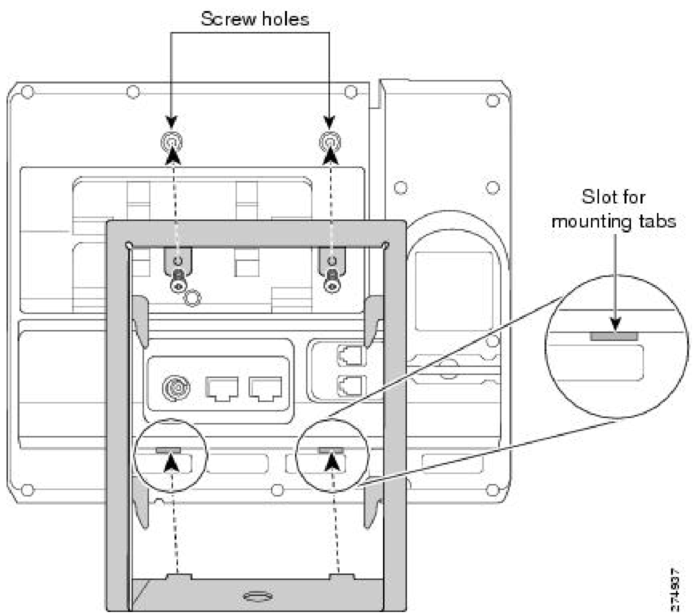


Step 2 Attach the phone bracket to the IP phone.

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 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.

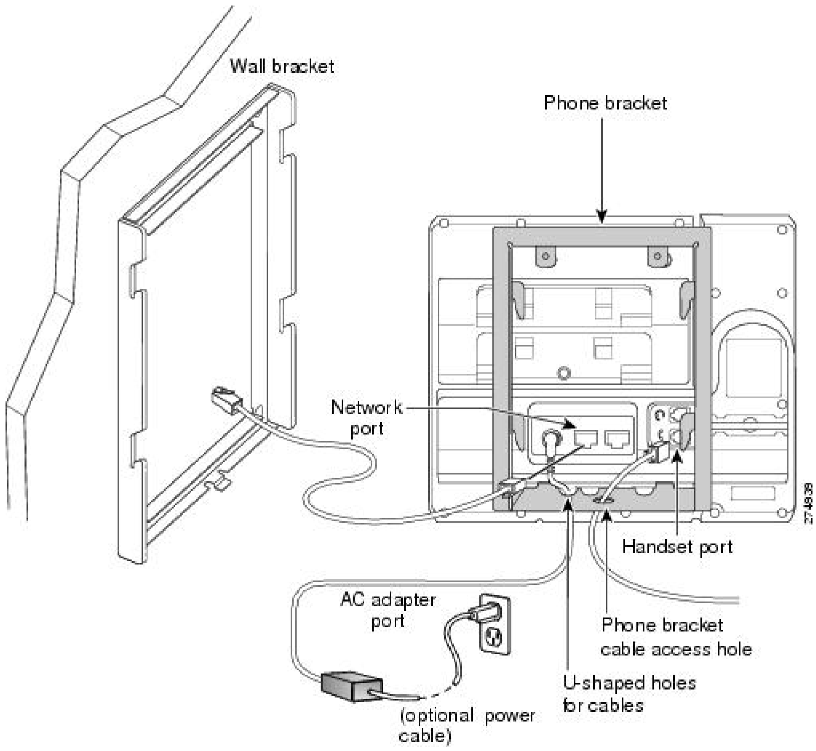
Figure 6: Attaching the Phone Bracket



Step 3 Attach the Ethernet cable to the 10/100 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 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 10/100 PC port.

