Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager 8.6 (SCCP and SIP)

For Cisco Unified IP Phones 7962G, 7942G, 7961G, 7961G-GE, 7941G, and 7941G-GE

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

Text Part Number: OL-23091-01

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager 8.6 (SCCP and SIP)

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

CONTENTS

Preface

Overview

Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager 8.6 (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. See Related Documentation, page xii for a list of related documentation.

Audience

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

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

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

Organization

This manual is organized as follows:

Chapter	Description
Chapter 1, An Overview of the Cisco Unified IP Phones	Provides a conceptual overview and description of the Cisco Unified IP Phones.
Chapter 2, Preparing to Install the Cisco Unified IP Phones on Your Network	Describes how the Cisco Unified IP Phones interact with other key IP telephony components, and provides an overview of the tasks required prior to installation.
Chapter 3, Setting Up the Cisco Unified IP Phones	Describes how to properly and safely install and configure the Cisco Unified IP Phones on your network.

Chapter 4, Configuring Settings on the Cisco Unified IP Phones	Describes how to configure network settings, verify status, and make global changes to the Cisco Unified IP Phones.
Chapter 5, Configuring Features, Templates, Services, and Users	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.
Chapter 6, Customizing the Cisco Unified IP Phones	Explains how to customize phone ring sounds, background images, and the phone idle display at your site.
Chapter 7, Monitoring the Cisco Unified IP Phones Remotely	Describes the information that you can obtain from the phone's web page to remotely monitor the operation of a phone and to assist with troubleshooting.
Chapter 8, Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phones	Explains how to view model information, status messages, network statistics, and firmware information from the Cisco Unified IP Phones.
Chapter 9, Troubleshooting and Maintenance	Provides tips for troubleshooting the Cisco Unified IP Phone and the Cisco Unified IP Phones Expansion Modules.
Appendix A, Providing Information to Users Via a Website	Provides suggestions for setting up a website for providing users with important information about their Cisco Unified IP Phones.
Appendix B, Feature Support by Protocol for Cisco Unified IP Phone	Provides information about feature support for the Cisco Unified IP Phones 7962G, 7942G, 7961G, 7961G-GE, 7941G, and 7941G-GE using the SCCP or SIP protocol with Cisco Unified Communications Manager Release.
Appendix C, Supporting International Users	Provides information about setting up phones in non-English environments.
Appendix D, Technical Specifications	Provides technical specifications of the Cisco Unified IP Phones.
Appendix E, Basic Phone Administration Steps	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.

Related Documentation

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

Cisco Unified IP Phone 7900 Series

These publications are available at the following URL:

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

Cisco Unified Communications Manager Administration

Related publications are available at the following URL:

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

Cisco Unified Communications Manager Business Edition

Related publications are available at the following URL:

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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

Cisco Product Security Overview

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

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

Document Conventions

This document uses the following conventions:

Table 1

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

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

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

Warning **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.**

CHAPTER 1

An Overview of the Cisco Unified IP Phones

The Cisco Unified IP Phones 7962G, 7942G, 7961G, 7961G-GE (gigabit Ethernet version), 7941G, and 7941G-GE (gigabit Ethernet version) are full-feature telephones that provide voice communication over an Internet Protocol (IP) network. The gigabit Ethernet Cisco Unified IP Phones 7961G-GE and 7941G-GE deliver the latest technology and advancements in Gigabit Ethernet VoIP telephony. The Cisco Unified IP Phones function much like a digital business phone, allowing you to place and receive phone calls and to access features such as mute, hold, transfer, speed dial, call forward, and more. In addition, because the phone is connected to your data network, it offers enhanced IP telephony features, including access to network information and services, and customizeable features and services. The phone also supports features that include file authentication, device authentication, signaling encryption, and media encryption.

Cisco Unified IP Phones, like other network devices, must be configured and managed. These phones encode G.711a, G.711µ, G.722, G.729a, G.729ab, and iLBC codecs and decode G.711a, G.711u, G.722, G.729, G729a, G729b, G729ab and iLBC codecs. These phones also support uncompressed wideband (16bits, 16kHz) audio.

This chapter includes the following topics:

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

Understanding the Cisco Unified IP Phone 7962G and 7942G 7962G, 7942G, 7961G, 7961G-GE, 7941G, and 7941G-GE

Figure 1-1 shows the main components of the Cisco Unified IP Phone 7962G.

Figure 1-2 shows the main components of the Cisco Unified IP Phone 7942G.

Figure 1-3 shows the main components of the Cisco Unified IP Phone 7961G and 7961G-GE.

Figure 1-4 shows the main components of the Cisco Unified IP Phone 7941G and 7941G-GE.

Figure 1-1 Cisco Unified IP Phone 7962G

Figure 1-2 Cisco Unified IP Phone 7942G

Figure 1-3 Cisco Unified IP Phone 7961G and 7961G-GE

Figure 1-4 Cisco Unified IP Phone 7941G and 7941G-GE

Table 1-1 describes the buttons on the Cisco Unified IP Phone 7962G and 7942G.

Table 1-1 Features on the Cisco Unified IP Phones 7962G, 7942G, 7961G, 7961G-GE, 7941G, and 7941 G-GE

1	Programmable buttons	Depending on configuration, programmable buttons provide access to: • Phone lines (line buttons) • Speed-dial numbers (speed-dial buttons, including the BLF speed-dial feature) • Web-based services (for example, a Personal Address Book [PAB] button) • Phone features (for example, a Privacy button) The buttons illuminate to indicate status: Green, steady—Active call Green, flashing—Held call Amber, steady—Privacy in use Amber, flashing—Incoming call Red steady—Remote line in use (shared line, BLF status, or active Mobile Connect call)
2	Phone screen	Shows phone features.
3	Footstand button	Allows you to adjust the angle of the phone base.
4	Messages button	Dials your voice-message service automatically (varies by service).
5	Directories button	Opens/closes the Directories menu. Use the button to access call logs and directories.

6	Help button 	Activates the Help menu.
7	Settings button 	Opens/closes the Settings menu. Use the button to control phone screen contrast and ring sounds.
8	Services button 	Opens/closes the Services menu.
9	Volume button 	Controls the handset, headset, and speakerphone volume (off-hook) and the ringer volume (on-hook).
10	Speaker button 	Toggles the speakerphone on or off. When the speakerphone is on, the button is lit.
11	Mute button 	Toggles the Mute feature on or off. When Mute is on, the button is lit.
12	Headset button 	Toggles the headset on or off. When the headset is on, the button is lit.
13	Navigation button 	Allows you to scroll through menus and highlight items. When the phone is on-hook, displays phone numbers from your Placed Calls log.
14	Keypad	Allows you to dial phone numbers, enter letters, and choose menu items.
15	Softkey buttons 	Each activates a softkey option (displayed on your phone screen).
16	Handset light strip	Indicates an incoming call or new voice message.

What Networking Protocols are Used?

Cisco Unified IP Phones support several industry-standard and Cisco networking protocols required for voice communication. Table 1-2 provides an overview of the networking protocols that the Cisco Unified IP Phones support.

Table 1-2 Supported Networking Protocols on the Cisco Unified IP Phones

Networking Protocol	Purpose	Usage Notes
Bootstrap Protocol (BootP)	BootP enables a network device such as the Cisco Unified IP Phones to discover certain startup information, such as its IP address.	If you use BootP to assign IP addresses to the Cisco Unified IP Phones, the BOOTP Server option shows “Yes” in the network configuration settings on the phone.

Table 1-2 Supported Networking Protocols on the Cisco Unified IP Phones (continued)

Networking Protocol	Purpose	Usage Notes
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. Using CDP, a device advertises its existence to other devices and receives information about other devices in the network.	The Cisco Unified IP Phones use CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Cisco Peer-to-Peer Distribution Protocol (CPPDP)	CPPDP is a Cisco proprietary protocol used to form a peer-to-peer hierarchy of devices. CPPDP is also used to copy firmware or other files from peer devices to neighboring devices.	CPPDP is used by the Peer Firmware Sharing feature.
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect an IP Phone into the network and have the phone become operational without your needing to manually assign an IP address or to configure additional network parameters.	DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each phone locally. Cisco recommends that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, see Dynamic Host Configuration Protocol and Cisco TFTP in the *Cisco Unified Communications Manager System Guide*.
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. Cisco Unified IP Phones do not support the use of IPv6 addresses in the URL. You cannot use a literal IPv6 address in the URL or a hostname that maps to an IPv6 address.
Hypertext Transfer Protocol Secure (HTTPS)	Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of servers.	Web applications with both HTTP and HTTPS support have two URLs configured. Cisco Unified IP Phones that support HTTPS choose the HTTPS URL out of the two URLs.
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 Phones implement 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. See Supporting 802.1X Authentication on Cisco Unified IP Phones, page 1-19 for additional information.

Table 1-2 Supported Networking Protocols on the Cisco Unified IP Phones (continued)

Networking 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 gateway identifications are automatically assigned if you are using the Cisco Unified IP Phones 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 concurrent IPv4 and IPv6 addresses. Configure the IP addressing mode (IPv4 only, IPv6 only, and both IPv4 and IPv6) in Cisco Unified Communications Manager Administration. 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 some Cisco and third-party devices support.	The Cisco Unified IP Phones support 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 Phones support LLDP-MED on the SW port to communicate information such as: • Voice VLAN configuration • Device discovery • Power management • Inventory management For more information about LLDP-MED support, see the *LLDP-MED and Cisco Discovery Protocol* white paper: http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	Cisco Unified IP Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.
Real-Time Control Protocol (RTCP)	RTCP works in conjunction with RTP to provide Quality of Service (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. For more information, see Network Configuration Menu, page 4-34.
Session Description Protocol (SDP)	SDP is the portion of the SIP protocol that determines which parameters are available during a connection between two endpoints. Conferences are established by using only the SDP capabilities that are supported by all endpoints in the conference.	SDP capabilities, such as codec types, DTMF detection, and comfort noise, are normally configured on a global basis by Cisco Unified Communications Manager or Media Gateway in operation. Some SIP endpoints may allow these parameters to be configured on the endpoint itself.

Table 1-2 Supported Networking Protocols on the Cisco Unified IP Phones (continued)

Networking Protocol	Purpose	Usage Notes
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 Phones 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.	Cisco Unified IP Phones use SCCP for call control. You can configure the Cisco Unified IP Phone to use either SCCP or Session Initiation Protocol (SIP).
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Cisco Unified IP Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.
Transport Layer Security (TLS)	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 Phones, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server. If you want a phone to use a TFTP server other than the one specified by the DHCP server, you must manually assign the IP address of the TFTP server by using the Network Configuration menu on the phone. For more information, see Cisco TFTP 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.

IPv6 Support on Cisco Unified IP Phones

The Cisco Unified IP Phones uses the internet protocol to provide voice communication over the network. Because it uses a 32-bit address, Internet Protocol version 4 (IPv4) cannot meet the increased demands for unique IP addresses for all devices that can connect to the internet. Internet Protocol version

6 (IPv6) is an updated version of the current Internet Protocol, IPv4. IPv6 uses a 128-bit address and provides end-to-end security capabilities, enhanced Quality of Service (QoS), and increased number of available IP addresses.

The Cisco Unified IP Phones support IPv4 only addressing mode, IPv6 only addressing mode, as well as an IPv4/IPv6 dual stack addressing mode. In IPv4, you can enter each octet of the IP address on the phone in dotted decimal notation; for example, 192.240.22.5. In IPv6, you can enter each octet of the IP address in hexadecimal notation with each octet separated by a colon; for example, 2005:db8:0:1:ef8:9876:ba72:dc9a. The phone truncates and removes leading zeros when it displays the IPv6 address.

Cisco Unified IP Phones support both IPv4 and an IPv6 address transparently, so users can handle all calls on the phone to which they are accustomed. Cisco Unified IP Phones with the Skinny Call Control Protocol (SCCP) support IPv6. Cisco Unified IP Phones with SIP do not support IPv6.

Cisco Unified IP Phones do not support URLs with IPv6 addresses in the URL. This affects all IP Phone Service URLs, including services, directories, messages, help, and any restricted web services that require the phone to use the HTTP protocol to validate the credentials with the Authentication URL. If you configure Cisco Unified IP Phone services for Cisco IP Phones, you must configure the phone and the servers that support the phone service with IPv4 addresses.

If you configure IPv6 Only as the IP Addressing Mode for phones that are running SIP, the Cisco TFTP service overrides the IP Addressing Mode configuration and uses IPv4 Only in the configuration file.

For more information on deploying IPv6 in your Cisco Unified Communications network, see Internet Protocol Version 6 (IPv6) in *Cisco Unified Communications Manager Features and Services Guide* and *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager.*

Related Topics

- Understanding Interactions with Other Cisco Unified IP Telephony Products, page 2-1
- Understanding the Phone Startup Process, page 2-7
- Network Configuration Menu, page 4-5

What Features are Supported on the Cisco Unified IP Phone 7962G and 7942G?

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 Phones include features that enable you to administer and monitor the phone as a network device.

This section includes the following topics:

- Feature Overview, page 1-10
- Configuring Telephony Features, page 1-10
- Configuring Network Parameters Using the Cisco Unified IP Phones, page 1-11
- Providing Users with Feature Information, page 1-11

Feature Overview

Cisco Unified IP Phones provide traditional telephony functionality, such as call forward, call transfer, redial, speed dial, conference call, and voice message system access. Cisco Unified IP Phones also provide a variety of other features. For an overview of the telephony features that the Cisco Unified IP Phones support and for tips on configuring them, see Telephony Features Available for the Cisco Unified IP Phone, page 5-1.

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

Cisco Unified IP Phones can interact with other services and devices on your IP network to provide enhanced functionality. For example, you can integrate the Cisco Unified IP Phones 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. For information about configuring such services, see Configuring Corporate Directories, page 5-24 and Setting Up Services, page 5-28.

Finally, because the Cisco Unified IP Phones are network devices, you can obtain detailed status information from it directly. This information can assist you with troubleshooting many problems users might encounter when using their Cisco Unified IP Phones. See Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phones for more information.

Related Topics

- Configuring Settings on the Cisco Unified IP Phones, page 4-1
- Configuring Features, Templates, Services, and Users, page 5-1
- Troubleshooting and Maintenance, page 9-1

Configuring Telephony Features

You can modify additional settings for the Cisco Unified IP Phones from Cisco Unified Communications Manager Administration. Use this web-based application to set up phone registration criteria and calling search spaces, to configure corporate directories and services, and to modify phone button templates, among other tasks. See Telephony Features Available for the Cisco Unified IP Phone, page 5-1 and the Cisco Unified Communications Manager documentation for additional information.

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 Topic

- Telephony Features Available for the Cisco Unified IP Phone, page 5-1

Configuring Network Parameters Using the Cisco Unified IP Phones

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

For more information about configuring features and viewing statistics from the phone, see Configuring Settings on the Cisco Unified IP Phones and Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phones.

Providing Users with Feature Information

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

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

From this site, you can view various user guides.

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

For a summary of some of the key information that phone users need their system administrators to provide, see Appendix A, Providing Information to Users Via a Website.

Understanding Security Features for Cisco Unified IP Phones

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

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

The Cisco Unified IP Phone 7962G and 7942G use the Phone security profile, which defines whether the device is nonsecure, authenticated, 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 contains 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 in *Cisco Unified Communications Manager Security Guide.*

Table 1-3 shows where you can find additional information about security in this and other documents.

Table 1-3 Cisco Unified IP Phones 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 Phones	See Overview of Supported Security Features, page 1-13
Restrictions regarding security features	See Security Restrictions, page 1-21
Viewing a security profile name	See Understanding Security Profiles, page 1-15
Identifying phone calls for which security is implemented	See Identifying Authenticated, Encrypted, and Protected Phone Calls, page 1-15
TLS connection	See these sections: • What Networking Protocols are Used?, page 1-5 • Adding Phones to the Cisco Unified Communications Manager Database, page 2-8
Security and the phone startup process	See Understanding the Phone Startup Process, page 2-7
Security and phone configuration files	See Adding Phones to the Cisco Unified Communications Manager Database, page 2-8
Changing the TFTP Server 1 or TFTP Server 2 option on the phone when security is implemented.	See Table 4-2, in Network Configuration Menu, page 4-5
Understanding security icons in the Unified CM1 through Unified CM5 options in the Device Configuration Menu on the phone	See Unified CM Configuration Menu, page 4-19
Items on the Security Configuration menu that you access from the Device Configuration menu on the phone	See Security Configuration Menu, page 4-32
Items on the Security Configuration menu that you access from the Settings menu on the phone	See Security Configuration Menu, page 4-39
Unlocking the CTL and ITL files	See Unlocking the CTL and ITL Files section on page 4-41
Disabling access to a phone's web pages	See Disabling and Enabling Web Page Access, page 7-3
Deleting the CTL file from the phone	See Resetting or Restoring the Cisco Unified IP Phones, page 9-13
Resetting or restoring the phone	See Resetting or Restoring the Cisco Unified IP Phones, page 9-13

Table 1-3 Cisco Unified IP Phones and Cisco Unified Communications Manager Security Topics (continued)

Topic	Reference
Cisco Extension Mobility HTTPS support	See What Networking Protocols are Used?, page 1-5
802.1X Authentication for Cisco Unified IP Phones	See these sections: • Supporting 802.1X Authentication on Cisco Unified IP Phones, page 1-19 • Security Configuration Menu, page 4-32 • Status Menu, page 8-2 • Troubleshooting Cisco Unified IP Phone Security, page 9-9

Overview of Supported Security Features

Table 1-4 provides an overview of the security features that the Cisco Unified IP Phones 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 **Settings > Security Configuration** and choose **Settings > Device Configuration > Security Configuration**. For more information, see Security Configuration Menu, page 4-32.

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 in *Cisco Unified Communications Manager Security Guide*.

Table 1-4 Overview of Security Features

Feature	Description
Image authentication	Signed binary files (with the extension .sbn) prevent tampering with the firmware image before it is loaded on a phone. Tampering with the image causes a phone to fail the authentication process and reject the new image.
Customer-site certificate installation	Each Cisco Unified IP Phone requires a unique certificate for device authentication. Phones include a manufacturing installed certificate (MIC), but for additional security, you can specify in Cisco Unified Communications Manager Administration that a certificate be installed by using the Certificate Authority Proxy Function (CAPF). Alternatively, you can install a Locally Significant Certificate (LSC) from the Security Configuration menu on the phone. See Configuring Security on the Cisco Unified IP Phones, page 3-15 for more information.
Device authentication	Occurs between the Cisco Unified Communications Manager server and the phone when each entity accepts the certificate of the other entity. Determines whether a secure connection between the phone and a Cisco Unified Communications Manager should occur, and if necessary, creates a secure signaling path between the entities by using TLS protocol. Cisco Unified Communications Manager will not register phones unless they can be authenticated by the Cisco Unified Communications Manager.