Figure 7: Attaching the Cables

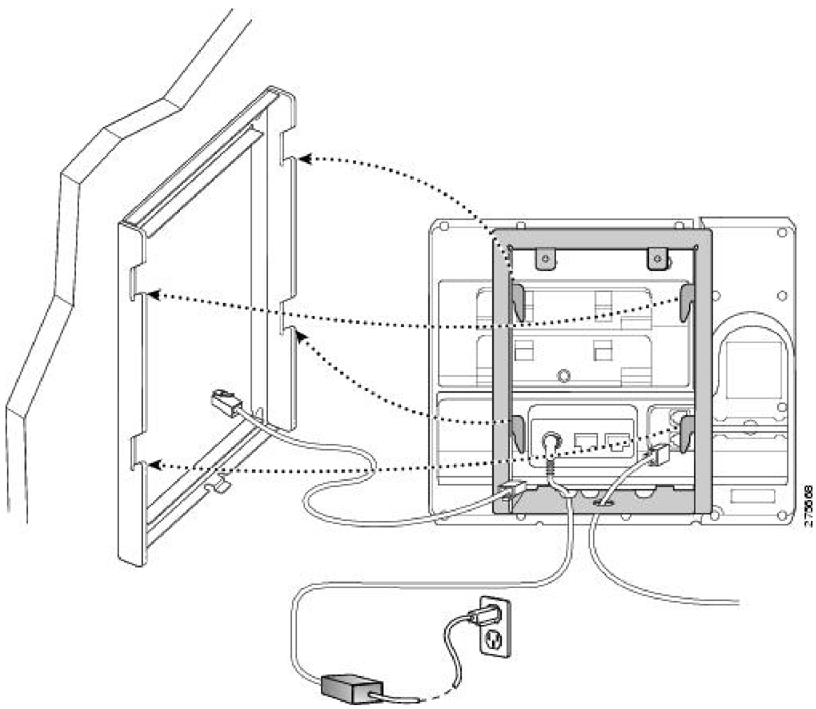


Step 4 Attach the phone to the wall bracket by inserting the tabs on the top of the phone bracket into the slots on the wall bracket. Ensure that the power cord and any other cable that does not terminate in the wall behind the

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.

Step 5 Use the locking key to lock the phone to the wall bracket.

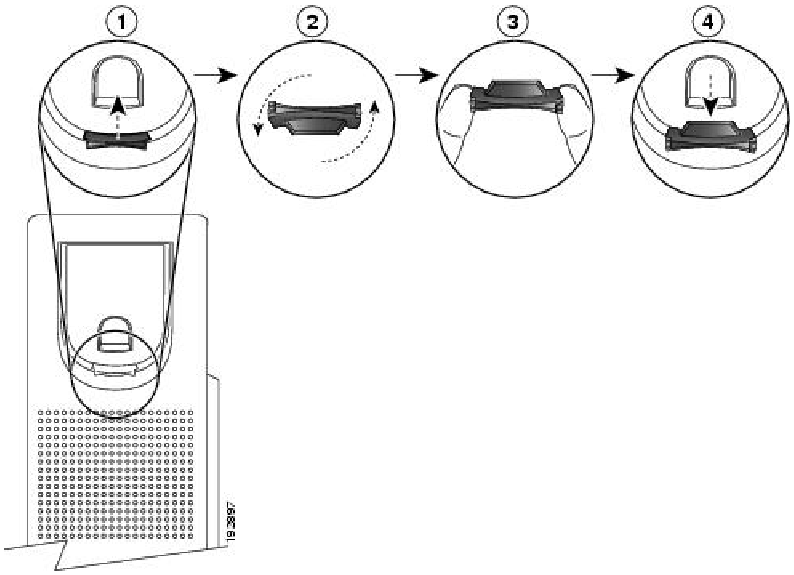
Figure 8: Attaching the Phone to the Wall Bracket



Adjust Handset Rest

With a wall-mounted phone, you might need to adjust the handset rest to ensure that the receiver does not slip out of the cradle. The hook should have a lip on which the handset catches when the phone is vertical. Follow the diagram and steps below to change the hookswitch hook.

Figure 9: Adjust the Handset Hook



1	Remove the 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.

APPENDIX F

Cisco Unified IP Phone Non-Lockable Wall Mount

This appendix contains the information for installing the following product:

- ADA Non-Lockable Wall Mount Kit for 6900 Series: Installed on the Cisco Unified IP Phone 6911, 6921, 6941, 6945, and 6961.

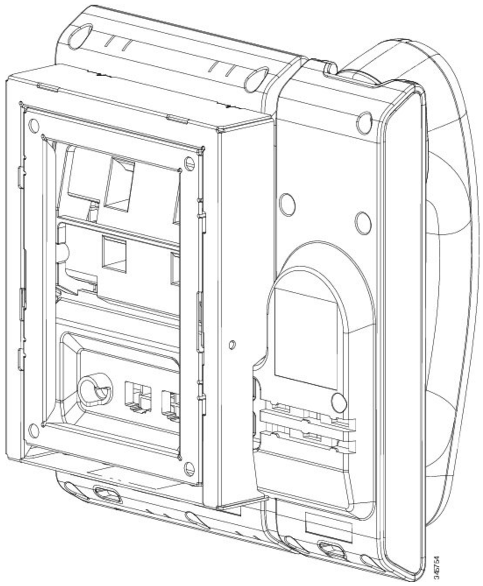
This nonlocking wall mount kit meets ADA 4.4.1 requirements.

ADA Non-Lockable Wall Mount Kit for 6900 Series

This section describes how to install the ADA Non-Lockable Wall Mount Kit for 6900 Series on a Cisco Unified IP Phone 6911, 6921, 6941, 6945, and 6961.

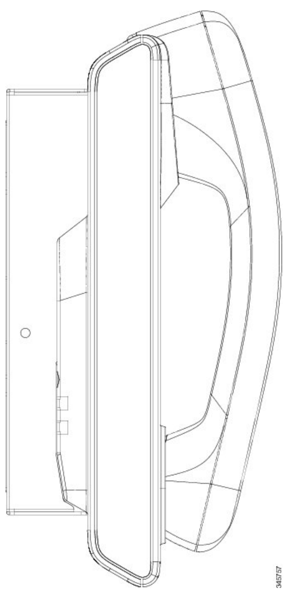
The following figure shows the wall mount kit installed on the phone.

Figure 10: 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.

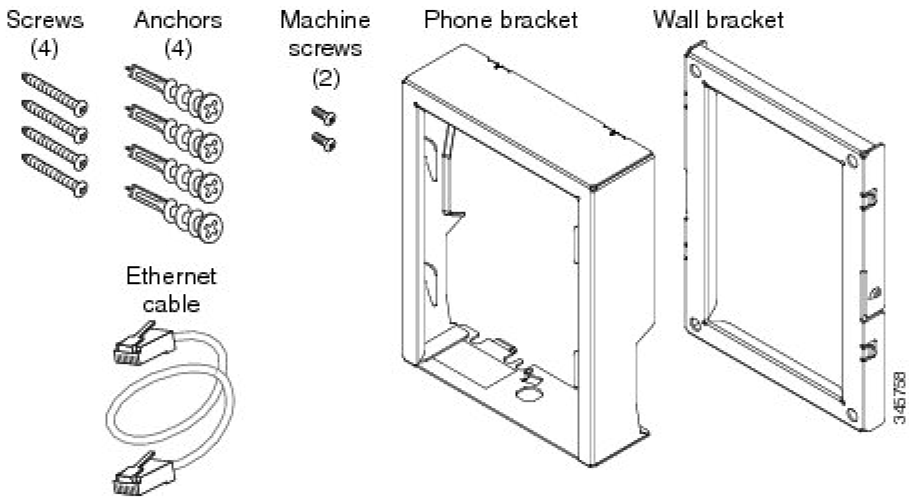
Figure 11: Side View of ADA Non-Lockable Wall Mount Kit Installed on Phone



Components

The following figure shows the contents of the Wall Mount kit.

Figure 12: Components



The package includes these items:

- One phone bracket
- One wall bracket
- Four #8-18 x 1.25-inch Phillips-head screws with four anchors
- Two M2.5 x 6 mm 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.