Table 1-4 Overview of Security Features (continued)

Feature	Description
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 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 an 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 and SIP 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.
Security profiles	Defines whether the phone is nonsecure, authenticated, encrypted, or protected. See Understanding Security Profiles, page 1-15 for more information.
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's web page, which displays a variety of operational statistics for the phone.

Table 1-4 Overview of Security Features (continued)

Feature	Description
Phone hardening	Additional security options, which you control from Cisco Unified Communications Manager Administration: • Disabling PC port • Disabling Gratuitous ARP (GARP) • Disabling PC Voice VLAN access • Disabling access to the Setting menus, or providing restricted access that allows access to the User Preferences menu and saving volume changes only • 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's Security Configuration menu. For more information, see Device Configuration Menu, page 4-18.
802.1X Authentication	The Cisco Unified IP Phone can use 802.1X authentication to request and gain access to the network. See Supporting 802.1X Authentication on Cisco Unified IP Phones, page 1-19 for more information.

Related Topics

- Understanding Security Profiles, page 1-15
- Identifying Authenticated, Encrypted, and Protected Phone Calls, page 1-15
- Security Restrictions, page 1-21
- Device Configuration Menu, page 4-18

Understanding Security Profiles

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

To view the phone security mode, look at the Security Mode setting in the Security Configuration menu. For more information, see Security Configuration Menu, page 4-32.

Related Topics

- Identifying Authenticated, Encrypted, and Protected Phone Calls, page 1-15
- Security Restrictions, page 1-21
- Device Configuration Menu, page 4-18

Identifying Authenticated, Encrypted, and Protected Phone Calls

When security is implemented for a phone, you can identify authenticated or 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 an authenticated call, all devices participating in the establishment of the call are trusted devices, and authenticated by Cisco Unified Communications Manager. When an in-progress call is authenticated, the call progress icon to the right of the call duration timer in the phone LCD screen changes to this icon: 

In an encrypted call, all devices participating in the establishment of the call are trusted devices, and authenticated by Cisco Unified Communications Manager. In addition, call signaling and media streams are encrypted. An encrypted call offers a high level of security, providing integrity and privacy to the call. When an in-progress call is being encrypted, the call progress icon to the right of the call duration timer in the phone LCD screen changes to this icon: 

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

In a protected 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 Protected calling is supported for connections between two phones only. Some features, such as conference calls, shared lines, Extension Mobility, and Join Across Lines are not available when protected calling is configured. Protected calls are not authenticated.

Related Topic

- Understanding Security Profiles, page 1-15
- Understanding Security Features for Cisco Unified IP Phones, page 1-11
- Security Restrictions, page 1-21

Establishing and Identifying Secure Conference Calls

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

1. A user initiates the conference from a secure phone (encrypted or authenticated security mode).
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 (encrypted or authenticated) and maintains the secure level for the conference.
4. The phone displays the security level of the conference call. A secure conference displays  (encrypted) or  (authenticated) icon to the right of “Conference” on the phone screen. If  icon displays, the conference is not secure.

Note There are interactions, restrictions, and limitations that affect the security level of the conference call depending on the security mode of the participants' phones and the availability of secure conference bridges. See Table 1-5 and Table 1-6 for information about these interactions.

Establishing and Identifying Protected Calls

A protected call is established when your phone, and the phone on the other end, is 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 non-protected phone, then the secure tone does not play.

Note Protected calling is supported for conversations between two phones. Some features, such as conference calls, 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. Table 1-5 provides information about changes to call security levels when using Barge.

Table 1-5 Call Security Interactions When Using Barge

Initiator's Phone Security Level	Feature Used	Call Security Level	Results of Action
Non-secure	Barge	Encrypted call	Call barged and identified as non-secure call
Secure (encrypted)	Barge	Authenticated call	Call barged and identified as authenticated call
Secure (authenticated)	Barge	Encrypted call	Call barged and identified as authenticated call
Non-secure	Barge	Authenticated call	Call barged and identified as non-secure call

Table 1-6 provides information about changes to conference security levels depending on the initiator's phone security level, the security levels of participants, and the availability of secure conference bridges.

Table 1-6 Security Restrictions with Conference Calls

Initiator's Phone Security Level	Feature Used	Security Level of Participants	Results of Action
Non-secure	Conference	Encrypted or authenticated	Non-secure conference bridge Non-secure conference
Secure (encrypted or authenticated)	Conference	At least one member is non-secure	Secure conference bridge Non-secure conference
Secure (encrypted)	Conference	All participants are encrypted	Secure conference bridge Secure encrypted level conference
Secure (authenticated)	Conference	All participants are encrypted or authenticated	Secure conference bridge Secure authenticated level conference
Non-secure	Conference	Encrypted or authenticated	Only secure conference bridge is available and used Non-secure conference
Secure (encrypted or authenticated)	Conference	Encrypted or authenticated	For Cisco Unified IP Phones 7962G and 7942G: • Only non-secure conference bridge is available and used • Non-secure conference For Cisco Unified IP Phones 7961G and 7941G: • Conference remains secure • When one participant tries to Hold the call with MOH, the MOH does not play.
Secure (encrypted or authenticated)	Conference	For Cisco Unified IP Phones 7962G and 7942G: • Encrypted or secure For Cisco Unified IP Phones 7961G and 7941G: • Member puts call on Hold with MOH	For Cisco Unified IP Phones 7962G and 7942G: • Conference remains secure. When one participant tries to hold the call with MOH, the MOH does not play. For Cisco Unified IP Phones 7961G and 7941G: • No music on hold is played • Conference remains secure.
Secure (encrypted)	Join	Encrypted or authenticated	Secure conference bridge Conference remains secure (encrypted or authenticated)
Non-secure	cBarge	All participants are encrypted	Secure conference bridge Conference changes to non-secure
Non-secure	MeetMe	Minimum security level is encrypted	Initiator receives message "Does not meet Security Level" and the call is rejected.

Table 1-6 Security Restrictions with Conference Calls (continued)

Initiator's Phone Security Level	Feature Used	Security Level of Participants	Results of Action
Secure (encrypted)	MeetMe	Minimum security level is authenticated	Secure conference bridge Conference accepts encrypted and authenticated calls
Secure (encrypted)	MeetMe	Minimum security level is non-secure	Only secure conference bridge available and used Conference accepts all calls

Supporting 802.1X Authentication on Cisco Unified IP Phones

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

Overview

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

In conjunction with the EAPOL pass-through mechanism, Cisco Unified IP Phones provide a proxy EAPOL-Logoff mechanism. In the event that the locally attached PC disconnects from the Cisco Unified IP Phone, the LAN switch does see the physical link fail, because the link between the LAN switch and the Cisco Unified IP Phone is maintained. To avoid compromising network integrity, the IP Phone sends an EAPOL-Logoff message to the switch on behalf of the downstream PC, which triggers the LAN switch to clear the authentication entry for the downstream PC.

The Cisco Unified IP Phones also contain an 802.1X supplicant, in addition to the EAPOL pass-through mechanism. This supplicant allows network administrators to control the connectivity of Cisco Unified IP Phones to the LAN switch ports. 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 Phones—The phone acts as the 802.1X *supplicant*, which initiates the request to access the network.
- Cisco Secure Access Control Server (ACS) (or other third-party authentication server)—The authentication server and the phone must both be configured with a shared secret that is used to authenticate the phone.

- Cisco Catalyst Switch (or other third-party switch)—The switch must support 802.1X, so it can act as the *authenticator* and pass the messages between the phone and the authentication server. When the exchange 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. See 802.1X Authentication and Status, page 4-44 for more information.
- Configure PC Port—The 802.1X standard does not take into account the use of VLANs and thus recommends that only a single device should authenticate to a specific switch port. However, some switches (including Cisco Catalyst switches) support multi-domain authentication. The switch configuration determines whether you can connect a PC to the phone's PC port.
  - Enabled—If you are using a switch that supports multi-domain authentication, you can enable the PC port and connect a PC to it. In this case, Cisco Unified IP Phones support proxy EAPOL-Logoff to monitor the authentication exchanges between the switch and the attached PC. For more information about IEEE 802.1X support on the Cisco Catalyst switches, see the Cisco Catalyst switch configuration guides at:

    http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
  - Disabled—If the switch does not support multiple 802.1X-compliant devices on the same port, you should disable the PC Port when 802.1X authentication is enabled. See Security Configuration Menu, page 4-32 for more information. If you do not disable this port and subsequently attempt to attach a PC to it, the switch will deny network access to both the phone and the PC.
- Configure Voice VLAN—Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.
  - Enabled—If you are using a switch that supports multi-domain authentication, you can continue to use the voice VLAN.
  - Disabled—If the switch does not support multi-domain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN. See Security Configuration Menu, page 4-32 for more information.
- Enter MD5 Shared Secret—If you disable 802.1X authentication or perform a factory reset on the phone, the previously configured MD5 shared secret is deleted. See 802.1X Authentication and Status, page 4-44 for more information.

Security Restrictions

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

If the initiator phone is configured for encryption, the barge initiator can barge into an authenticated or 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.

A user can barge into an authenticated call, even if the phone that is used to barge is nonsecure. The authentication icon continues to appear on the authenticated devices in the call, even if the initiator phone does not support security.

Reducing Power Consumption on the Phones

The Cisco Unified IP Phones support Cisco EnergyWise (EW). EnergyWise is also known as Power Save Plus. When your network contains an EnergyWise controller, you can configure these phones to sleep (power down) and wake (power up) on a schedule to reduce your power consumption. The phone is powered with switch's Power over Ethernet (PoE) port instead of the power adapter.

You set up each phone to enable or disable the EnergyWise settings. You can also configure EnergyWise parameters on the enterprise and common phone configuration. If EnergyWise is enabled, you 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.

The switch administrator can wake the phone up before the scheduled time. For more information on powering up the phones from the switch, see the switch documentation.

Overview of Configuring and Installing Cisco Unified IP Phones

When deploying a new IP telephony system, system administrators and network administrators must complete several initial configuration tasks to prepare the network for IP telephony service. For information and a checklist for setting up and configuring a complete Cisco IP telephony network, see System Configuration Overview 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 Cisco Unified IP Phones to the system.

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

- Configuring Cisco Unified IP Phones in Cisco Unified Communications Manager, page 1-21
- Installing Cisco Unified IP Phones, page 1-25

Configuring Cisco Unified IP Phones in Cisco Unified Communications Manager

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

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

For more information about these choices, see Adding Phones to the Cisco Unified Communications Manager Database, page 2-8.

For general information about configuring phones in Cisco Unified Communications Manager, see Cisco Unified IP Phones in *Cisco Unified Communications Manager System Guide*.

Checklist for Configuring the Cisco Unified IP Phones in Cisco Unified Communications Manager Administrations

Table 1-7 provides an overview and checklist of configuration tasks for the Cisco Unified IP Phones in Cisco Unified Communications Manager Administration. The list presents a suggested order to guide you through the phone configuration process. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, see the sources in the list.

Table 1-7 Checklist for Configuring the Cisco Unified IP Phone 7962G and 7942G in Cisco Unified Communications Manager

Task	Purpose	For More Information
1.	Gather the following information about the phone: • Phone Model • MAC address • Physical location of the phone • Name or user ID of phone user • Device pool • Partition, calling search space, and location information • Number of lines and associated directory numbers (DNs) to assign to the phone • Cisco Unified Communications Manager user to associate with the phone • Phone usage information that affects phone button template, softkey template, phone features, IP Phone services, or phone applications Provides list of configuration requirements for setting up phones. Identifies preliminary configuration that you need to perform before configuring individual phones, such as phone button templates or softkey templates.	See these sections: • See *Cisco Unified Communications Manager System Guide,* Cisco Unified IP Phones. • See Telephony Features Available for the Cisco Unified IP Phone, page 5-1.
2.	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. You must specify a service URL with an IPv4 address.	See these sections: • *Cisco Communications Manager Administration Guide*, Phone Button Template Configuration. • Modifying Phone Button Templates, page 5-25.
3.	Add and configure the phone by completing the required fields in the Phone Configuration window. Required fields are indicated by an asterisk (*) next to the field name; for example, MAC address and device pool. Adds the device with its default settings to the Cisco Unified Communications Manager database.	See *Cisco Communications Manager Administration Guide*, Cisco Unified IP Phone Configuration. For information about Product Specific Configuration fields, see "?" Button Help in the Phone Configuration window.
4.	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.	See these sections: • See *Cisco Unified Communications Manager Administration Guide*, Directory Number Configuration. • See Telephony Features Available for the Cisco Unified IP Phone, page 5-1.

Table 1-7 Checklist for Configuring the Cisco Unified IP Phone 7962G and 7942G in Cisco Unified Communications Manager (continued)

Task	Purpose	For More Information
5.	Customize softkey templates. Adds, deletes, or changes order of softkey features that display on the user's phone to meet feature usage needs.	See *Cisco Unified Communications Manager Administration Guide*, Softkey Template Configuration. See Configuring Softkey Templates, page 5-27.
6.	Configure speed-dial buttons and assign speed-dial numbers (optional). Adds speed-dial buttons and numbers. **Note** Users can change speed-dial settings on their phones by using Cisco Unified CM User Options.	See *Cisco Unified Communications Manager Administration Guide*, Cisco Unified IP Phone Configuration chapter, Configuring Speed-Dial Buttons section.
7.	Configure Cisco Unified IP Phone services and assign services (optional). Provides IP Phone services. **Note** Users can add or change services on their phones by using the Cisco Unified CM User Options. **Note** You must specify a service URL with an IPv4 address.	See these sections: • See *Cisco Communications Manager Administration Guide*, Cisco Unified IP Phone Services Configuration. • See Setting Up Services, page 5-28.
8.	Assign services to phone buttons (optional). Provides single button access to an IP Phone service or URL.	See *Cisco Unified Communications Manager Administration Guide*, Cisco Unified IP Phone Configuration.
9.	Add user information by configuring required fields. Required fields are indicated by an asterisk (*); for example, User ID and last name. **Note** Assign a password (for User Options web pages) and PIN (for Extension Mobility and Personal Directory). Adds user information to the global directory for Cisco Unified Communications Manager.	See *Cisco Unified Communications Manager Administration Guide*, End User Configuration. See Adding Users to Cisco Unified Communications Manager, page 5-28. **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, see Configuring Corporate Directories, page 5-24. **Note** If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, see the User/Phone Add Configuration chapter in the *Cisco Unified Communications Manager Administration Guide*.

Table 1-7 Checklist for Configuring the Cisco Unified IP Phone 7962G and 7942G in Cisco Unified Communications Manager (continued)

Task	Purpose	For More Information
10.	Add a user to a user group. Assigns to 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.	See *Cisco Unified Communications Manager Administration Guide*: • End User Configuration. • User Group Configuration.
11.	Associate a user with a phone (optional). Provides users with control over their phone such a forwarding calls or adding speed-dial numbers or services. **Note** Some phones, such as those in conference rooms, do not have an associated user.	See *Cisco Unified Communications Manager Administration Guide*, End User Configuration.

Installing Cisco Unified IP Phones

After you have added the phones to the Cisco Unified Communications Manager database, you can complete the phone installation. You can install the phones at the desired location, or you can give the phone users the information they need to do perform the installation. The Cisco Unified IP Phone Installation Guide, which is available at http://www.cisco.com, provides directions for connecting the phone handset, cables, and other accessories.

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

http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser

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

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

Checklist for Installing the Cisco Unified IP Phones

Table 1-8 provides an overview and checklist of installation tasks for the Cisco Unified IP Phones. The list presents a suggested order to guide you through the phone installation. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, see the sources in the list.

Table 1-8 Checklist for Installing the Cisco Unified IP Phones

Task	Purpose	For More Information
1.	Choose the power source for the phone: • Power over Ethernet (PoE) • External power supply Determines how the phone receives power.	See Providing Power to the Cisco Unified IP Phones, page 2-3.
2.	Assemble the phone, adjust phone placement, and connect the network cable. Locates and installs the phone in the network.	See Installing the Cisco Unified IP Phones, page 3-6. See Feature Key Capacity Increase for Cisco Unified IP Phones, page 3-10.
3.	Add a Cisco Unified IP Phone Expansion Module: Adds the device with its default settings to the Cisco Unified Communications Manager database. Extends functionality of a Cisco Unified IP Phone 7962G by adding 14 (7914) or 24 (7915 and 7916) line appearances or speed-dial numbers. Extends functionality of a Cisco Unified IP Phones 7961G and 7961G-GE by adding 14 (7914) line appearances or speed-dial numbers. **Note** Cisco Unified IP Phone Expansion Module 7914 is not supported on the Cisco Unified IP Phones 7942G, 7941G, and 7941G-GE. **Note** Cisco Unified IP Phone Expansion Modules 7915 and 7916 are not supported on the Cisco Unified IP Phones 7942G, 7961G, 7961G-GE, 7941G, and 7941G-GE. **Note** Up to 54 keys can be configured for Cisco Unified IP Phones 7962G.	See Attaching a Cisco Unified IP Phone Expansion Module, page 3-9.
4.	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 Verifying the Phone Startup Process, page 3-14.

Table 1-8 Checklist for Installing the Cisco Unified IP Phones (continued)

Task	Purpose	For More Information
5.	If you are configuring the network settings on the phone for an IPv4 network, you can set up an IP address for the phone by either using DHCP or manually entering an IP address. Using DHCP—To enable DHCP and allow the DHCP server to automatically assign an IP address to the Cisco Unified IP Phone and direct the phone to a TFTP server, choose **Settings > Network Configuration> IPv4 Configuration** and configure the following: • To enable DHCP, set DHCP Enabled to **Yes.** DHCP is enabled by default. • To use an alternate TFTP server, set Alternate TFTP Server to **Yes,** and enter the IP address for the TFTP Server. **Note** Consult with the network administrator to determine whether you need to assign an alternative TFTP server instead of using the TFTP server assigned by DHCP. Without DHCP—You must configure the IP address, subnet mask, TFTP server, and default router locally on the phone, choose **Settings > Network Configuration> IPv4 Configuration**: To disable DHCP and manually set an IP address: **a.** To disable DHCP, set DHCP Enabled to **No**. **b.** Enter the static IP address for phone. **c.** Enter the subnet mask. **d.** Enter the default router IP addresses. **e.** Set Alternate TFTP Server to **Yes**, and enter the IP address for TFTP Server 1. You must also enter the domain name where the phone resides by Choosing **Settings > Network Configuration**. The Cisco Unified IP Phones support having both IPv4 and an IPv6 address concurrently. You can configure Cisco Unified Communications Manager to support IPv4 addresses only, IPv6 addresses only, or support both IPv4/IPv6 addresses.	See Configuring Startup Network Settings, page 3-15. See Network Configuration Menu, page 4-5.

Table 1-8 Checklist for Installing the Cisco Unified IP Phones (continued)

Task	Purpose	For More Information
6.	If you are configuring the network settings on the phone for an IPv6 network, you can set up an IP address for the phone by either using DHCPv6 or by manually entering an IP address. Using DHCPv6—To enable DHCPv6 and allow the DHCPv6 server to automatically assign an IP address to the Cisco Unified IP Phone and direct the phone to a TFTP server, choose **Settings > Network Configuration> IPv6 Configuration** and configure the following: • To enable DHCPv6, set DHCPv6 to **Yes.** DHCPv6 is enabled by default. • To use an alternate TFTP server, set IPv6 Alternate TFTP Server to **Yes**, and enter the IP address for IPv6 TFTP Server 1. **Note** Consult with the network administrator if you need to assign an alternate TFTP server instead of using the TFTP server assigned by DHCP. Without DHCP—You must configure the IP address, subnet mask and TFTP server locally on the phone, choose **Settings > Network Configuration> IPv6 Configuration**: To disable DHCP and manually set an IP address: **a.** To disable DHCPv6, set DHCPv6 to **No**. **b.** Enter the static IP address for phone. **c.** Enter the IPv6 prefix length. **d.** Set IPv6 Alternate TFTP Server to **Yes**, and enter IP address for IPv6 TFTP Server 1. You must also enter the domain name where the phone resides by Choosing **Settings > Network Configuration.** **Note** The Cisco Unified IP Phones support having both IPv4 and an IPv6 address concurrently. You can configure Cisco Unified Communications Manager to support IPv4 devices only, IPv6 devices only, or to support both IPv4 and IPv6 devices concurrently.	See Configuring Startup Network Settings, page 3-15. See Network Configuration Menu, page 4-5.
7.	Set up security on the phone. Provides protection against data tampering threats and identity theft of phones.	See Configuring Security on the Cisco Unified IP Phones, page 3-15.
8.	Make calls with the Cisco Unified IP Phones. Verifies that the phone and features work correctly.	See *Cisco Unified IP Phone 7962G, 7942G, 7961G, 7961G-GE, 7941G, and 7941G-GE User Guide.*
9.	Provide information to end users about how to use their phones and how to configure their phone options. Ensures that users have adequate information to successfully use their Cisco Unified IP Phones.	See Appendix A, Providing Information to Users Via a Website.

CHAPTER 2

Preparing to Install the Cisco Unified IP Phones on Your Network

Cisco Unified IP Phones enable you to communicate by using voice over a data network. To provide this capability, the Cisco Unified 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 Phones and Cisco Unified Communications Manager, DNS, DHCP, and TFTP servers, and switches. It also describes options for powering phones.

For related information about voice and IP communications, see:

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

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

Understanding Interactions with Other Cisco Unified IP Telephony Products

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

This section includes the following topics:

Understanding How the Cisco Unified IP Phones Interact with Cisco Unified Communications Manager

Cisco Unified Communications Manager is an open and industry-standard call processing system. Cisco Unified Communications Manager software sets up and tears down calls between phones, integrating traditional PBX functionality with the corporate IP network. Cisco Unified Communications Manager manages the components of the IP telephony system—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
- Authentication and encryption (if configured for the telephony system)
- Configuration, certificate trust list (CTL), and Identity Trust List (ITL) files via the TFTP service
- Phone registration
- Call preservation, so that a media session continues if signaling is lost between the primary Communications Manager and a phone

For information about configuring Cisco Unified Communications Manager to work with the IP devices described in this chapter, refer to *Cisco Unified Communications Manager Administration Guide*, *Cisco Unified Communications Manager System Guide*, and *Cisco Unified Communications Manager Security Guide.*

For an overview of security functionality for the Cisco Unified IP Phones, see Understanding Security Features for Cisco Unified IP Phones, page 1-11.

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

Related Topic

Telephony Features Available for the Cisco Unified IP Phone, page 5-1

Understanding How the Cisco Unified IP Phones Interact with the VLAN

The Cisco Unified IP Phones 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 VoIP traffic.
- Network security may 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 phone (auxiliary VLAN on the Cisco Catalyst 6000 series, for example)
- Data traffic to and from the PC connected to the switch through the access port of the phone (native VLAN)

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

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

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

Related Topics

- Understanding the Phone Startup Process, page 2-7
- Network Configuration Menu, page 4-5

Providing Power to the Cisco Unified IP Phones

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

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

The following sections provide more information about powering a phone:

- Power Guidelines, page 2-4
- Power Outage, page 2-4
- Obtaining Additional Information about Power, page 2-5

Power Guidelines

Table 2-1 provides guidelines for powering the Cisco Unified IP Phones.

Table 2-1 Guidelines for Powering the Cisco Unified IP Phones

Power Type	Guidelines
External power—Provided through the CP-PWR-CUBE-3 external power supply.	• The Cisco Unified IP Phones 7962G, 7942G, 7961G, and 7941G use the CP-PWR-CUBE-3 power supply. • The Cisco Unified IP Phones 7961G-GE and 7941G-GE use the CP-PWR-CUBE-3 external power supply only.
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 Phones 7962G, 7942G, 7961G, and 7941G support Cisco inline PoE, but the Cisco Unified IP Phones 7961G-GE, and 7941G-GE do not. • The Cisco Unified IP Phones 7962G and 7942G support IEEE 802.3af Class 2 power on signal pairs and spare pairs. The Cisco Unified IP Phones 7961G-GE, and 7941G-GE are not compatible with Cisco switches that are not IEEE compliant. • 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 Outage

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

Obtaining Additional Information about Power

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

- Cisco switches that work with the Cisco Unified IP Phones
- The Cisco IOS releases that support bidirectional power negotiation
- Other requirements and restrictions regarding power

Table 2-2 Related Documentation for Power

Document Topics	URL
Cisco Unified IP Phones Power Injector	http://www.cisco.com/en/US/products/ps6951/index.html
PoE Solutions	http://www.cisco.com/en/US/netsol/ns340/ns394/ns147/ns412/networking_solutions_package.html
Cisco Catalyst Switches	http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
Integrated Service Routers	http://www.cisco.com/en/US/products/hw/routers/index.html
Cisco IOS Software	http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.html

Understanding Phone Configuration Files

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

Configuration files also contain information about which image load the phone should be running. If this image load differs from the one currently loaded on a phone, the phone contacts the TFTP server to request the required load files. These load files are digitally signed to ensure the authenticity of the files' source.

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. For SIP phones, a TLS connection requires that the transport protocol in the phone configuration file be set to TLS, which corresponds to the transport type in the SIP Security Profile in Cisco Unified Communications Manager Administration.

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

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-related settings in Cisco Unified Communications Manager Administration, the phone configuration file contains sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For detailed information, refer to Configuring Encrypted Phone Configuration Files 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 accesses the configuration file named SEPmac_address.cnf.xml, where mac_address is the MAC address of the phone.

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, see *Cisco Unified Communications Manager Administration Guide*.

Understanding the Phone Startup Process

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

Table 2-3 Cisco Unified IP Phone Startup Process

Task	Purpose	Related Topics
1.	Obtaining Power from the Switch If a phone is not using external power, the switch provides in-line power through the Ethernet cable attached to the phone.	• Adding Phones to the Cisco Unified Communications Manager Database, page 2-8. • Resolving Startup Problems, page 9-1.
2.	Loading the Stored Phone Image The Cisco Unified IP Phone has non-volatile Flash memory in which it stores firmware images and user-defined preferences. At startup, the phone runs a bootstrap loader that loads a phone image stored in Flash memory. Using this image, the phone initializes its software and hardware.	• Resolving Startup Problems, page 9-1.
3.	Configuring 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.	• Network Configuration Menu, page 4-5. • Resolving Startup Problems, page 9-1.
4.	Obtaining 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 your network does not use DHCP, you must assign static IP addresses to each phone locally.	• Network Configuration Menu, page 4-5. • Resolving Startup Problems, page 9-1.
5.	Accessing 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.	• Network Configuration Menu, page 4-5. • Resolving Startup Problems, page 9-1.
6.	Requesting the CTL file The TFTP server stores the certificate trust list (CTL) file. This file contains the certificates necessary for establishing a secure connection between the phone and Cisco Unified Communications Manager.	Refer to *Cisco Unified Communications Manager Security Guide*, Configuring the Cisco CTL Client.

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

Task	Purpose	Related Topics
7.	Requesting the ITL file. The phone requests the ITL file after it requests the CTL file. The ITL file contains the certificates of the entities that the phone can trust. The certificates are used for authenticating a secure connection with the servers or authenticating a digital signature signed by the servers.	Refer to *Cisco Unified Communications Manager Security Guide*, Security by Default.
8.	Requesting the Configuration File The TFTP server has configuration files, which define parameters for connecting to Cisco Unified Communications Manager and other information for the phone.	• Adding Phones to the Cisco Unified Communications Manager Database, page 2-8. • Resolving Startup Problems, page 9-1.
9.	Contacting 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. When security is implemented, if the security profile of the phone is configured for secure signaling (encrypted or authenticated), and the Cisco Unified Communications Manager is set to secure mode, the phone makes a TLS connection. Otherwise, it makes a nonsecure TCP connection. If the phone was manually added to the database, Cisco Unified Communications Manager identifies the phone. If the phone was not manually added to the database and auto-registration is enabled in Cisco Unified Communications Manager, the phone attempts to auto-register itself in the Cisco Unified Communications Manager database. **Note** Auto-registration is disabled when you configure the CTL client. In this case, the phone must be manually added to the Cisco Unified Communications Manager database.	• Resolving Startup Problems, page 9-1.

Adding Phones to the Cisco Unified Communications Manager Database

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

- Adding Phones with Auto-Registration, page 2-9

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

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

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

Method	Requires MAC Address?	Notes
Auto-registration	No	• Results in automatic assignment of directory numbers. • Not available when security or encryption is enabled.
Auto-registration with TAPS	No	Requires auto-registration and the Bulk Administration Tool (BAT); updates information in the Cisco Unified IP Phone and in Cisco Unified Communications Manager Administration.
Using the Cisco Unified Communications Manager Administration	Yes	Requires phones to be added individually.
Using BAT	Yes	Allows for simultaneous registration of multiple phones.

Adding Phones with Auto-Registration

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

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

Note We recommend that you use auto-registration to add less than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT). See Adding Phones with BAT, page 2-11.

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

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

Related Topics

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

Adding Phones with Auto-Registration and TAPS

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

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

Note We recommend that you use auto-registration and TAPS to add less than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT). See Adding Phones with BAT, page 2-11.

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

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

Note When you configure the cluster for mixed mode through the Cisco CTL client, auto-registration is automatically disabled. When you configure the cluster for non-secure mode through the Cisco CTL client, auto-registration is automatically enabled.

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

Related Topics

- Adding Phones with Auto-Registration, page 2-9
- Adding Phones with Cisco Unified Communications Manager Administration, page 2-11
- Adding Phones with BAT, page 2-11

Adding Phones with Cisco Unified Communications Manager Administration

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

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

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

For complete instructions and conceptual information about Cisco Unified Communications Manager, refer to *Cisco Unified Communications Manager Administration Guide* and to *Cisco Unified Communications Manager System Guide*.

Related Topics

- Adding Phones with Auto-Registration, page 2-9
- Adding Phones with Auto-Registration and TAPS, page 2-10
- Adding Phones with BAT, page 2-11

Adding Phones with BAT

Cisco Unified Communications Manager Bulk Administration Tool (BAT), a standard Cisco Unified Communications Manager application, enables you to perform batch operations, including registration, on multiple phones.

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

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

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

Procedure

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

Step 2 Click **Add New**.

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

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

Step 5 Click **Save**.

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

For more information on BAT, see *Cisco Unified Communications Manager Bulk Administration Guide*. For more information on creating BAT Phone Templates, see *Cisco Unified Communications Manager Bulk Administration Guide*, Phone Template.

Related Topics

- Adding Phones with Auto-Registration, page 2-9
- Adding Phones with Auto-Registration and TAPS, page 2-10
- Adding Phones with Cisco Unified Communications Manager Administration, page 2-11

Using Cisco Unified IP Phones with Different Protocols

The Cisco Unified IP Phones can operate with SCCP (Skinny Client Control Protocol) or SIP (Session Initiation Protocol). You can convert a phone from using one protocol to using the other protocol.

This section includes these topics:

- Converting a New Phone from SCCP to SIP, page 2-12
- Converting an In-Use Phone from One Protocol to the Other, page 2-13
- Deploying a Phone in an SCCP and SIP Environment, page 2-13

Converting a 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 auto-register the phone, set the Auto Registration Phone Protocol enterprise parameter in Cisco Unified Communications Manager Administration to SIP.
- To provision the phone by using the Bulk Administration Tool (BAT), choose the appropriate phone model and choose SIP from 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 on Cisco Unified Communications Manager configuration, see *Cisco Unified Communications Manager Administration Guide*. For more information on 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 Configuring Startup Network Settings, page 3-15.

Step 3 Save the configuration updates, click **Apply Config**, click **OK** in the Apply Configuration Information window, and have the user power cycle the phone.

Converting an In-Use Phone from One Protocol to the Other

For information on 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.

Deploying a Phone in an 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 Auto-Registration parameter is SCCP, perform these general steps:

1. Set the Cisco Unified Communications Manager Auto Registration Protocol enterprise parameter to SCCP.

   From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.
2. Install the phones.
3. Change the Auto Registration Protocol enterprise parameter to SIP.
4. Auto-register the SIP phones.

Determining the MAC Address for a Cisco Unified IP Phones

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

- From the phone, press the **Settings** button, select **Model Information** and look at the MAC Address field.
- Look at the MAC label on the back of the phone.
- Display the web page for the phone and click the **Device Information** hyperlink.

  For information about accessing the web page, see Accessing the Web Page for a Phone, page 7-2.

CHAPTER 3

Setting Up the Cisco Unified IP Phones

This chapter includes the following topics, which help you install the Cisco Unified IP Phones 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 Preparing to Install the Cisco Unified IP Phones on Your Network.

Before You Begin

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

Network Requirements

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

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

Note The Cisco Unified IP Phone displays the date and time from Cisco Unified Communications Manager. If the Cisco Unified Communications Manager server is located in a different time zone than the phones, the phones will not display the correct local time.

Cisco Unified Communications Manager Configuration

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

If you plan to use auto-registration, verify that it is enabled and properly configured in Cisco Unified Communications Manager before connecting any Cisco Unified IP Phone to the network. For information about enabling and configuring auto-registration, see *Cisco Unified Communications Manager Administration Guide*. Also, see Adding Phones to the Cisco Unified Communications Manager Database, page 2-8.

You must use Cisco Unified Communications Manager to configure and assign telephony features to the Cisco Unified IP Phones. See Telephony Features Available for the Cisco Unified IP Phone, page 5-1 for details.

In Cisco Unified Communications Manager, you can add users to the database and associate them with specific phones. In this way, users gain access to web pages that allow them to configure items such as call forward, speed dial, and voice message system options. See Adding Users to Cisco Unified Communications Manager, page 5-28 for details.

Understanding the Cisco Unified IP Phone Components

The Cisco Unified IP Phones include these components on the phone or as accessories for the phone:

Network and Access Ports

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

- Network port
  - Labeled 10/100 SW on the 7962G, 7942G, 7961G, and 7941G
  - Labeled 10/100/1000 SW on the 7961G-GE and 7941G-GE
- Access port
  - Labeled 10/100 PC on the 7962G, 7942G, 7961G, and 7941G
  - Labeled 10/100/1000 PC on the 7961G-GE and 7941G-GE

Each port supports 10/100 or 10/100/1000 Mbps half- or full-duplex connections to external devices.

- For the Cisco Unified IP Phones 7962G and 7942G, you can use either Category 3/5/5e cabling for 10-Mbps connections, but you must use Category 5 or 5e for 100 Mbps connections.
- For the Cisco Unified IP Phones 7961G, 7961G-GE, 7941G, and 7941G-GE, you can use either Category 3 or 5 cabling for 10-Mbps connections, but you must use Category 5 for 100 and 1000 Mbps connections.

Use the SW network port to connect the phone to the network. You must use a straight-through cable on this port. The phone can also obtain inline power from a switch over this connection. See Providing Power to the Cisco Unified IP Phones, page 2-3 for details.

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.

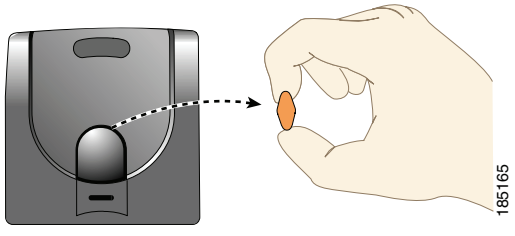
Handset

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

To connect the handset to the Cisco Unified IP Phones 7962G and 7942G, plug the cable into the handset and the Handset port on the back of the phone.

To connect the handset to the Cisco Unified IP Phones 7961G, 7961G-GE, 7941G, and 7941G-GE, remove the hookswitch clip (see Figure 3-1) from the cradle area. Then plug the cable into the handset and into the Handset port on the back of the phone.

Figure 3-1 Removing the Hookswitch Clip



Speakerphone

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

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

Headset

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

We recommend that 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. See Using External Devices, page 3-5, for more information.

Note In some cases, hum can 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.

We recommend 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 Phones support wideband headsets.

Audio Quality

Beyond its 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 more information, see http://www.cisco.com/en/US/partner/prod/voicesw/ucphone_headsets.html.

Connecting a Headset

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

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

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

Disabling a Headset

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

To disable the headset from Cisco Unified Communications Manager Administration, perform the following actions:

Procedure

Step 1 Choose **Device > Phone** and locate the phone that you want to modify.

Step 2 Check the **Disable Speakerphone and Headset** check box in the Phone Configuration window.