Related Topics

Cisco Unified IP Phone Setup, on page 61

Install Non-Lockable Wall Mount Kit 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

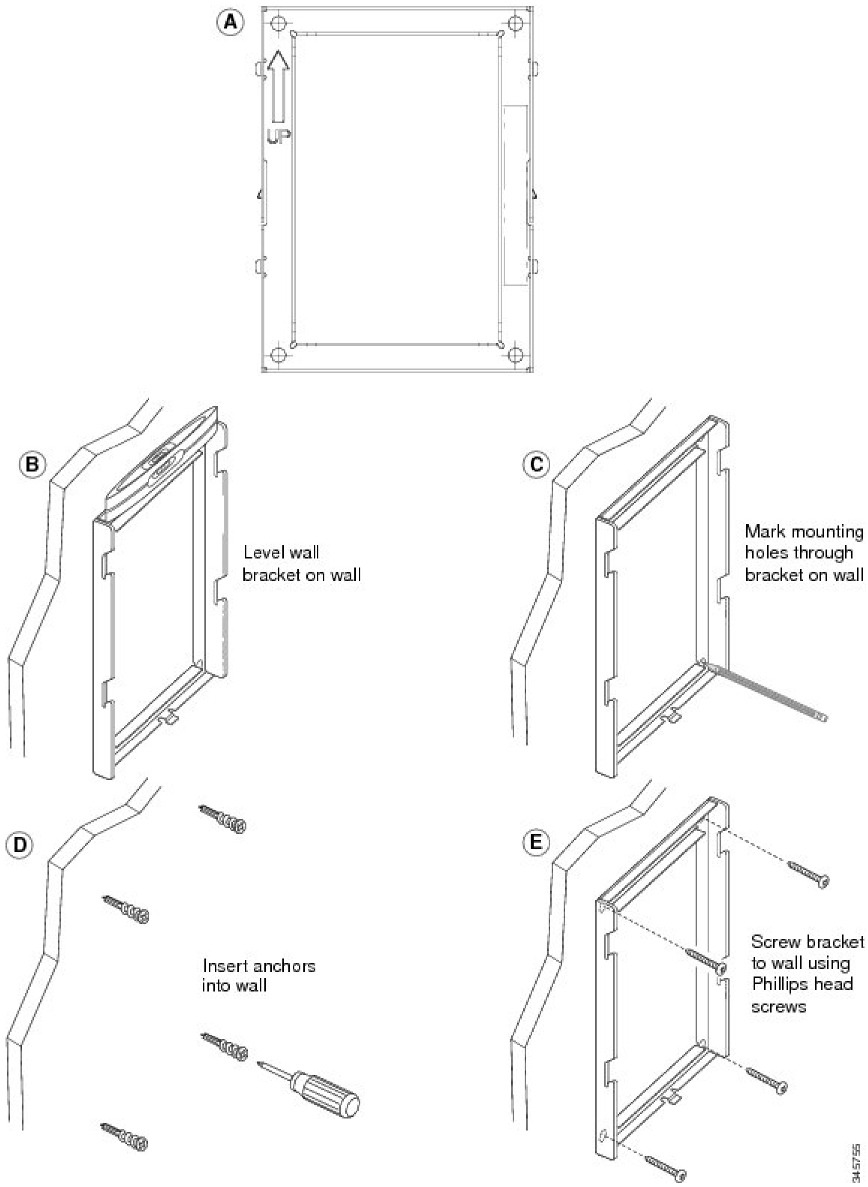
Step 1 Mount the wall bracket in the desired location. You can install the bracket over an Ethernet jack, or you can run the Ethernet network cable to a jack nearby.

Note If the jack is to be placed behind the phone, the Ethernet 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 and use a pencil to mark the screw holes.
c) Use a #2 Phillips-head screwdriver to 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 to mount the wall bracket.