Enabling a Wireless Headset on the Cisco Unified IP Phones

By default, the Wireless Headset Hookswitch Control option is disabled. You can enable the option in the Cisco Unified Communications Manager Administration application.

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

Modifying the Headset Hookswitch Control

Procedure

Step 1 Choose **Device > Phone** and locate the phone you want to modify.

Step 2 Select **Enable** for Headset Hookswitch Control, in the Phone Configuration window.

Verifying the Wireless Headset Hookswitch Control

Procedure

Step 1 Choose **Settings > Device Configuration > Media Configuration** to verify that the feature is enabled.

Step 2 Select **Enable** to verify that the Wireless Headset Hookswitch Control is set.

Using External Devices

The following information applies when you use external devices with the Cisco Unified IP Phone.

We recommend the use of good quality external devices 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, We recommend 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 using good quality cables and connectors.

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

Installing the Cisco Unified IP Phones

You must connect the Cisco Unified IP Phone to the network and to a power source before using it. See Figure 3-2 for a graphical representation of the connections.

Note Before you install a phone, even if it is new, upgrade the phone to the current firmware image. Before using external devices, read the Using External Devices, page 3-5 for safety and performance information.

Before You Begin

Remove the hookswitch clip (see Handset, page 3-3) from the cradle area.

To install a Cisco Unified IP Phone, perform the tasks described in Table 3-1:

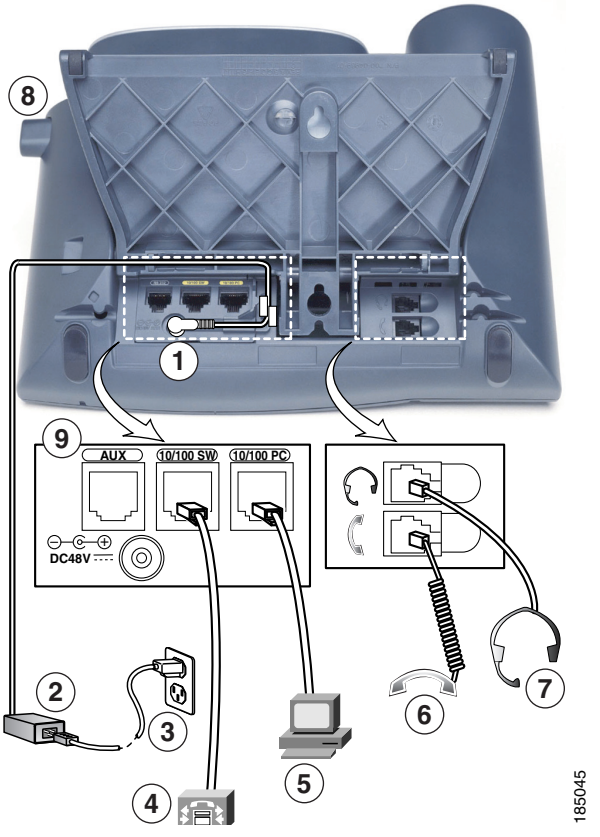
Table 3-1 Installing the Cisco Unified IP Phone 7962G and 7942G

Task	Purpose	Related Topics
1.	Connect the handset to the Handset port.	—
2.	Connect a headset to the Headset port. Optional. You can add a headset later if you do not connect one now.	See Headset, page 3-4 for supported headsets.
3.	(Cisco Unified IP Phones 7962G and 7942G only) Connect a wireless headset. Optional. You can add a wireless headset later if you do not want to connect one now.	See the wireless headset documentation for information.
4.	(Optional) Connect the power supply to the Cisco DC Adapter port.	See Adding Phones to the Cisco Unified Communications Manager Database, page 2-8 for guidelines.

Table 3-1 Installing the Cisco Unified IP Phone 7962G and 7942G (continued)

Task	Purpose	Related Topics
5.	Connect a straight-through Ethernet cable from the switch to the network port labeled 10/100 SW on the Cisco Unified IP Phones 7962G, 7942G, 7961G, and 7941G, or to the network port labeled 10/100/1000 SW on the Cisco Unified IP Phones 7961G-GE and 7941G-GE. Each Cisco Unified IP Phone ships with one Ethernet cable in the box. You can use either Category 3/5/5e cabling for 10-Mbps connections, but you must use Category 5/5e for 100 Mbps connections.	See Network and Access Ports, page 3-3 for guidelines.
6.	Connect a straight-through Ethernet cable from another network device, such as a desktop computer, to the access port labeled 10/100 PC port on the Cisco Unified IP Phones 7962G, 7942G, 7961G, and 7941G, or to the network port labeled 10/100/1000 PC on the Cisco Unified IP Phones 7961G-GE and 7941G-GE. (Optional) You can connect another network device later if you do not connect one now. You can use either Category 3/5/5e cabling for 10-Mbps connections, but you must use Category 5/5e for 100 Mbps connections.	See Network and Access Ports, page 3-3 for guidelines.

Figure 3-2 Cisco Unified IP Phone 7962G and 7942G Cable Connections



1	DC adaptor port (DC48V) for phones not provided with inline power	6	Handset port
2	AC-to-DC power supply	7	Headset port
3	AC power cord	8	Footstand adjustment button
4	Network port (10/100 SW on the 7962G/7942G/7961G/7941G; 10/100/1000 SW on the 7961G-GE/7941G-GE) for connecting to the network	9	Auxiliary port (AUX)
5	Access port (10/100 PC on the 7962G/7942G/7961G/7941G; 10/100/1000 PC on the 7961G-GE/7941G-GE) for connecting your phone to your computer		

Related Topics

- Feature Key Capacity Increase for Cisco Unified IP Phones, page 3-10
- Verifying the Phone Startup Process, page 3-14
- Configuring Startup Network Settings, page 3-15
- Configuring Security on the Cisco Unified IP Phones, page 3-15

Attaching a Cisco Unified IP Phone Expansion Module

The Cisco Unified IP Phone Expansion Module attaches to a Cisco Unified IP Phone 7962G, 7961G and 7961G-GE to extend the number or line appearances or programmable buttons on your phone. These phones support the Cisco Unified IP Phone Expansion Model 7914, 7915, and 7916. You can customize the button templates for the Cisco Unified IP Phone Expansion Module to determine the number of line appearances and speed dial buttons. See Modifying Phone Button Templates, page 5-25 for details.

Note The Cisco Unified IP Phone 7941G, 7941G-GX, and 7942G do not support the Cisco Unified IP Phone Expansion Model 7914, 7915, and 7916.

You can attach one or more Cisco Unified IP Phone Expansion Modules 7914, 7915, or 7916 to the Cisco Unified IP Phone 7962G by using one of the following methods:

- When you initially add the phone to Cisco Unified Communications Manager, by selecting **7914 14-Button Line Expansion Module** for the Cisco Unified IP Phone Expansion 7914, **7915 12-Button Line Expansion Module** or **7915 24-Button Line Expansion Module** for the Cisco Unified IP Phone Expansion Module 7915, or **7916 12-Button Line Expansion Module** or **7916 24-Button Line Expansion Module** for the Cisco Unified IP Phone Expansion Module 7916 in the Module 1 or Module 2 fields, and choosing the appropriate expansion module firmware. See in the following procedure.
- After the phone is configured in Cisco Unified Communications Manager.

You can attach a Cisco Unified IP Phone Expansion Module 7914 to the Cisco Unified IP Phone 7961G and 7961G-GE by using one of the following methods:

- When you initially add the phone to Cisco Unified Communications Manager, you can choose **7914 14-Button Line Expansion Module** in the Module 1 or Module 2 fields and then choose the appropriate expansion module firmware. See in the following procedure.
- After the phone is configured in Cisco Unified Communications Manager.

To configure the Cisco Unified IP Phone Expansion Module on the Cisco Unified IP Phone, follow these steps.

Procedure

Step 1 Log in to Cisco Unified Communications Manager Administration.

Cisco Unified Communications Manager Administration window displays.

Step 2 From the menu, choose **Device > Phone**.

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

Step 3 Select and enter your search criteria and click **Find**.

The Find and List Phone window displays showing a list of the phones that match your search criteria.

Step 4 Click the IP Phone that you want to configure for the Cisco Unified IP Phone Expansion Module.

The Phone Configuration window displays.

Step 5 Scroll to the Expansion Module Information section.

Step 6 To add support for one expansion module on Cisco Unified IP Phones 7961G and 7961G-GE, in the Module 1 field, select **7914 14-Button Line Expansion Module**.

To add support for one expansion module on Cisco Unified IP Phone 7962G, in the Module 1 field, choose:

- **7914 14-Button Line Expansion Module** for the Cisco Unified IP Phone Expansion Module 7914,
- **7915 12-Button Line Expansion Module** or **7915 24-Button Line Expansion Module** for the Cisco Unified IP Phone Expansion Module 7915, or
- **7916 12-Button Line Expansion Module** or **7916 24-Button Line Expansion Module** for the Cisco Unified IP Phone Expansion Module 7916.

Step 7 To add support for a second expansion module on Cisco Unified IP Phones 7961G and 7961G-GE, in the Module 2 field, choose **7914 14-Button Line Expansion Module.**

To add support for a second expansion module on Cisco Unified IP Phone 7962G, in the Module 2 field, choose:

- **7914 14-Button Line Expansion Module** for the Cisco Unified IP Phone Expansion Modules 7914,
- **7915 12-Button Line Expansion Module** or **7915 24-Button Line Expansion Module** for the Cisco Unified IP Phone Expansion Module 7915, or
- **7916 12-Button Line Expansion Module** or **7916 24-Button Line Expansion Module** for the Cisco Unified IP Phone Expansion Module 7916.

Note In the Firmware Load Information section, there are two fields that specify the firmware load for Modules 1 and 2. You can leave these fields blank to use the default firmware load.

Step 8 Click the **Save** icon.

A message displays asking you to click the **Apply Config** for the changes to take effect.

Step 9 Click **OK**.

Step 10 Click **Apply Config**.

The Apply Configuration Information dialog appears.

Step 11 Click **OK**.

Note Refer users to their Cisco Unified CM User Options web pages, so they can configure speed-dial buttons and program buttons to access phone services on the Cisco Unified IP Phone Expansion Module. See How Users Subscribe to Services and Configure Phone Features, page A-3 for more details.

Feature Key Capacity Increase for Cisco Unified IP Phones

The Cisco Unified IP Phone Expansion Modules 7915 and 7916 attach to your Cisco Unified IP Phone 7962G, adding up to 48 extra line appearances or programmable buttons to your phone. The line capability increase includes Directory Numbers (DN), line information menu, line ring menu, and line help ID.

You can configure all 48 additional keys on the Cisco Unified IP Phone Expansion Modules 7915 and 7916.

Cisco Unified IP Phones 7961G-GE and 7941G-GE do not support Cisco Unified IP Phone Expansion Modules 7915 and 7916.

Use the Phone Button Template Configuration to configure the buttons.

Cisco Unified Communications Manager includes several default phone button templates. When adding phones, you can assign one of these templates to the phones or create a new template.

To configure the 48 additional buttons, follow these steps:

Procedure

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

Step 2 Click the **Add New** button.

Step 3 From the drop-down list, choose a template and click **Copy**.

Step 4 Rename the new template.

Step 5 Update the table to 54 Directory Numbers for Cisco Unified IP Phone 7962G.

See *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide* for more information on creating and modifying templates.

Note You can also attach two Cisco Unified IP Phone Expansion Modules 7915s or two Cisco Unified IP Phone Expansion Modules 7916s, to provide 48 additional lines or speed-dial and feature buttons.

Related Topic

Configuring Softkey Templates, page 5-27

Adjusting the Placement of the Cisco Unified IP Phone

The Cisco Unified IP Phone includes an adjustable footstand. When placing the phone on a desktop surface, you can adjust the tilt height to several different angles in 7.5 degree increments from flat to 60 degrees. You can also mount these phones to the wall by using the footstand or by using the optional locking wall mount kit.

Adjusting Cisco Unified IP Phone Placement on the Desktop

You can adjust the footstand adjustment plate on the Cisco Unified IP Phone to the height that provides optimum viewing of the phone screen. See Figure 3-4 for more information.

Procedure

Step 1 Push in the footstand adjustment button.

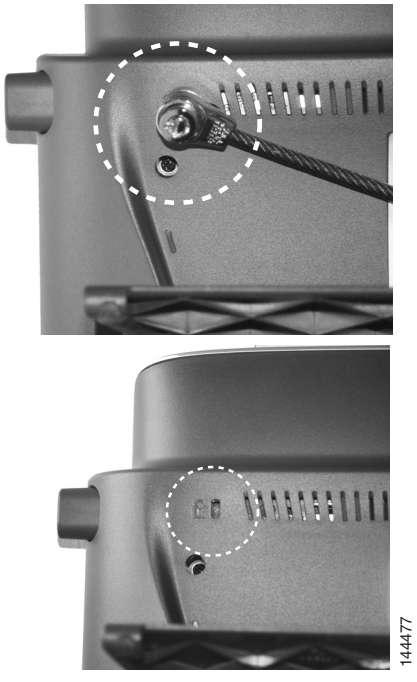
Step 2 Adjust the footstand to desired height.

Securing the Phone with a Cable Lock

You can secure the Cisco Unified IP Phone to a desktop by using a laptop cable lock. The lock connects to the security slot on the back of the phone, and the cable can be secured to a desktop.

The security slot can accommodate a lock up to 20 mm. Compatible laptop cable locks include the Kensington® laptop cable lock and laptop cable locks from other manufacturers that can fit into the security slot on the back of the phone. See Figure 3-3.

Figure 3-3 Connecting a Cable Lock to the Cisco Unified IP Phone



Mounting the Phone to the Wall

You can mount the Cisco Unified IP Phone on the wall by using the footstand as a mounting bracket or you can use special brackets available in a Cisco Unified IP Phone wall mount kit. Wall mount kits must be ordered separately from the phone.

If you attach the Cisco Unified IP Phone to a wall by using the standard footstand and not the wall mount kit, you need to supply the following tools and parts:

- Screwdriver
- Screws to secure the Cisco Unified IP Phone to the wall

See Figure 3-4 for a graphical overview of the phone parts.

Before You Begin

To ensure that the handset attaches securely to a wall-mounted phone, remove the handset wall hook from the handset rest, rotate the hook 180 degrees, and reinsert the hook. Turning the hook exposes a lip on which the handset catches when the phone is vertical. For an illustrated procedure, see *Installing the Wall Mount Kit for the Cisco Unified IP Phone* at:

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

Caution Use care not to damage wires or pipes located inside the wall when securing screws to wall studs.

Procedure

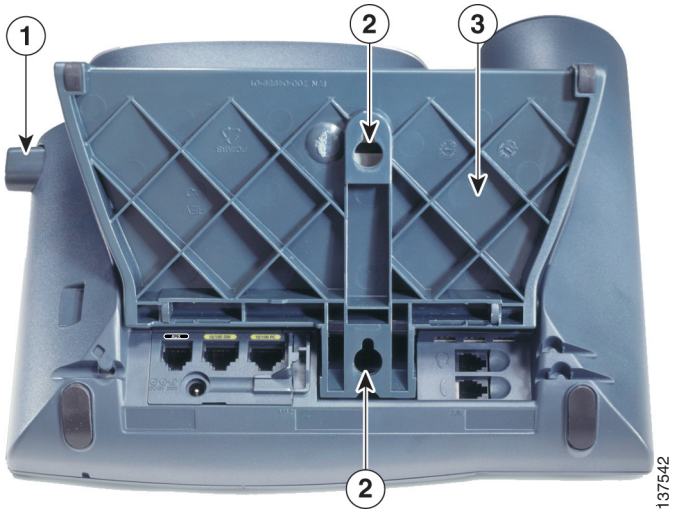
Step 1 Push in the footstand adjustment button.

Step 2 Adjust the footstand, so it is flat against the back of the phone.

Step 3 Insert two screws into a wall stud, matching them to the two screw holes on the back of the footstand. The keyholes fit standard phone jack mounts.

Step 4 Hang the phone on the wall.

Figure 3-4 Parts Used in Wall Mounting the Cisco Unified IP Phone



1	Footstand adjustment button—Raises and lowers adjustment plate
2	Wall mounting screw holes
3	Adjustment plate—Raises and lowers phone vertically

Verifying the Phone Startup Process

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

1. These buttons flash on and off in sequence:
   - Headset (only if the handset is off-hook when the phone powers up. Hang up the handset within 3 seconds to have the phone launch its secondary load. To continue with the primary load, leave the handset off-hook.)
   - Mute
   - Speaker
2. Some or all of the line keys flash amber in sequence.

Caution If the line keys flash red in sequence after flashing amber, do not power down the phone until the sequence of red flashes completes. This sequence can take several minutes to complete.

3. Some or all of the line keys flash green.

   Normally, this sequence takes just a few seconds. However, if the phone's Flash memory is erased or the phone load is corrupted, the sequence of green flashes will continue while the phone begins a software update procedure. If the phone performs this procedure, the following buttons light to indicate progress:
   - Headset—Phone is waiting for the network and completing CDP and DHCP configuration. A DHCP server must be available in your network.
   - Mute—Phone is downloading images from the TFTP server.
   - Speaker—Phone is writing images to its Flash memory.
4. The phone screen displays the Cisco Systems, Inc., logo screen.
5. These messages appear as the phone starts:
   - Verifying Load (if the phone load does not match the load on the TFTP server). If this message appears, the phone starts up again and repeats step 1 through step 4 above.
   - Configuring IP
   - Updating the Trust List
   - Updating Locale
   - Configuring Unified CM List
   - Registering
6. The phone screen displays:
   - Current date and time
   - Primary directory number
   - Additional directory numbers and speed dial numbers, if configured
   - Softkeys

If the phone successfully passes through these stages, it has started up properly. If the phone does not start up properly, see Resolving Startup Problems, page 9-1.

Configuring Startup Network Settings

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

- IP address
- IP subnet information (subnet mask for IPv4 and subnet prefix length for IPv6)
- Default gateway IP address
- 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 Configuring Settings on the Cisco Unified IP Phones.

Configuring Security on the Cisco Unified IP Phones

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

For more information about the security features, see Understanding Security Features for Cisco Unified IP Phones, page 1-11. Also, see *Cisco Unified Communications Manager Security Guide*.

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

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

To configure an LSC on the phone manually, 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 **Settings > Security Configuration**.