Figure 13: Mount Wall Bracket

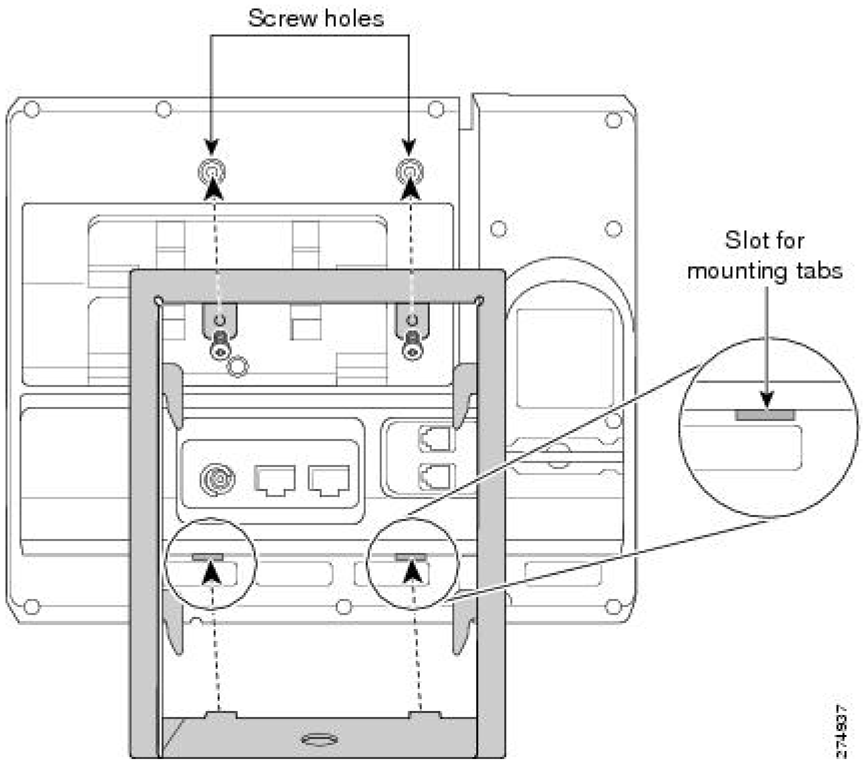


Step 2 Attach the phone bracket to the IP phone.

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 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 the #1 Phillips-head screwdriver.
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 to attach the phone bracket.