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

Step 3 Press ****#** to unlock settings on the Security Configuration menu. See Unlocking and Locking Options, page 4-2 for information using locking and unlocking options.

Note If a Settings Menu password has been set up, SIP Phones present an "Enter password" prompt after you enter **#.

Step 4 Scroll to LSC and press the **Update** softkey.

The phone prompts for an authentication string.

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

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

The LSC install, update, or removal process can take a long time to complete. You can stop the process at any time by pressing the **Stop** softkey from the Security Configuration menu. (Settings must be unlocked before you can press this softkey.)

When the phone successfully completes the installation procedure, it displays "Success." If the phone displays "Failure," the authorization string may be incorrect or the phone may not be enabled for upgrading. See error messages generated on the CAPF server and take appropriate actions.

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

Related Topic

- Understanding Security Features for Cisco Unified IP Phones, page 1-11

CHAPTER 4

Configuring Settings on the Cisco Unified IP Phones

Cisco Unified IP Phones includes many configurable network and device settings that you may need to modify before the phone is functional for your users. You can access these settings, and change many of them, through menus on the phone.

This chapter includes the following topics:

Configuration Menus on the Cisco Unified IP Phones

The Cisco Unified IP Phone includes the following configuration menus:

- Network Configuration—Provides options for viewing and making a variety of network settings. For more information, see Network Configuration Menu, page 4-5.
- Device Configuration—Provides access to sub-menus from which you can view a variety of non network-related settings. For more information, see Device Configuration Menu, page 4-18.
- Security Configuration—Provides options for displaying and modifying security settings. For more information, see Security Configuration Menu, page 4-32.

Before you can change option settings on the Network Configuration menu, you must unlock options for editing. See Unlocking and Locking Options, page 4-2 for instructions.

For information about the keys you can use to edit or change option settings, see Editing Values, page 4-3.

You can control whether a phone user has access to phone settings by using the Settings Access field in the Cisco Unified Communications Manager Administration Phone Configuration window.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Unlocking and Locking Options, page 4-2

- Editing Values, page 4-3
- Overview of Options Configurable from a Phone, page 4-4
- Network Configuration Menu, page 4-5
- Device Configuration Menu, page 4-18

Displaying a Configuration Menu

To display a configuration menu, perform the following steps.

Note 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 Settings menu, check the Settings Access field.

Procedure

Step 1 Press the **Settings** button to access the Settings menu.

Step 2 Perform one of these actions to display the desired menu:

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

Step 3 To display a submenu, repeat Step 2.

Step 4 To exit a menu, press the **Exit** softkey.

Related Topics

- Unlocking and Locking Options, page 4-2
- Editing Values, page 4-3
- Overview of Options Configurable from a Phone, page 4-4
- Network Configuration Menu, page 4-5
- Device Configuration Menu, page 4-18

Unlocking and Locking Options

Configuration options that can be changed from a phone are locked by default to prevent users from making changes that could affect the operation of a phone. You must unlock these options before you can change them.

When options are inaccessible for modification, a *locked* padlock icon appears on the configuration menus. When options are unlocked and accessible for modification, an *unlocked* padlock icon appears on these menus.

To unlock or lock options, press ****#**. This action either locks or unlocks the options, depending on the previous state.

Note If a Settings Menu password has been provisioned, SIP Phones present an "Enter password" prompt after you enter **#.

Make sure to lock options after you have made your changes.

Caution Do not press ****#** to unlock options and then immediately press ****#** again to lock options. The phone interprets this sequence as **#**, which resets the phone. To lock options after unlocking them, wait at least 10 seconds before you press ****#** again.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Editing Values, page 4-3
- Overview of Options Configurable from a Phone, page 4-4
- Network Configuration Menu, page 4-5
- Device Configuration Menu, page 4-18

Editing 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 the **2** key once for "a," twice quickly for "b," and three times quickly for "c." After you pause, the cursor automatically advances to allow you to enter the next letter.
- To enter a period (for example, in an IP address under IPv4 Configurations), press the **.** (period) softkey or press ***** on the keypad.
- To enter a colon (for example, in an IP address under IPv6 Configurations), press the : (colon) softkey or press * on the keypad.
- Press the **<<** softkey if you make a mistake. This softkey deletes the character to the left of the cursor.
- Press the **Cancel** softkey before pressing the **Save** softkey to discard any changes that you have made.

Note The Cisco Unified IP Phone provides several methods that you can use to reset or restore option settings, if necessary. For more information, see Resetting or Restoring the Cisco Unified IP Phones, page 9-13.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Unlocking and Locking Options, page 4-2
- Overview of Options Configurable from a Phone, page 4-4
- Network Configuration Menu, page 4-5
- Device Configuration Menu, page 4-18
- Security Configuration Menu, page 4-39

Overview of Options Configurable from a Phone

The settings that you can change on a phone fall into several categories, as shown in Table 4-1. For a detailed explanation of each setting and instructions for changing them, see Network Configuration Menu, page 4-5.

Note There are several options on the Network Configuration menu and on the Device Configuration Menu that are for display only or that you can configure from Cisco Unified Communications Manager. These options are also described in this chapter.

Table 4-1 Settings Configurable from the Phone

Category	Description	Network Configuration Menu Option
General Network Settings		
VLAN settings	Admin. VLAN ID allows you to change the administrative VLAN used by the phone. PC VLAN allows the phone to interoperate with third-party switches that do not support a voice VLAN.	Admin. VLAN ID PC VLAN
Port settings	Allows you to set the speed and duplex of the network and access ports.	SW Port Configuration PC Port Configuration
IPv4 Network Settings		
DHCP settings	Dynamic Host Configuration Protocol (DHCP) automatically assigns IP address to devices when you connect them to the network. Cisco Unified IP Phones enable DHCP by default.	DHCP DHCP Address Released
IP settings	If you do not use DHCP in your network, you can make IP settings manually.	Domain Name IP Address Subnet Mask Default Router 1-5 DNS Server 1-5
TFTP settings for TFTP IPv4 servers	If you do not use DHCP to direct the phone to a TFTP server, you must manually assign a TFTP server. You can also assign an alternative TFTP server to use instead of the one assigned by DHCP.	Alternate TFTP TFTP Server 1 TFTP Server 2

Table 4-1 Settings Configurable from the Phone (continued)

Category	Description	Network Configuration Menu Option
IPv6 Network Settings		
DHCP settings	Dynamic Host Configuration Protocol (DHCP) automatically assigns IP address to devices when you connect them to the network. Cisco Unified IP Phones enable DHCP by default.	DHCPv6
		DHCPv6 Address Released
IP settings	If you do not use DHCP in your network, you can make IP settings manually.	Domain Name
		IPv6 Address
		IPv6 Prefix Length
		IPv6 DNS Server 1-2
TFTP settings for TFTP IPv6 servers (SCCP phones only)	If you do not use DHCP to direct the phone to a TFTP server, you must manually assign a TFTP server. You can also assign an alternative TFTP server to use instead of the one assigned by DHCP.	IPv6 Alternate TFTP
		IPv6 TFTP Server 1
		IPv6 TFTP Server 2

Related Topics

- Displaying a Configuration Menu, page 4-2
- Unlocking and Locking Options, page 4-2
- Editing Values, page 4-3
- Network Configuration Menu, page 4-5
- Device Configuration Menu, page 4-18

Network Configuration Menu

The Network Configuration menu provides options for viewing and making a variety of network settings. Table 4-2, Table 4-3, and Table 4-4 describe these options and, where applicable, explain how to change them.

For information about how to access the Network Configuration menu, see Displaying a Configuration Menu, page 4-2.

Note The phone also has a Network Configuration menu that you access directly from the Settings menu. For information about the options on that menu, see Network Configuration Menu, page 4-34.

Before you can change an option on this menu, you must unlock options as described in the Unlocking and Locking Options, page 4-2. The **Edit**, **Yes**, or **No** softkeys for changing network configuration options appear only if options are unlocked.

For information about the keys you can use to edit options, see Editing Values, page 4-3.

Table 4-2 Network Configuration Menu Options

Option	Description	To Change
IPv4 Configuration	Internet Protocol v4 address menu. In the IPv4 Configuration menu, you can do the following: • Enable or disable the phone to use the IPv4 address that is assigned by the DHCPv4 server. • Manually set the IPv4 Address, Subnet Mask, Default Routers, DNSv4 Server, and Alternate TFTP servers for IPv4. For more information on the IPv4 address fields, see the specific field within this table.	1. Unlock network configuration options. 2. Scroll to IPv4 Configuration and press the **Select** softkey.
IPv6 Configuration	Internet Protocol v6 address menu. In the IPv6 Configuration menu, you can do the following: • Enable or disable the phone to use the IPv6 address that is assigned by the DHCPv6 server or to use the IPv6 address that it acquires through Stateless Address Autoconfiguration (SLAAC). • Manually set the IPv6 Address, Subnet Prefix Length, DNSv6 Server, and IPv6 TFTP Servers. For more information on the IPv6 address fields, see Table 4-4. For more information on SLAAC, see *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager.*	1. Unlock network configuration options. 2. Scroll to IPv6 Configuration and press the **Select** softkey.
mac address	Unique Media Access Control (MAC) address of the phone.	Display only—Cannot configure.
Host Name	Unique host name that the DHCP server assigned to the phone.	Display only—Cannot configure.

Table 4-2 Network Configuration Menu Options (continued)

Option	Description	To Change
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides. **Note** If the phone receives different domain names from the DHCPv4 and DHCPv6 servers, the domain name from the DHCPv6 will take precedence.	1. Unlock network configuration options. 2. Disable DHCP. If the IP Addressing mode is configured for IPv4 only, set the DHCP option to **No**. If the IP Addressing mode is configured for IPv6 only, set the DHCPv6 option to **No**. If the IP Addressing mode is configured for both IPv4 and IPv6, set both DHCP option and DHCPv6 to **No**. 3. Scroll to the Domain Name option, press the **Edit** softkey, and then enter a new domain name. 4. Press the **Validate** softkey and then press the **Save** softkey.
Operational VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member. If the phone has not received an auxiliary VLAN, this option indicates the Administrative VLAN. If neither the auxiliary VLAN nor the Administrative VLAN are configured, this option is blank.	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.	1. Unlock network configuration options. 2. Scroll to the Admin. VLAN ID option, press the **Edit** softkey, and then enter a new Admin VLAN setting. 3. Press the **Validate** softkey and then press the **Save** softkey.

Table 4-2 Network Configuration Menu Options (continued)

Option	Description	To Change
SW Port Configuration	Speed and duplex of the network port. Valid values: • Auto Negotiate • 10 Half—10-BaseT/half duplex • 10 Full—10-BaseT/full duplex • 100 Half—100-BaseT/half duplex • 100 Full—100-BaseT/full duplex • 1000 Full—1000-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to auto-negotiate. If you change the setting of this option, you must change the PC Port Configuration option to the same setting.	1. Unlock network configuration options. 2. Scroll to the SW Port Configuration option and then press the **Edit** softkey. 3. Scroll to the setting that you want and then press the **Select** softkey. 4. Press the **Save** softkey.
PC Port Configuration	Speed and duplex of the access port. Valid values: • Auto Negotiate • 10 Half—10-BaseT/half duplex • 10 Full—10-BaseT/full duplex • 100 Half—100-BaseT/half duplex • 100 Full—100-BaseT/full duplex • 1000 Full—1000-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to auto-negotiate. If you change the setting of this option, you must change the SW Port Configuration option to the same setting.	1. Unlock network configuration options. 2. Scroll to the PC Port Configuration option and then press the **Edit** softkey. 3. Scroll to the setting that you want and then press the **Select** softkey. 4. Press the **Save** softkey. To configure the setting on multiple phones simultaneously, enable the Remote Port Configuration in the Enterprise Phone Configuration (**System > Enterprise Phone Configuration**). **Note** If the ports are configured for Remote Port Configuration in Unified CM, the data cannot be changed on the phone.

Table 4-2 Network Configuration Menu Options (continued)

Option	Description	To Change
PC VLAN	Allows the phone to interoperate with third-party switches that do not support a voice VLAN. The Admin VLAN ID option must be set before you can change this option.	1. Unlock network configuration options. 2. Make sure the Admin VLAN ID option is set. 3. Scroll to the **PC VLAN** option, press the **Edit** softkey, and then enter a new PC VLAN setting. 4. Press the **Validate** softkey and then press the **Save** softkey.
VPN	Shows the virtual private network (VPN) Client state: • Connected • Not Connected (Supported only for the Cisco Unified IP Phone 7942G, and 7962G.)	Display only—Cannot configure.

Table 4-3 describes the IPv4 configuration menu options.

Table 4-3 IPv4 Configuration 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 anIPv4 address. When DHCP is disabled, you manually assign an IPv4 address to the phone.	1. Unlock network configuration options. 2. Scroll to the DHCP option and press the **No** softkey to disable DHCP, or press the **Yes** softkey to enable DHCP. 3. Press the **Save** softkey.
IP Address	Internet Protocol version 4 (IPv4) address of the phone. If you assign an IPv4 address with this option, you must also assign a subnet mask and default router. See Subnet Mask and Default Router 1 options in this table.	1. Unlock network configuration options. 2. Set the DHCP option to **No**. 3. Scroll to the IP Address option, press the **Edit** softkey, and then enter a new IP Address. 4. Press the **Validate** softkey and then press the **Save** softkey.

Table 4-3 IPv4 Configuration Menu Options (continued)

Option	Description	To Change
Subnet Mask	Subnet mask used by the phone.	1. Unlock network configuration options. 2. Set the DHCP option to **No**. 3. Scroll to the Subnet Mask option, press the **Edit** softkey, and then enter a new subnet mask. 4. Press the **Validate** softkey and then press the **Save** softkey.
Default Router 1 Default Router 2 Default Router 3 Default Router 4 Default Router 5	Default router used by the phone (Default Router 1) and optional backup routers (Default Router 2–5).	1. Unlock network configuration options. 2. Set the DHCP option to **No**. 3. Scroll to the appropriate Default Router option, press the **Edit** softkey, and then enter a new router IP address. 4. Press the **Validate** softkey. 5. Repeat Steps 3 and 4 as needed to assign backup routers. 6. Press the **Save** softkey.
DNS Server 1 DNS Server 2 DNS Server 3 DNS Server 4 DNS Server 5	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) used by the phone.	1. Unlock network configuration options. 2. Set the DHCP option to **No**. 3. Scroll to the appropriate DNS Server option, press the **Edit** softkey, and then enter a new DNS server IP address. 4. Press the **Validate** softkey. 5. Repeat Steps 3 and 4 as needed to assign backup DNS servers. 6. Press the **Save** softkey.
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IPv4 address.	Display only—Cannot configure.

Table 4-3 IPv4 Configuration Menu Options (continued)

Option	Description	To Change
DHCP Address Released	Releases the IPv4 address assigned by DHCP.	1. Unlock network configuration options. 2. Scroll to the DHCP Address Released option and press the **Yes** softkey to release the IP address assigned by DHCP, or press the **No** softkey if you do not want to release this IP address. 3. Press the **Save** softkey.
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.	1. Unlock network configuration options. 2. Scroll to the Alternate TFTP option and press the **Yes** softkey if the phone should use an alternative TFTP server. 3. Press the **Save** softkey.

Table 4-3 IPv4 Configuration Menu Options (continued)

Option	Description	To Change
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone. If you are not using DHCP in your network and you want to change this server, you must use the TFTP Server 1 option. If you set the Alternate TFTP option to Yes, you must enter a non-zero value for the TFTP Server 1 option. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL file or ITL file on the phone, you must unlock the files before you can save changes to the TFTP Server 1 option. In this case, the phone will delete the file when you save changes to the TFTP Server 1 option. A new CTL or ITL file will be downloaded from the new TFTP Server 1 address. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order 1. Any manually assigned IPv6 TFTP servers 2. Any manually assigned IPv4 TFTP servers 3. DHCPv6 assigned TFTP servers 4. DHCP assigned TFTP servers **Note** For information about the CTL and ITL files, see *Cisco Unified Communications Manager Security Guide*. For information about unlocking CTL and ITL files, see Unlocking the CTL and ITL Files, page 4-41.	1. Unlock the CTL or ITL file if necessary (for example, if you are changing the administrative domain of the phone). If the CTL and ITL files both exist, unlock either file. 2. If DHCP is enabled, set the Alternate TFTP option to **Yes**. 3. Scroll to the TFTP Server 1 option, press the **Edit** softkey, and then enter a new TFTP server IP address. 4. Press the **Validate** softkey, and then press the **Save** softkey.

Table 4-3 IPv4 Configuration Menu Options (continued)

Option	Description	To Change
TFTP Server 2	Optional backup TFTP server that the phone with an IPv4 address uses if the primary TFTP server is unavailable. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL or ITL files on the phone, you must unlock the file before you can save changes to the TFTP Server 2 option. In this case, the phone will delete the file when you save changes to the TFTP Server 2 option. A new CTL file or ITL file will be downloaded from the new TFTP Server 2 address. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: 1. Manually assigned IPv6 TFTP servers 2. Manually assigned IPv4 TFTP servers 3. DHCPv6 assigned TFTP servers 4. DHCP assigned TFTP servers **Note** For information about the CTL and ITL files, see *Cisco Unified Communications Manager Security Guide*. For information about unlocking CTL and ITL files, see Unlocking the CTL and ITL Files, page 4-41	1. Unlock the CTL or ITL files if necessary (for example, if you are changing the administrative domain of the phone). If the CTL and ITL files both exist, unlock either file. 2. Unlock network configuration options. 3. Enter an IP address for the TFTP Server 1 option. 4. Scroll to the TFTP Server 2 option, press the **Edit** softkey, and then enter a new backup TFTP server IP address. 5. Press the **Validate** softkey, and then press the **Save** softkey. **Note** If you forgot to unlock the CTL file, you can change the TFTP Server 2 address in the CTL file, then erase the CTL file by pressing the Erase softkey from the Security Configuration menu. A new CTL file will be downloaded from the new TFTP Server 2 address.
BOOTP Server	Indicates whether the phone obtains its configuration from a Bootstrap Protocol (BootP) server instead of from a DHCP server.	Display only—Cannot configure.

Table 4-4 describes the IPv6 configuration menu options.

Table 4-4 IPv6 Configuration Menu Options

Option	Description	To Change
DHCPv6	Indicates whether the phone has DHCP 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. The DHCPv6 setting along with the Auto IP Configuration setting determine how the IP Phone obtains its network settings. For more information on how these two settings affect the network settings on the phone, see Table 4-5.	1. Unlock network configuration options. 2. Scroll to the DHCPv6 option and press the **No** softkey to disable DHCP, or press the **Yes** softkey to enable DHCP. 3. Press the **Save** softkey.
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. See IPv6 Subnet Prefix option in this table.	1. Unlock network configuration options. 2. Set the DHCPv6 option to **No**. 3. Scroll to the IP Address option, press the **Edit** softkey, and then enter a new IP Address. 4. Press the **Validate** softkey and then press the **Save** softkey.
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.	1. Unlock network configuration options. 2. Set the DHCPv6 option to **No**. 3. Scroll to the IPv6 Prefix Length option, press the **Edit** softkey, and then enter a new subnet mask. 4. Press the **Validate** softkey and then press the **Save** softkey.
IPv6 Default Router 1	Default router used by the phone (Default Router 1). **Note** The phone obtains information on the default router from IPv6 Router Advertisements.	Display only—Cannot configure.

Table 4-4 IPv6 Configuration Menu Options (continued)

Option	Description	To Change
IPv6 DNS Server 1 IPv6 DNS Server 2	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2) used by the phone. If your configuration includes both DNSv6 and DNSv4 servers, the phone will look for its DNS server in the following order: 1. IPv6 DNS Server 1 2. IPv6 DNS Server 2 3. DNS Server 1-5 for IPv4 (respectively)	1. Unlock network configuration options. 2. Set the DHCPv6 option to No. 3. Scroll to the appropriate DNS Server option, press the **Edit** softkey, and then enter a new DNS server IP address. 4. Press the **Validate** softkey. 5. Repeat Steps 3 and 4 as needed to assign the backup DNS server. 6. Press the **Save** softkey.
DHCPv6 Address Released	Releases the IPv6 address that the phone has acquired from the DHCPv6 server or by stateless address autoconfiguration. **Note** This field is only editable when the DHCPv6 option is enabled.	1. Unlock network configuration options. 2. Scroll to the DHCPv6 Address Released option and press the **Yes** softkey to release the IP address assigned by DHCP, or press the **No** softkey if you do not want to release this IP address. 3. Press the **Save** softkey.
IPv6 Alternate TFTP	Indicates whether the phone is using the IPv6 Alternate TFTP server.	1. Unlock network configuration options. 2. Scroll to the IPv6 Alternate TFTP option and press the **Yes** softkey if the phone should use an alternative TFTP server. 3. Press the **Save** softkey.

Table 4-4 IPv6 Configuration Menu Options (continued)

Option	Description	To Change
IPv6 TFTP Server 1 (SCCP phones only)	Primary IPv6 Trivial File Transfer Protocol (TFTP) server used by the phone. If you are not using DHCPv6 in your network and you want to change this server, you must use the IPv6 TFTP Server 1 option. If you set the IPv6 Alternate TFTP option to Yes or you disable DHCPv6, you must enter a non-zero value for the IPv6 TFTP Server 1 option. If you make changes to the Alternate TFTP or IPv6 TFTP servers, you must first unlock the CTL file or ITL file on the phone. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: 1. Manually assigned IPv6 TFTP Servers 2. Manually assigned IPv4 TFTP Servers 3. DHCPv6 assigned TFTP Servers 4. DHCP assigned TFTP Servers For information about the CTL or ITL file, see *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL file, see Unlocking the CTL and ITL Files, page 4-41.	1. Unlock the CTL file or ITL file, if necessary. If the CTL and ITL files both exist, unlock either file. 2. If DHCPv6 is enabled, set the IPv6 Alternate TFTP option to **Yes**. 3. Scroll to the IPv6 TFTP Server 1 option, press the **Edit** softkey, and then enter a new TFTP server IP address. 4. Press the **Validate** softkey, and then press the **Save** softkey.

Table 4-4 IPv6 Configuration Menu Options (continued)

Option	Description	To Change
IPv6 TFTP Server 2 (SCCP phones only)	Optional backup IPv6 TFTP server that the phone uses if the primary IPv6 TFTP server is unavailable. If you make changes to the Alternate TFTP or IPv6 TFTP servers, you must first unlock the CTL file or ITL file on the phone. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: 1. Manually assigned IPv6 TFTP Servers 2. Manually assigned IPv4 TFTP Servers 3. DHCPv6 assigned TFTP Servers 4. DHCP assigned TFTP Servers For information about the CTL file or ITL file, see *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL file, see Unlocking the CTL and ITL Files, page 4-41.	1. Unlock the CTL file or ITL file if necessary. If both the CTL file and ITL file exist, unlock either of the files. 2. Unlock network configuration options. 3. Enter an IP address for the IPv6 TFTP Server 1 option. 4. Scroll to the IPv6 TFTP Server 2 option, press the **Edit** softkey, and then enter a new backup TFTP server IP address. 5. Press the **Validate** softkey, and then press the **Save** softkey.

Understanding DHCPv6 and Autoconfiguration

You can choose to configure the IP address and other network settings, such as the TFTP server, DNS server, domain, and name on an IP Phone manually or by using a router or a DHCP server to automatically assign the IP address and other network information. For more information on how the Auto IP Configuration and DHCPv6 settings determine where the IP Phone acquires its IPv6 address and other network settings, see Table 4-5.

Table 4-5 Determining Where a Phone Acquires Its Network Settings

DHCPv6	Auto IP Configuration	How the Phone Acquires its IP address and Network Settings
Disabled	Disabled	You must manually configure an IP address and the other network settings. **Note** When DHCPv6 is disabled, the Auto IP Configuration setting is ignored.
Disabled	Enabled	You must manually configure an IP address and the other network settings. **Note** When DHCPv6 is disabled, the Auto IP Configuration setting is ignored.

Table 4-5 Determining Where a Phone Acquires Its Network Settings (continued)

DHCPv6	Auto IP Configuration	How the Phone Acquires its IP address and Network Settings
Enabled	Disabled	The DHCP server assigns the IP address and the other network settings to the phone.
Enabled	Enabled	When the M-bit is set on the router, the O-bit is ignored. The phone can set its IPv6 address based on an IPv6 address received from a DHCPv6 server or the phone can acquire its IPv6 address through stateless address autoconfiguration. When the M-bit is not set, you should set the O-bit on the router. The phone will then acquire its IPv6 address through stateless address autoconfiguration. The phone will not request an IPv6 address from the DHCPv6 server, but it will request other network configuration information.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Unlocking and Locking Options, page 4-2
- Editing Values, page 4-3
- Overview of Options Configurable from a Phone, page 4-4
- Device Configuration Menu, page 4-18

Device Configuration Menu

The Device Configuration menu provides access to eight sub-menus from which you can view a variety of settings that are specified in the configuration file for a phone. The phone downloads the configuration file from the TFTP server. These sub-menus are:

- Unified CM Configuration Menu, page 4-19
- SIP Configuration Menu for SIP Phones Only, page 4-20
- Call Preferences Menu for SIP Phones, page 4-22
- HTTP Configuration Menu, page 4-23
- Locale Configuration Menu, page 4-24
- UI Configuration Menu, page 4-26
- Media Configuration Menu, page 4-28
- Ethernet Configuration Menu, page 4-31
- Security Configuration Menu, page 4-32
- QoS Configuration Menu, page 4-33
- Network Configuration Menu, page 4-34

For instructions about how to access the Device Configuration menu and its sub-menus, see Displaying a Configuration Menu, page 4-2.

Unified CM Configuration Menu

The Unified CM Configuration menu contains the options Unified CM1, Unified CM2, Unified CM3, Unified CM4, and Unified CM5. These options show the Cisco Unified Communications Manager servers that are available for processing calls from the phone, in prioritized order. To change these options, use Cisco Unified Communications Manager Administration, Cisco Unified CM Group Configuration.

For an available Cisco Unified Communications Manager server, an option on the Unified CM Configuration menu will show the Cisco Unified Communications Manager server IP address or name and one of the states shown in Table 4-6.

Table 4-6 Cisco Unified Communications Manager Server States

State	Description
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 option may also display one of more of the designations or icons shown in Table 4-7.

Table 4-7 Cisco Unified Communications Manager Server Designations

Designation	Description
SRST	Indicates a Survivable Remote Site Telephony 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. For more information, see Survivable Remote Site Telephony Configuration in the *Cisco Unified Communications Manager Administration Guide*.
TFTP	Indicates that the phone was unable to register with a Cisco Unified Communications Manager listed in its configuration file, and it registered with the TFTP server instead.

Table 4-7 Cisco Unified Communications Manager Server Designations (continued)

Designation	Description
 (Authentication icon)	Appears as a shield and indicates that the call is from a trusted device, and that the connection to the Cisco Unified Communications Manager is authenticated. For more information about authentication, see *Cisco Unified Communications Manager Security Guide*.
 (Encryption icon)	Appears as a padlock and indicates that the call is from a trusted device, and that the connection to the Cisco Unified Communications Manager is authenticated and encrypted. For more information about authentication and encryption, see *Cisco Unified Communications Manager Security Guide*. The Encryption icon is also displayed when a Cisco Unified IP Phone is configured as *protected*. For more information about protected calls, see *Cisco Unified Communications Manager Security Guide*. Protected calls are not authenticated.

SIP Configuration Menu for SIP Phones Only

The SIP Configuration menu contains these sub-menus:

- SIP General Configuration Menu, page 4-20
- Line Settings Menu for SIP Phones, page 4-21

SIP General Configuration Menu

The SIP General Configuration menu displays information about the configurable SIP parameters on the phone. Table 4-8 describes the options in this menu.

Table 4-8 SIP General Configuration Menu Options

Option	Description	To Change
Preferred CODEC	Displays the CODEC to use when a call is initiated. This value will always be set to none.	Display only—cannot configure.
Out of Band DTMF	Displays the configuration of the out-of-band signaling (for tone detection on the IP side of a gateway). The Cisco Unified IP Phone (SIP) supports out-of-band signaling by using the AVT tone method. This value will always be set to avt.	Display only—cannot configure.
Register with Proxy	This value will always be set to Yes.	Display only—cannot configure.
Register Expires	Displays the amount of time, in seconds, after which a registration request expires.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.
Phone Label	Displays the text that is displayed on the top right status line of the LCD on the phone. This text is for end user display only and has no effect on caller identification or messaging. This value will always be set to null.	Display only—cannot configure.

Table 4-8 SIP General Configuration Menu Options (continued)

Option	Description	To Change
Enable VAD	This value is set to No by default.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.
Start Media Port	Displays the start Real-Time Transport Protocol (RTP) range for media.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.
End Media Port	Displays the end Real-Time Transport Protocol (RTP) range for media.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.
NAT Enabled	Displays if Network Address Translation (NAT) is enabled. This value will always be set to false.	Display only—cannot configure.
NAT Address	Displays the WAN IP address of the NAT or firewall server. This value will always be set to null.	Display only—cannot configure.
Call Statistics	This value is set to No by default.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Device Configuration Menu, page 4-18

Line Settings Menu for SIP Phones

The Line Settings menu displays information that relates to the configurable parameters for the lines on your SIP Phone. Table 4-9 describes the options in this menu.

Table 4-9 Line Settings Menu Options

Option	Description	To Change
Name	Displays the lines and the number used to register each line.	Use Cisco Unified Communications Manager Administration to modify.
Short Name	Displays the short name configured for the line.	Use Cisco Unified Communications Manager Administration to modify.

Table 4-9 Line Settings Menu Options (continued)

Option	Description	To Change
Longer Authentication Name	Displays the name used by the phone for authentication if a registration is challenged by the call control server during initialization. The length of the SIP digest authentication name is 128 characters for Cisco Unified 7900 Series SIP Phones. The authentication name is used to verify that the phone is allowed to send SIP messages (REGISTER, INVITE, and SUBSCRIBE) to the Cisco Unified CM.	Use Cisco Unified Communications Manager Administration to modify.
Display Name	Displays the identification the phone; used for display for caller identification purposes.	Use Cisco Unified Communications Manager Administration to modify.
Proxy Address	Displays the IP address of the proxy server used by the phone. The value is left blank because it is not applicable to SIP Phones that are using Cisco Unified Communications Manager.	Display only—cannot configure.
Proxy Port	The value is left blank because it is not applicable to SIP Phones that are using Cisco Unified Communications Manager.	Display only—cannot configure.
Shared Line	Displays if the line is part of a shared line (Yes) or not (No).	Display only—cannot configure.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Device Configuration Menu, page 4-18

Call Preferences Menu for SIP Phones

The Call Preferences menu displays settings that relate to the settings for the call preferences on the SIP Phone. Table 4-10 describes the options in this menu.

Table 4-10 Call Preferences Menu Options

Option	Description	To Change
Caller ID Blocking	Indicates whether caller ID blocking is enabled (Yes) or disabled (No) for the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.
Anonymous Call Block	Indicates whether anonymous call block is enabled (Yes) or disabled (No) for the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.
Call Waiting Preferences	Displays a sub-menu that indicates whether call waiting is enabled (Yes) or disabled (No) for each line.	Use Cisco Unified Communications Manager Administration to modify.
Call Hold Ringback	Indicates whether the call hold ringback feature is enabled (Yes) or disabled (No) for the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.

Table 4-10 Call Preferences Menu Options (continued)

Option	Description	To Change
Stutter Msg Waiting	Indicates whether stutter message waiting is enabled (Yes) or disabled (No) for the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile**.
Call Logs BLF Enabled	Indicates whether BLF for call logs is enabled (Yes) or disabled (No) for the phone.	Use Cisco Unified Communications Manager Administration to modify.
Auto Answer Preferences	Displays a sub-menu that indicates whether auto answer is enabled (Yes) or disabled (No) for the each line.	From Cisco Unified Communications Manager Administration, choose **Call Routing > Directory Number**.
Speed Dials	Displays a sub-menu that displays the lines available on the phone. Select a line to see the speed dial label and number assigned to that line.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Add a New Speed Dial**.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Device Configuration Menu, page 4-18

HTTP Configuration Menu

The HTTP Configuration menu displays the URLs of servers from which the phone obtains a variety of information. This menu also displays information about the idle display on the phone.

Note Cisco Unified IP Phones do not support URLs with IPv6 addresses in the URL. This includes hostname which maps to a IPv6 address for directories, services, messages, and information URLs. If you support the phone using URLs, you must configure the phone and the servers that provide URL services with IPv4 addresses.

Table 4-11 describes the options on the HTTP Configuration menu.

Table 4-11 HTTP Configuration Menu Options

Option	Description	To Change
Directories URL	URL of the server from which the phone obtains directory information.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Messages URL	URL of the server from which the phone obtains message services.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Information URL	URL of the help text that appears on the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Table 4-11 HTTP Configuration Menu Options (continued)

Option	Description	To Change
Authentication URL	URL that the phone uses to validate requests made to the phone web server.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Proxy Server URL	URL of proxy server, which makes HTTP requests to non-local host addresses on behalf of the phone HTTP client and provides responses from the non-local host to the phone HTTP client.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Idle URL	URL of an XML service that the phone displays when the phone has not been used for the time specified in the Idle URL Time option and no menu is open. For example, you could use the Idle URL option and the Idle URL Time option to display a stock quote or a calendar on the LCD screen when the phone has not been used for 5 minutes.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Idle URL Time	Number of seconds that the phone has not been used and no menu is open before the XML service specified in the Idle URL option is activated.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Locale Configuration Menu

The Locale Configuration menu displays information about the user locale and the network locale used by the phone. Table 4-12 describes the options on this menu.

Table 4-12 Locale Configuration Menu Options

Option	Description	To Change
User Locale	User locale associated with the phone user. The user locale identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information. For more information on installing user locale, see *Cisco Unified Communications Operating System Administration Guide*.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
User Locale Version	Version of the user locale loaded on the phone.	Display only—cannot configure.
User Locale Char Set	Character set that the phone uses for the user locale.	Display only—cannot configure.
Network Locale	Network locale associated with the phone user. The network locale identifies a set of detailed information that supports the phone in a specific location, including definitions of the tones and cadences used by the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Table 4-12 Locale Configuration Menu Options (continued)

Option	Description	To Change
Network Locale Version	Version of the network locale loaded on the phone.	Display only—cannot configure.
NTP Configuration (SIP Phones only)	Menu to view information on NTP server and mode configuration. For more information, see NTP Configuration Menu for SIP Phones, page 4-25.	From Cisco Unified Communications Manager Administration, choose **System > Phone NTP Reference**.

NTP Configuration Menu for SIP Phones

The NTP Configuration menu displays information about the NTP server and mode configuration used by SIP Phones. Table 4-13 describes the options on this menu.

Table 4-13 NTP Configuration Menu Options

Option	Description	To Change
NTP IP Address 1	IP address of the primary NTP server.	From Cisco Unified Communications Manager Administration, choose **System > Phone NTP Reference.**
NTP IP Address 2	IP address of the secondary or backup NTP server.	From Cisco Unified Communications Manager Administration, choose **System > Phone NTP Reference.**
NTP Mode 1	Primary server mode. Supported modes are Directed Broadcast, Unicast, Multicast, Any cast.	From Cisco Unified Communications Manager Administration, choose **System > Phone NTP Reference.**
NTP Mode 2	Secondary server mode. Supported modes are Directed Broadcast, Unicast, Multicast, Any cast.	From Cisco Unified Communications Manager Administration, choose **System > Phone NTP Reference.**

UI Configuration Menu

The UI Configuration menu displays the status of various user interface features on the phone. Table 4-14 describes the fields in this menu.