Figure 14: Attach Phone Bracket

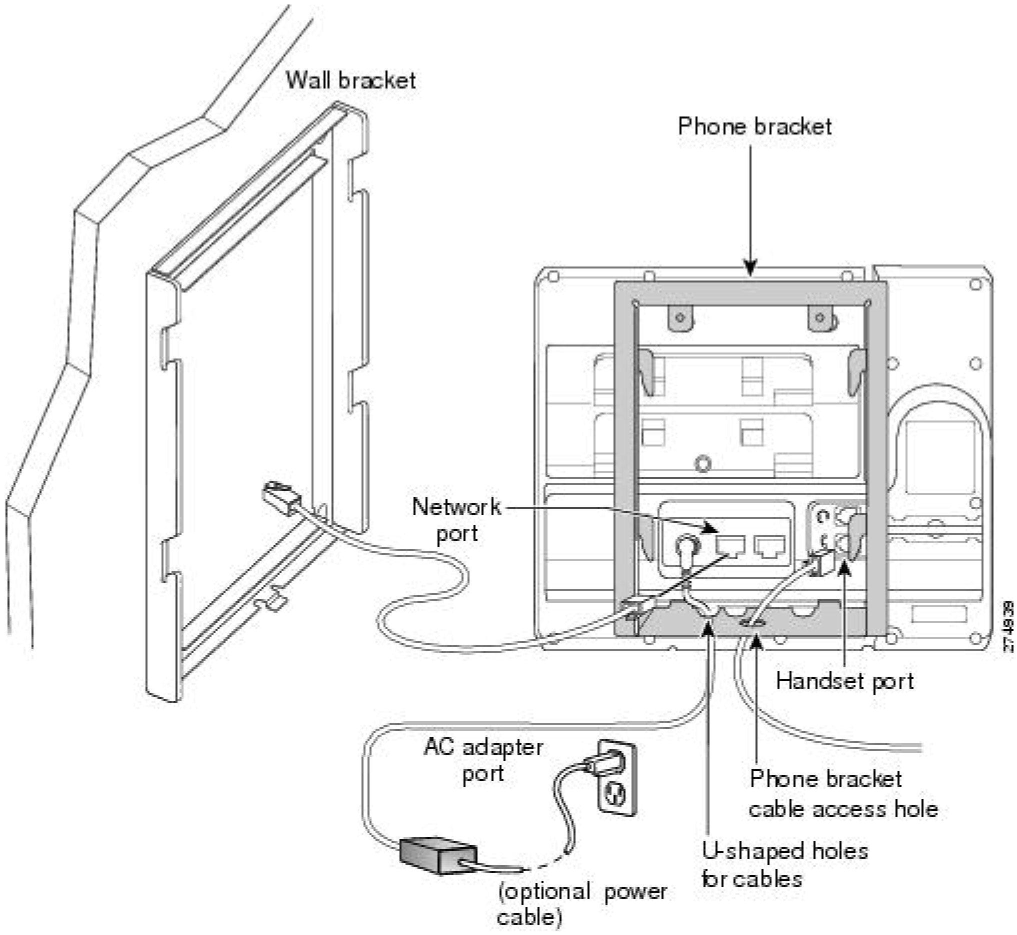


Step 3 Attach the cables.

a) Attach the Ethernet cable to the 10/100 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 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 incorporated into the phone body next to the 10/100 PC port.
d) (Optional) If the cables terminate inside the wall bracket, connect the cables to the jacks.

The following figure shows the cable attachment.

Figure 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.

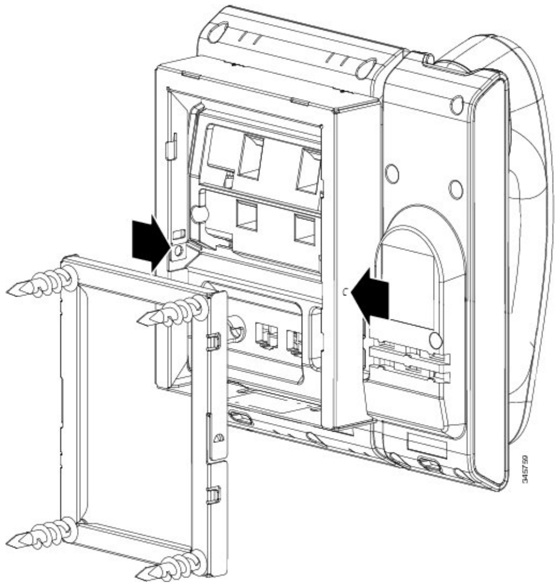
Step 5 Proceed to Adjust Handset Rest, on page 217.

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.

The following figure shows the tab location.

Figure 16: 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.

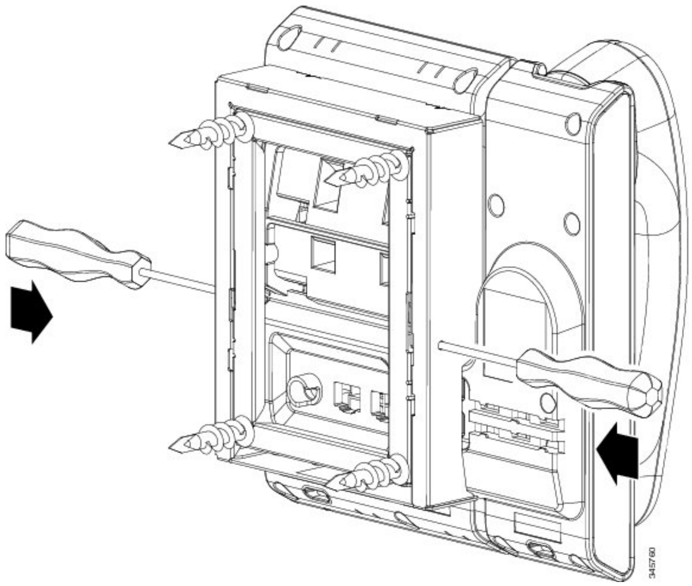
Procedure

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 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.

The following figure shows how to disengage the tabs.

Figure 17: Disengage Tabs



APPENDIX G

Feature support by protocol

This appendix provides information about feature support for the Cisco Unified IP Phone 6921, 6941, 6945, and 6961 using the SCCP or SIP protocol with Cisco Unified Communications Manager Release 9.0.