Table 4-14 UI Configuration Menu Options

Option	Description	To Change
Auto Line Select	Indicates whether the phone shifts the call focus to incoming calls on all lines. When this option is disabled, the phone only shifts the call focus to incoming calls on the line that is in use. When this option is enabled, the phone shifts the call focus to the line with the most recent incoming call. Default: Disabled	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
BLF for Call Lists	Indicates whether the Busy Lamp Field (BLF) is enabled for call lists.	From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.
Reverting Focus Priority	Indicates whether the phone shifts the call focus on the phone screen to an incoming call or a reverting hold call. Settings include: **Lower**—Focus priority given to incoming calls. **Higher**—Focus priority given to reverting calls. **Even**—Focus priority given to the first call.	From Cisco Unified Communications Manager Administration, choose **System > Device Pool**. See also: Hold Reversion.
Auto Call Select	Indicates whether the phone automatically shifts the call focus to an incoming call on the same line when the user is already on a call. When this option is enabled, the phone shifts the call focus to the most recent incoming call. When this option is disabled, all automatic focus changes, including Auto Line Select, are disabled regardless of the setting. Default: Enabled	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
“more” Softkey Timer	Indicates the number of seconds that additional softkeys are displayed after the user presses **more**. If this timer expires before the user presses another softkey, the display reverts to the initial softkeys. Range: 5 to 30; 0 represents an infinite timer. Default: 5	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Table 4-14 UI Configuration Menu Options (continued)

Option	Description	To Change
Wideband Handset UI Control	Indicates whether the user can configure the Wideband Handset option in the phone user interface. Values: • Enabled—The user can configure the Wideband Handset option in the Audio Preferences menu on the phone (choose > **User Preferences > Audio Preferences> Wideband Handset**). • Disabled—The value of the Wideband Handset option in Cisco Unified Communications Manager Administration gets used (see Media Configuration Menu, page 4-28). Default: Enabled	Use Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Wideband Headset UI Control	Indicates whether the user can configure the Wideband Headset option in the phone user interface. Values: • Enabled—The user can configure the Wideband Headset option in the Audio Preferences menu on the phone (choose > **User Preferences > Audio Preferences> Wideband Headset**). • Disabled—The value of the Wideband Headset option in Cisco Unified Communications Manager Administration gets used (see Media Configuration Menu, page 4-28). Default: Enabled	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Personalization	Indicates whether the user can configure custom ring tones and wallpaper images.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Single Button Barge	Indicates whether the Single Button Barge feature is enabled for the phone. Default: Disabled.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Enbloc Dialing (SCCP only)	Indicates whether the phone will use Enbloc dialing. If Enabled, the phone will use Enbloc dialing when possible. If Disabled, the phone will not use Enbloc dialing. You should disable Enbloc dialing if either Forced Authorization Codes (FAC) or Client Matter Codes (CMC) dialing is being used. Default: Enabled	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Media Configuration Menu

The Media Configuration menu displays whether the headset, wireless headset, speakerphone, and video capability are enabled on the phone. This menu also displays options for recording tones that the phone may play to indicate that a call may be recorded. Table 4-15 describes the options on this menu.

Table 4-15 Media Configuration Menu Options

Option	Description	To Change
Headset Enabled	Indicates whether the Headset button is enabled on the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Headset Hookswitch Control Enabled (Cisco Unified IP Phones 7962G and 7942G only)	Indicates whether the wireless headset hookswitch feature is enabled on the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Speaker Enabled	Indicates whether the speakerphone is enabled on the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Video Capability Enabled	Indicates whether the phone can participate in video calls when connected to an appropriately equipped computer.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Table 4-15 Media Configuration Menu Options (continued)

Option	Description	To Change
Recording Tone	Indicates whether a recording tone (often referred to as a *beep tone*) is enabled or disabled for the phone. If the recording tone option is enabled, the phone plays the beep tone in both directions of every call, regardless of whether the call actually gets recorded. The beep tone first sounds when a call is answered. You may want to notify your users if you enable this option. Default: Disabled Related Parameters: • Recording Tone Local Volume • Recording Tone Remote Volume • Recording Tone Duration **Note** Other related parameters—Beep tone frequency in hz, the length of the beep tone (called *duration*), and how often the beep tone plays (called *interval*)—are defined on a per-Network Locale basis in the xml file that defines tones. This xml file is usually named tones.xml or g3-tones.xml.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Recording Tone Local Volume	Indicates the loudness setting for the beep tone that is received by the party whose phone has the Recording Tone option enabled. This setting applies for each listening device (handset, speakerphone, headset). Range: 0 percent (no tone) to 100 percent (same level as current volume setting on the phone). Default: 100 See also: Recording Tone	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Recording Tone Remote Volume	Indicates the loudness setting for the beep tone that the *remote party* receives. The *remote party* is the party who is on a call with the party whose phone has the Recording Tone option enabled. Range: 0 percent to 100 percent. (0 percent is –66 dBM and 100 percent is –3 dBM.) Default: 84 percent (–10dBM) See also: Recording Tone	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Table 4-15 Media Configuration Menu Options (continued)

Option	Description	To Change
Recording Tone Duration	Indicates the length of time in milliseconds for which the beep tone plays. If the value you configure here is less than one third the interval, then this value overrides the default provided by the Network Locale. Range: 0 to 3000 **Note** For some Network Locales that use a complex cadence, this setting applies only to the first beep tone. See also: Recording Tone	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Wideband Handset	Indicates whether wideband is enabled or disabled for the handset. Default: "Use Phone Default" on Cisco Unified Communications Manager Administration. (This default means that the phone will be enabled for a wideband handset only if the phone was shipped with a wideband handset.)	• If Wideband Handset UI Control is enabled, you or the user can choose **> User Preferences > Audio Preferences > Wideband Handset.** • If Wideband Handset UI Control is disabled, use Cisco Unified Communications Manager Administration and choose **Device > Phone > Phone Configuration** to set this value. **Note** If you allow this option to be user controllable (in the Wideband Handset UI Control option), the user-configured value takes precedence.
Wideband Headset	Indicates whether wideband is enabled or disabled for the headset. Default: Disabled	• If Wideband Headset UI Control is enabled, you or the user can use the phone and choose **> User Preferences > Audio Preferences > Wideband Headset**. • If Wideband Headset UI Control is disabled, use Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration** to set this value. **Note** If you allow this option to be user controllable (in the Wideband Headset UI Control option), the user-configured value takes precedence.

Table 4-15 Media Configuration Menu Options (continued)

Option	Description	To Change
Enterprise Advertise G.722 Codec	Enables/disables Cisco Unified IP Phones to advertise the G.722 codec to Cisco Unified Communications Manager. For more information, see the *Cisco Unified Communications Manager System Guide*, Cisco Unified IP Phones. **Note** When a phone is registered with a Cisco Unified Communications Manager that does not support this setting, the default is Disabled.	From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.
Device Advertise G.722 Codec	Allows you to override the Enterprise Advertise G.722 Codec on a per-phone basis. Default: Use System Default, which means the value configured for the Enterprise Advertise G.722 Codec parameter gets used.	From Cisco Unified Communications Manager Administration, choose **Device > Phone**.

Ethernet Configuration Menu

The Ethernet Configuration menu includes the options that are described in Table 4-16.

Table 4-16 Ethernet Configuration Menu Option

Option	Description	To Change
Forwarding Delay	Indicates whether the internal switch begins forwarding packets between the PC port and switched port on the phone when the phone becomes active. • When forwarding delay is set to disabled, the internal switch begins forwarding packets immediately. • When forwarding delay is set to enabled, the internal switch waits eight seconds before forwarding packets between the PC port and the switch port. Default is disabled.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Span to PC Port	Indicates whether the phone will forward packets transmitted and received on the network port to the access port. Enable this option if an application that requires monitoring of the phone's traffic is being run on the access port. These applications include monitoring and recording applications (common in call center environments) and network packet capture tools that are used for diagnostic purposes.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Security Configuration Menu

The Security Configuration that you access directly from the Settings menu provides information about various security settings. It also provides access to the Trust List menu. The Trust List menu indicates if the CTL or ITL files are installed on the phone.

Note The phone also has a Security Configuration menu that you access directly from the Settings menu. For information about the security options on that menu, see Security Configuration Menu, page 4-39.

Table 4-17 describes the options on the Security Configuration menu.

Table 4-17 Security Configuration Menu Options

Option	Description	To Change
PC Port Disabled	Indicates whether the access port on the phone is enabled (Yes) or disabled (No). Must be set to enabled for video support on the phone	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
GARP Enabled	Indicates if the phone accepts MAC addresses from Gratuitous ARP (GARP) responses.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Voice VLAN Enabled	Indicates whether the phone allows a device attached to the access port to access the Voice VLAN. Setting this option to No (disabled) prevents the attached PC from sending and receiving data on the Voice VLAN. Setting this option also prevents the PC from receiving data sent and received by the phone. Set this setting to Yes (enabled) if an application that requires monitoring of the phone's traffic is running on the PC. These applications include monitoring and recording applications and network monitoring software.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.	For more information, see Disabling and Enabling Web Page Access, page 7-3.
Security Mode	Displays the security mode that is set for the phone.	Use Cisco Unified Communications Manager Administration to modify.
Logging Display	For use by the Cisco Technical Assistance Center (TAC), if necessary.	

QoS Configuration Menu

The QoS Configuration menu displays information that relates to quality of service (QoS) for the phone. Table 4-18 describes the options on this menu.

Table 4-18 QoS Configuration Menu Options

Option	Description	To Change
DSCP for Call Control	Differentiated Services Code Point (DSCP) IP classification for call control signaling.	From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.
DSCP for Configuration	DSCP IP classification for any phone configuration transfer.	From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.
DSCP for Services	DSCP IP classification for phone-based services.	From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Network Configuration Menu, page 4-5

Network Configuration Menu

The Network Configuration menu displays device-specific network configuration settings on the phone. Table 4-19 describes the options in this menu.

Note The phone also has a Network Configuration menu that you access directly from the Settings menu. For information about the options on that menu, see Network Configuration Menu, page 4-5.

Table 4-19 Network Configuration Menu Options

Option	Description	To Change
Load Server	Used to optimize installation time for phone firmware upgrades and offload the WAN by storing images locally, negating the need to traverse the WAN link for each phone's upgrade. You can set the Load Server to another TFTP server IP address or name (other than the TFTP Server 1 or TFTP Server 2) from which the phone firmware can be retrieved for phone upgrades. When the Load Server option is set, the phone contacts the designated server for the firmware upgrade. **Note** The Load Server option allows you to specify an alternate TFTP server for phone upgrades only. The phone continues to use TFTP Server 1 or TFTP Server 2 to obtain configuration files. The Load Server option does not provide management of the process and of the files, such as file transfer, compression, or deletion.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
RTP Control Protocol	Indicates whether the phone supports the Real-Time Control Protocol (RTCP). Settings include: • Enabled • Disabled—default If this feature is disabled, several call statistic values display as 0. For additional information, see the following sections: • Call Statistics Screen, page 8-14 • Streaming Statistics, page 7-11	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.

Table 4-19 Network Configuration Menu Options (continued)

Option	Description	To Change
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. **Note** 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. **Note** The current PC and switch port CDP values are shown on the Settings menu.	From Cisco Unified Communications Manager Administration, choose **Device > Phone**.
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. **Note** 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. **Note** The current PC and switch port CDP values are shown on the Settings menu.	From Cisco Unified Communications Manager Administration, choose **Device > Phone**.

Table 4-19 Network Configuration Menu Options (continued)

Option	Description	To Change
Peer Firmware Sharing	The Peer Firmware Sharing feature provides these advantages in high speed campus LAN settings: • Limits congestion on TFTP transfers to centralized remote TFTP servers • Eliminates the need to manually control firmware upgrades • Reduces phone downtime during upgrades when large numbers of devices are reset simultaneously Peer Firmware Sharing may also aid in firmware upgrades in branch/remote office deployment scenarios over bandwidth-limited WAN links. When enabled, it allows the phone to discover similar phones on the subnet that are requesting the files that make up the firmware image, and to automatically assemble transfer hierarchies on a per-file basis. The individual files making up the firmware image are retrieved from the TFTP server by only the root phone in the hierarchy, and are then rapidly transferred down the transfer hierarchy to the other phones on the subnet using TCP connections. This menu option indicates whether the phone supports peer firmware sharing. Settings include: • Enabled—default • Disabled	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Log Server	Indicates the IP address and port of the remote logging machine to which the phone sends log messages. These log messages help in debugging the Peer Firmware Sharing feature. **Note** The remote logging setting does not affect the sharing log messages sent to the phone log.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
LLDP: PC Port	Enables and disables Link Layer Discovery Protocol (LLDP) on the PC port. Use this setting to force the phone to use a specific discovery protocol. Settings include: • Enabled—default • Disabled	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration.**

Table 4-19 Network Configuration Menu Options (continued)

Option	Description	To Change
LLDP-MED: SW 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.**
LLDP Asset ID	Identifies the asset ID assigned to the phone for inventory management.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
Wireless Headset Hookswitch Control	Enables users to receive notifications of incoming calls and answer or end calls while working in a wireless environment.	From Cisco Unified Communications Manager Administration, choose **Device** > **Phone** > **Phone Configuration**.
LLDP Power Priority	Advertises the phone's power priority to the switch, enabling the switch to appropriately provide power to the phones. Settings include: • Unknown—default • Low • High • Critical	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
IP Addressing Mode	Displays the IP addressing mode that is available on the phone—IPv4 only, IPv6 only, or IPv4 and IPv6.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Common Device Configuration**.
IP Addressing Mode Preference for Signaling	Indicates the IP address version that the phone uses during signaling with Cisco Unified Communications Manager when both IPv4 and IPv6 are available on the phone. Displays one of the following options on the phone: • Use System Default—The dual-stack phone uses the default system addressing • IPv4—The dual-stack phone prefers to establish a connection via an IPv4 address during a signaling event • IPv6—The dual-stack phone prefers to establish a connection via an IPv6 address during a signaling event Default: Use System Default	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Common Device Configuration**.

Table 4-19 Network Configuration Menu Options (continued)

Option	Description	To Change
Auto IP Configuration	Displays whether the auto configurations is enabled or disabled on the phone. The Auto IP Configuration setting along with the DHCPv6 setting determine how the IP Phone obtains its IPv6 address and other network settings. For more information on how these two settings affect the network settings on the phone, see Table 4-5. **Note** Use the "Allow Auto-Configuration for Phones" setting in Cisco Unified Communications Manager Administration.	From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Common Device Configuration**.
IPv6 Load Server	Used to optimize installation time for phone firmware upgrades and off load the WAN by storing images locally, negating the need to traverse the WAN link for each phone's upgrade. You can set the Load Server to another TFTP server IP address or name (other than the IPv6 TFTP Server 1 or IPv6 TFTP Server 2) from which the phone firmware can be retrieved for phone upgrades. When the Load Server option is set, the phone contacts the designated server for the firmware upgrade. **Note** The Load Server option allows you to specify an alternate TFTP server for phone upgrades only. The phone continues to use IPv6 TFTP Server 1 or IPv6 TFTP Server 2 to obtain configuration files. The Load Server option does not provide management of the process and of the files, such as file transfer, compression, or deletion. **Note** When you configure both an IPv6 Load Server and a Load Server (for IPv4), the IPv6 Load server takes precedence.	Use Cisco Unified Communications Manager Administration to modify.
IPv6 Log Server	Indicates the IP address and port of the remote logging machine to which the phone sends log messages. These log messages help in debugging the peer to peer image distribution feature. **Note** The remote logging setting does not affect the sharing log messages sent to the phone log.	Use Cisco Unified Communications Manager Administration to modify.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Network Configuration Menu, page 4-5

Security Configuration Menu

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

Table 4-20 describes the options in this menu.

Note The phone also has a Security Configuration menu that you access from the Device menu. For information about the security options on that menu, see Security Configuration Menu, page 4-32.

Table 4-20 Security Menu Settings

Option	Description	To Change
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.	For more information, see Disabling and Enabling Web Page Access, page 7-3.
Security Mode	Displays the security mode that is set for the phone.	From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**.
MIC	Indicates whether a manufacturing installed certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).	For information about how to manage the MIC for your phone, see Using the Certificate Authority Proxy Function in *Cisco Unified Communications Manager Security Guide*.
LSC	Indicates whether a locally significant certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).	For information about how to manage the LSC for your phone, see Using the Certificate Authority Proxy Function in *Cisco Unified Communications Manager Security Guide*.
CTL File	Displays the MD5 hash of the certificate trust list (CTL) file that is installed in the phone, and provides access to the CTL File submenu. If no CTL file is installed on the phone, this field displays No. If security is configured for the phone, the CTL file installs automatically when the phone reboots or resets.	For more information about this file, see Configuring the Cisco CTL Client in *Cisco Unified Communications Manager Security Guide*.) If a CTL file is installed on the phone, also provides access to the CTL File screen. For more information, see CTL File Submenu, page 4-40.
Trust List	The Trust List is a top-level menu that provides submenus for the CTL, ITL, and Signed Configuration files. The CTL File submenu displays the contents of the CTL file. The ITL File submenu displays contents of the ITL file. The CTL File and ITL File submenus also display the MD5 hash of the file. The MD5 hash value from the phone can be compared with the MD5 hash value of the file from the TFTP server to verify if the correct file is installed on the phone. The Signed Configuration File submenu displays the SRST certificate that is installed via the authenticated digitally signed configuration file.	For more information, see Trust List Menu, page 4-43.

Table 4-20 Security Menu Settings (continued)

Option	Description	To Change
VPN Configuration	Allows you to configure VPN configuration for this phone. (Supported only for the Cisco Unified IP Phone 7942G, 7945G, and 7962G.)	For more information, see the *Cisco Unified Communications Manager Security Guide*, Virtual Private Network Configuration.
802.1X Authentication	Allows you to enable 802.1X authentication for this phone.	See 802.1X Authentication and Status, page 4-44.
802.1X Authentication Status	Displays real-time status progress of the 802.1X authentication transaction.	Display only—Cannot configure.

CTL File Submenu

The CTL File screen includes the options described in Table 4-21.

If a CTL file is installed on the phone, you can access the CTL File submenu by pressing the **Settings** button and choosing **Security Configuration > Trust List**.

To exit the CTL File submenu, press the **Exit** softkey.

Table 4-21 CTL File Settings

Option	Description	To Change
Unified CM/TFTP Server	Common Name (from the Cisco Unified Communications Manager Certificate) of a Cisco Unified Communications Manager and TFTP server used by the phone. Also displays a certificate icon  if a certificate is installed for this server. If neither the primary TFTP (TFTP Server 1) server nor the backup TFTP server (TFTP Server 2) is listed in the CTL file, you must unlock the CTL file before you can save changes that you make to the TFTP Server 1 option or to the TFTP Server 2 option on the Network Configuration menu.	For information about changing these options, see Network Configuration Menu, page 4-5.
Application Server	Common Name (from the Cisco Unified Communications Manager Certificate) of the trusted application server used by the phone. Also displays a certificate  icon. A phone-trust certificate is used to authenticate application servers with which the phone communicates. One Application Server menu item appears for each phone-trust store whose certificates have been uploaded into Cisco Unified OS Administration and later downloaded into the phone's CTL file.	For more information about phone-trust certificates, see the following manuals: • *Cisco Unified Communications Operating System Administration Guide*, Security. • *Cisco Unified Communications Manager Security Guide*, Security Overview.