The following table provides a high-level overview of calling features and their support by protocol. This table focuses primarily on end-user calling features and is not intended to represent a comprehensive listing of all available phone features. For details about user interface differences and feature use, see the *Cisco Unified IP Phone 6921, 6941, 6945, and 6961 User Guide for Cisco Unified Communications Manager (SCCP and SIP)*.

The guide is available at this URL:

http://www.cisco.com/en/US/products/ps10326/tsd_products_support_series_home.html

The specific sections that describe the features in the user guide are referenced in the following table.

Table 40: Cisco Unified IP Phone 6921, 6941, 6945, and 6961 Feature Support by Protocol

Features	**Protocol: SCCP**	**Protocol: SIP**	**For more information, see the following section in the user guide**
Calling Features			
Abbreviated Dialing	Supported	Supported	
Agent Greeting	Supported	Supported	Calling features - Agent Greeting
Assisted Directed Call Park	Not supported	Supported	Calling features - Call Park
Audible Message Waiting Indicator (AMWI)	Supported	Supported	Messages
Auto Answer	Supported	Supported	Calling features - Auto Answer

Features	Protocol: SCCP	Protocol: SIP	For more information, see the following section in the user guide
Auto-pickup	Supported	Supported	
Automatic Port Synchronization	Supported	Supported	
cBarge	Supported	Supported	Calling features - Shared lines
Block external to external transfer	Supported	Supported	
Busy Lamp Field (BLF)	Supported	Supported	Calling features - Line status
Busy Lamp Field (BLF) Pickup	Supported	Supported	Calling features - Line status
Call Back	Supported	Supported	Calling features - Call Back
Call Display Restrictions	Supported	Supported	
Call Forward All	Supported	Supported	Calling features - Call Forward
Call Forward All Breakout	Supported	Supported	Calling features - Call Forward
Call Forward All Loop Prevention	Supported	Supported	Calling features - Call Forward
Call Forward Busy	Supported	Supported	Calling features - Call Forward
Call Forward Configurable Display	Supported	Supported	Calling features - Call Forward
Call Forward Destination Override	Supported	Supported	Calling features - Call Forward
Call Forward No Answer	Supported	Supported	Calling features - Call Forward
Call History for Shared Line	Supported	Supported	Applications - Call History
Call Park	Supported	Supported	Calling features - Call Park

Features	Protocol: SCCP	Protocol: SIP	For more information, see the following section in the user guide
Call Pickup Group Call Pickup Directed Call Pickup	Supported	Supported	Calling features - Call Pickup
Call Recording	Supported	Supported	Calling features - Monitoring and Recording
Call Waiting	Supported	Supported	Calling features - Call Waiting
Call Waiting Ring	Supported	Supported	
Caller ID	Supported	Supported	
Caller ID Blocking	Supported	Supported	
Calling Party Normalization	Supported	Supported	
Cisco Extension Mobility	Supported	Supported	Calling features - Cisco Extension Mobility
Cisco Extension Mobility Cross Cluster	Supported	Supported	
Client Matter Codes (CMC)	Supported	Supported	Calling features - Codes
Computer Telephony Integration (CTI) Applications	Supported	Some support (such as Call Park, MWI)	
Configurable Call Forward Display	Supported	Supported	
Debug Phone	Supported	Supported	
Device Invoked Recording	Supported	Supported	Calling features - Monitoring and Recording
Direct Transfer	Supported	Supported	Calling features - Transfer

Features	Protocol: SCCP	Protocol: SIP	For more information, see the following section in the user guide
Directed Call Park	Supported	Supported	Calling features - Call Park
Disable Single Button Barge	Supported	Supported	
Do Not Disturb (DND)	Supported	Supported	Calling features - Do Not Disturb
Distinctive Ring	Supported	Supported	Applications - Ringtones
Electronic Hookswitch	Supported (6945 only)	Supported (6945 only)	Features of Your Cisco Unified IP Phone—Cisco Unified IP Phone 6945 - Wireless headset using auxiliary port
EnergyWise	Supported	Supported	Features of your Cisco Unified IP Phone—Power-Saving mode
Enhanced Version Negotiation with Cisco Unified Manager Express	Not supported	Supported	
Fast Dial Service	Supported	Supported	Calling features - Speed Dial
Forced Authorization Codes (FAC)	Supported	Not supported	Calling features - Codes
Group Call Pickup	Supported	Supported	Calling features - Call Pickup
Hold/Resume	Supported	Supported	Calling features - Hold
Hold Reversion	Supported	Supported	Calling features - Hold
Hunt Group	Supported	Supported	
HTTPS	Supported	Supported	
Immediate Divert	Supported	Supported	Calling features - Divert
Incoming Call Toast Timer	Supported	Supported	

Features	Protocol: SCCP	Protocol: SIP	For more information, see the following section in the user guide
Intercom	Supported	Supported	Calling features - Intercom
Jitter Buffer	Supported	Supported	
Join	Supported	Supported	Calling features - Conference
Join Across Lines	Supported	Supported	Calling features - Conference
Line Status for Call Lists	Supported	Supported	Applications - Call History
Log Out of Hunt Groups	Supported	Supported	Calling features - Hunt groups
Malicious Call ID	Supported	Supported	Calling features - Malicious Call Identification
Meet Me Conference	Supported	Supported	Calling features - Conference
Message Waiting Indicator	Supported	Supported	Messages
Minimum Ring Volume	Supported	Supported	Features of Your Cisco Unified IP Phone
Mobile Connect	Supported	Supported	Calling features - Mobile Connect
Mobile Voice Access	Supported	Supported	
Monitoring and Recording	Supported	Supported	Calling features - Monitoring and Recording
Multilevel Precedence and Preemption (MLPP)	Supported	Not supported	Calling features - Multilevel Precedence and Preemption
Multiple Calls Per Line appearance	Supported	Supported	Calling features - Multiple calls per line
Music on Hold	Supported	Supported	
Mute	Supported	Supported	Calling features - Mute

Features	Protocol: SCCP	Protocol: SIP	For more information, see the following section in the user guide
No Alert Name	Not Supported	Supported	
On-hook Dialing	Supported	Supported	Calling features - On-hook dialing
Other Group Pickup	Supported	Supported	Calling features - Call Pickup
Phone Display Message for Extension Mobility Users	Supported	Supported	Calling features - Extension Mobility
PLK Support for Queue Statistics	Supported	Supported	Calling features - Hunt groups
Plus Dialing	Supported	Supported	Calling features - Plus Dialing
Privacy	Supported	Supported	Calling features - Privacy
Private Line Automated Ringdown (PLAR)	Supported	Supported	
Programmable Feature Buttons	Supported	Supported	
Programmable Feature Buttons as Softkeys	Supported	Supported	
Quality Reporting Tool (QRT)	Supported	Supported	
Redial	Supported	Supported	Calling features - Redial
Ring Setting	Supported	Supported	Applications - Ringtones
Ringer Volume Control	Supported	Supported	
Secure Conference	Supported	Supported	Calling features - Conference
Secure EMCC	Supported	Supported	

Features	Protocol: SCCP	Protocol: SIP	For more information, see the following section in the user guide
Security by Default	Supported	Supported	
Services	Supported	Supported	Applications - Services
Services URL button	Supported	Supported	Applications - Services
Shared Line	Supported	Supported	Calling features - Shared lines
Show Calling ID and Calling Number	Supported	Supported	Phone Screen
Speed Dialing	Supported	Supported	Calling features - Speed Dial
SRST Notification	Supported	Supported	
SSH Access	Supported	Supported	
Time-of-Day Routing	Supported	Supported	
Transfer	Supported	Supported	Calling features - Transfer
Transfer - Direct Transfer	Supported	Supported	Calling features - Transfer
Time Zone Update	Supported	Supported	
TVS	Supported **Note** Both IPv4 and IPv6 are supported.	Not Supported **Note** Only IPv4 is supported.	
UCR 2008	Supported	Not supported	
Voice Mail	Supported	Supported	Messages
Web Access Disabled by Default	Supported	Supported	

INDEX

C

D

E

F

G

H

I

J

K

L

O

P

Q

R

S

T

U

V

W