Unlocking the CTL and ITL Files

To unlock the CTL and ITL files from the Security Configuration screen, follow these steps:

Procedure

Step 1 Press **# to unlock options on the overall setting menu of the Cisco Unified IP Phone.

Step 2 Select **Trust List > CTL file or ITL file** (depending on which file is installed in your phone).

Note If both CTL and ITL files are installed in your phone, you can choose either option.

Step 3 Press **Unlock** softkey to unlock Trust List files on the phone. The CTL or ITL files, if installed on your phone, will be unlocked together.

Note When you press the **Unlock** softkey, it changes to **Lock**. If you decide not to change the TFTP server option, press the **Lock** softkey to lock the CTL file.

ITL File Submenu

The ITL File screen includes the options that are described in Table 4-22.

If an ITL file is installed on the phone, you can access the ITL File submenu by pressing the Settings button and choosing **Security Configuration > Trust List**.

Note The TFTP server generates the ITL file. The Trust Verification Service does not generate the ITL file.

Table 4-22 ITL File Settings

Option	Description	To Change
ITL File	Displays the MD5 hash of the Identity Trust List (ITL) file that is installed in the phone. If security is configured for the phone, the ITL file installs automatically when the phone reboots or resets. A locked padlock icon in this option indicates that the ITL file is locked. An unlocked padlock icon indicates that the ITL file is unlocked.	For more information about the ITL file, see Security by Default in *Cisco Unified Communications Manager Security Guide.*

Table 4-22 ITL File Settings

Option	Description	To Change
CAPF Server	Common Name (from the Cisco Unified Communications Manager Certificate) of the CAPF used by the phone. Also displays a certificate icon  if a certificate is installed for this server.	For more information about this server, see Using the Certificate Authority Proxy Function in *Cisco Unified Communications Manager Security Guide.*
Unified CM/TFTP Server	Common Name (from the Cisco Unified Communications Manager Certificate) of a Cisco Unified Communications Manager and TFTP server used by the phone. Also displays a certificate icon  if a certificate is installed for this server. If neither the certificate of TFTP (TFTP Server 1) nor the certificate of backup TFTP (TFTP Server 2) is not in the CTL or ITL file, you must unlock the CTL file.	For information about changing these options, see Network Configuration Menu, page 4-5.
Application Server	Common Name (from the Cisco Unified Communications Manager Certificate) of the trusted application server used by the phone. Also displays a certificate icon  . A phone-trust certificate is used to authenticate application servers with which the phone communicates. One Application Server menu item appears for each phone-trust store whose certificates have been uploaded into Cisco Unified OS Administration and later downloaded into the phone's ITL file.	For more information about phone-trust certificates, see the following manuals: • *Cisco Unified Communications Operating System Administration Guide*, Security. • *Cisco Unified Communications Manager Security Guide*, Security Overview.

Table 4-22 ITL File Settings

Option	Description	To Change
Trust Verification Service Server	Common Name (from the Cisco Unified Communications Manager Certificate) of the trusted application server used by the phone. Also displays a certificate icon  . A phone-trust TVS certificate is used to authenticate TVS servers with which the phone communicates. There can be more than one entry for the TVS servers.	For more information, see *Cisco Unified Communications Manager System Administrator Guide*.

Trust List Menu

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

The Trust List menu displays information about all of the servers that the phone trusts and includes the options described in Table 4-23.

To exit the Trust List menu, press the **Exit** softkey.

Table 4-23 Trust List Menu Settings

Option	Description	To Change
CAPF Server	Common Name (from the Cisco Unified Communications Manager Certificate) of the CAPF server used by the phone. Also displays a certificate icon  if a certificate is installed for this server.	For more information about this file, see Configuring the Cisco CTL Client in *Cisco Unified Communications Manager Security Guide*.
Unified CM/TFTP Server	Common Name (from the Cisco Unified Communications Manager Certificate) of a Cisco Unified Communications Manager and the TFTP server used by the phone. Also displays a certificate icon  if a certificate is installed for this server. If the certificate of the TFTP (TFTP Server 1) or the certificate of the backup TFTP (TFTP Server 2) is not in the CTL or ITL file, one of the files must be unlocked.	For more information about this file, see Configuring the Cisco CTL Client in *Cisco Unified Communications Manager Security Guide*.

Table 4-23 Trust List Menu Settings (continued)

Option	Description	To Change
SRST Router	Common Name (from the Cisco Unified Communications Manager Certificate) of the trusted SRST router that is available to the phone, if such a device has been configured in Cisco Unified Communications Manager Administration. Also displays a certificate icon  if a certificate is installed for this server.	For more information about this file, see Configuring the Cisco CTL Client in *Cisco Unified Communications Manager Security Guide*.
Application Server	Common Name (from the Cisco Unified Communications Manager Certificate) of the trusted application server used by the phone. Also displays a certificate  icon. A phone-trust certificate is used to authenticate application servers with which the phone communicates. One Application Server menu item appears for each phone-trust store whose certificates have been uploaded into Cisco Unified OS Administration and later downloaded into the Cisco Unified IP Phone CTL file.	For more information about phone-trust certificates, see the following manuals: • *Cisco Unified Communications Operating System Administration Guide*, Security. • *Cisco Unified Communications Manager Security Guide*, Security Overview.

802.1X Authentication and Status

The 802.1X Authentication and 802.1X Authentication Status menus allow you to enable 802.1X authentication and monitor its progress. These options are described in Table 4-24 and Table 4-25.

You can access the 802.1X Authentication settings by pressing the **Settings** button and choosing one of the following:

- To configure your 802.1x authentication, choose **Security Configuration > 802.1X Authentication**
- To view the transaction status of your 802.1x authentication, choose **Security Configuration > 802.1X Authentication Status.**

To exit these menus, press the **Exit** softkey.

Table 4-24 802.1X Authentication Settings

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

Table 4-25 describes the 802.1X Authentication Real-Time Status.

Table 4-25 802.1X Authentication Real-Time Status

Option	Description	To Change
802.1X Authentication Status	Real-time progress of the 802.1X authentication status, displaying one of the following states: • Disabled—802.1X is disabled and transaction was not attempted • Disconnected—Physical link is down or disconnected • Connecting—Trying to discover or acquire the authenticator • Acquired—Authenticator acquired, awaiting authentication to begin • Authenticating—Authentication in progress • Authenticated—Authentication successful or implicit authentication due to timeouts • Held—Authentication failed, waiting before next attempt (approximately 60 seconds)	Display only—Cannot configure.

VPN Configuration

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

Note VPN Client is supported only for the Cisco Unified IP Phones 7942G and 7962G.

You configure the VPN Client feature as needed. If it is enabled and the VPN Client mode is enabled on the phone, you are prompted for your credentials as follows:

- If your phone is located outside the corporate network, you are prompted at login to enter your credentials based on the authentication method that you configure on your phone.

If your phone is located inside the corporate network,

Note

- When the power is lost
  - If Auto Network Detection is disabled, you are prompted for credentials, and a VPN connection is possible.
  - If Auto Network Detection is enabled, you cannot connect through VPN so you are not prompted.

Connecting to VPN

Use this procedure to access the VPN Configuration settings and connect through VPN.

Step 1 Press the **Settings** button and choose **Security Configuration > VPN Configuration**.

Step 2 After the phone starts up and the VPN Login screen appears, enter your credentials based on the configured authentication method:

- Username and password—Enter your username and the password that your system administrator gave you.
- Password and certificate—Enter the password that your system administrator gave you. Your username is derived from the certificate.
- Certificate—If the phone uses only a certificate for authentication, you do not need enter authentication data. The VPN Login screen displays the status of the phone attempting the VPN connection.

Note When the power is lost or in some scenarios when the phone is reset, all stored credentials are removed.

Step 3 To establish the VPN connection, press the **Submit** softkey.

Step 4 To disable the VPN login process, press the **Cancel** softkey.

VPN Configuration Settings

Table 4-26 shows the VPN option on the Cisco Unified IP Phone.

Table 4-26 VPN Configuration Settings

Option	Description	To Change
VPN	Determines if the VPN Client is enabled or disabled: • Enable—Enables VPN feature. (When enabled, the Disable softkey is shown.) • Disable—Disables VPN feature (When disabled, the Enable softkey is shown). Settings do not have to be unlocked to set this option.	1. Choose **Settings > Security Configuration > VPN Configuration > VPN**. 2. Set the VPN option to Enabled or Disabled. If the feature is disabled on the Cisco Unified Communications Manager, this option is disabled.
Clear Username and Password	Clears the current username and password.	This option is inactive when the authentication method is certificate only, or if the feature is disabled on the Cisco Unified Communications Manager.
Auto Network Detection	Shows if option is Enabled or Disabled.	Display only—Configured on Cisco Unified Communications Manager.

Table 4-26 VPN Configuration Settings (continued)

Option	Description	To Change
Concentrator 1 Concentrator 2 Concentrator 3	Allows you to see if concentrator 1, 2, or 3 is Connected or Inactive and view the concentrator details. In the VPN Configuration menu, choose **Concentrator 1**, **Concentrator 2**, or **Concentrator 3**, as desired: • For a configured concentrator, a status of Connected or Inactive displays on the VPN Configuration screen. • For an unconfigured concentrator, no status displays, and the Select softkey is inactive.	For configured concentrators, press the **Select** softkey to view concentrator details. A new screen appears that has a title of "Concentrator X," where X is the concentrator number. The URL configured for the concentrator displays in the window with the link to the URL on the first line and the URL itself on the second line.
Authentication Mode	Shows the authentication method: • Certificate • Username and Password • Password and Certificate	Display only—Configured on Cisco Unified Communications Manager.
Encryption Method	Shows the encryption method if the VPN tunnel is connected: • AES128-SHA • AES256-SHA • DES-CBC3-SHA If VPN is not connected, no method is shown.	Displays the encryption method only if a VPN tunnel is connected; otherwise, no value is displayed.

CHAPTER 5

Configuring Features, Templates, Services, and Users

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

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

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

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

This chapter includes following topics:

Telephony Features Available for the Cisco Unified IP Phone

After you add Cisco Unified IP Phones to Cisco Unified Communications Manager, you can add functionality to the phones. Table 5-1 includes a list of supported telephony features, many of which you can configure using Cisco Unified Communications Manager Administration. The Reference column lists Cisco Unified Communications Manager and other documentation that contains configuration procedures and related information.

For information about using most of these features on the phone, see *Cisco Unified IP Phone 7962G, 7942G, 7961G, 7961G-GE, 7941G, and 7941G-GE User Guide*. For a comprehensive listing of features on the phone, see *Cisco Unified IP Phone Features A–Z*.

Note Cisco Unified Communications Manager Administration also provides service parameters that you can use to configure various telephony functions. For more information about service parameters and the functions that they control, see *Cisco Unified Communications Manager Administration Guide*.

Table 5-1 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 Phones.
Add Select to Join (Cisco Unified IP Phones 7961G-GE, 7961G, 7941G-GE, and 7941G Only)	Creates a conference by joining together existing calls that are on a single phone line.	For more information, see *Cisco Unified IP Phone Guide*, Basic Call Handling.
Agent Greeting	Allows an agent or administrator to create and play a prerecorded greeting automatically at the beginning of a call, such as a customer call, before the agent begins the conversation with the caller. An Agent can prerecord a single greeting or multiple ones as needed and create and update them. When a customer calls, both callers hear the prerecorded greeting. The agent can remain on mute until the greeting ends or answer the call over the greeting. All codecs supported for the phone are supported for Agent Greeting calls. To enable Agent Greeting in the Cisco Unified CM Administration application, choose **Device > Phone**, locate IP Phone that you want to configure. Scroll to the Device Information Layout pane and set Builtin Bridge to **On** or **Default**. If Builtin Bridge is set to **Default**, in the Cisco Unified CM Administration application, choose **System > Service Parameter** and select the appropriate Server and Service. Scroll to the Clusterwide Parameters (Device - Phone) pane and set Builtin Bridge Enable to **On**.	For more information, see: • *Cisco Unified Communications Manager Features and Services Guide*, Barge and Privacy. • *Cisco Unified Communications Manager System Guide,* Cisco Unified IP Phones.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Anonymous Call Block (SIP Phones only)	Allows a user to reject calls from anonymous callers.	See *Cisco Unified Communications Manager Administration Guide,* SIP Profile Configuration.
Any Call Pickup	Allows users to pick up a redirected call via the Computer Telephony Integration (CTI) application, on any line in their call pickup group, regardless of how the call was routed to the phone.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, Call Pickup Configuration.
Assisted Directed Call Park	Enables users to park a call by pressing only one button using the Direct Park feature. You 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.
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*:* • *Cisco Unified Communications Manager System Guide,* Cisco Unified IP Phones*.* • *Cisco Unified Communications Manager Administration Guide,* Directory Number Configuration.
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 *Cisco Unified Communications Manager Administration Guide,* Directory Number Configuration.
Auto dial	Allows the phone user to choose from matching numbers in the Placed Calls log while dialing. To place the call, the user can choose a number from the Auto Dial list or continue to enter digits manually.	Requires no configuration.
Auto-pickup	Allows a user to use one-touch pickup functionality for call pickup features.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, Call Pickup.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Automatic Port Synchronization	When the Cisco Unified CM administrator uses the Remote Port Configuration feature to set the speed and duplex function of an IP Phone remotely, loss of packets can occur if one port is slower than the other. The Automatic Port Synchronization feature synchronizes the ports to the lowest speed among the two ports, which eliminates packet loss. When automatic port synchronization is enabled, it is recommended that both ports be configured for autonegotiate. If one port is enabled for autonegotiate and the other is at a fixed speed, the phone synchronizes to the fixed port speed. **Note** If both the ports are configured for fixed speed, the Automatic Port Synchronization feature is ineffective. **Note** The Remote Port Configuration and Automatic Port Synchronization features are compatible only with IEEE 802.3AF Power of Ethernet (PoE) switches. Switches that support only Cisco Inline Power are not compatible. Enabling this feature on phones that are connected to these types of switches could result in loss of connectivity to Cisco Unified CM, if the phone is powered by PoE.	To configure the parameter in the Cisco Unified CM Administration application, choose **Device > Phone**, select the appropriate IP Phones, and scroll to the Product Specific Configuration Layout pane. To configure the setting on multiple phones simultaneously, enable Automatic Port Synchronization in the Enterprise Phone Configuration (**System > Enterprise Phone Configuration**).
Barge (and cBarge)	Allows a user to join a non-private call on a shared phone line. Barge features include cBarge and Barge. • cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features. • Barge adds a user to a call but does not convert the call into a conference. The phones support Barge in two conference modes: • Built-in conference bridge at the target device (the phone that is being barged). This mode uses the **Barge** softkey. • Shared conference bridge. This mode uses the **cBarge** softkey.	For more information, see: • *Cisco Unified Communications Manager Administration Guide,* Cisco Unified IP Phone Configuration. • *Cisco Unified Communications Manager System Guide,* Cisco Unified IP Phones. • *Cisco Unified Communications Manager Features and Services Guide,* Barge and Privacy.
Block external to external transfer	Prevents users from transferring an external call to another external number.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, External Call Transfer Restrictions.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Busy Lamp Field (BLF)	Allows a user to monitor the call state of a directory number associated with a speed-dial button, call log, or directory listing on the phone.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, Presence.
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 *Cisco Unified Communications Manager Feature and Services Guide,* Call Pickup.
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 Phones. • *Cisco Unified Communications Manager Features and Services Guide*, Call Back.
Call Chaperone	Allows an authorized Chaperone user to supervise and record a call. The Call Chaperone user intercepts and answers the call from the calling party, manually creates a conference to the called party, and remains on the conference to supervise and record the call. Cisco Unified IP Phones that have the Call Chaperone feature configured on them have a Record softkey. The Call Chaperone user presses the Record softkey to record a call. For chaperoned calls, an announcement is played or spoken by one of the participants at the start of the call. An announcement will alert later participants in the call that the call is being recorded. The Call Chaperone feature is supported only with External Call Control, which allows Cisco Unified Communications Manager to route audio and video calls to a route server that hosts routing rules.	
Call display restrictions	Determines the information that displays 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.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Call forward	Allows users to redirect incoming calls to another number. Call forward options include Call Forward All, Call Forward Busy, Call Forward No Answer, and Call Forward No Coverage.	For more information, see: • *Cisco Unified Communications Manager Administration Guide,* Directory Number Configuration. • *Cisco Unified Communications Manager System Guide,* Cisco Unified IP Phones. • Specifying Options that Appear on the User Options Web Pages, page 5-30.
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 *Cisco Unified Communications Manager System Guide*, Cisco Unified IP Phones.
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 *Cisco Unified Communications Manager System Guide*, Cisco Unified IP Phones.
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,* Cisco Unified IP Phone Configuration. • *Cisco Unified Communications Manager System Guide*, Cisco Unified IP Phones.
Call forward all 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 *Cisco Unified Communications Manager System Guide*, Understanding Directory Numbers.
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 *Cisco Unified Communications Manager Features and Services Guide*, Call Park and Directed Call Park.
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 or visual alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group.	For more information, see *Cisco Unified Communications Manager Features and Services Guide,* Call Pickup Configuration.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

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 *Cisco Unified Communications Manager Features and Services Guide,* Monitoring and Recording.
Call Waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. Displays incoming call information on the phone screen.	For more information, see *Cisco Unified Communications Manager System Guide,* Understanding Directory Numbers.
Caller ID	Displays caller identification such as a phone number, name, or other descriptive text on the phone screen.	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.
Caller ID Blocking	Allows a user to block their phone number or e-mail address from phones that have caller identification enabled.	For more information, see: *Cisco Unified Communications Manager System Guide*, Understanding Route Plans. *Cisco Unified Communications Manager Administration Guide*, Directory Number Configuration. *Cisco Unified Communications Manager Administration Guide*, SIP Profile Configuration.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Calling Party Normalization	Globalizes or localizes the incoming calling party number so that the appropriate calling number presentation displays on the phone. Supports the international escape character +.	For more information, see *Cisco Unified Communications Features and Services Guide*, Calling Party Normalization.
Cisco Extension Mobility	Allows a user to temporarily apply a phone number and user profile settings to a shared Cisco Unified IP Phone by logging into the Extension Mobility service on that phone. 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 *Cisco Unified Communications Manager Features and Services Guide,* Cisco Extension Mobility.
Cisco Extension Mobility Change PIN	Enables a user to change the PIN from a Cisco Unified IP Phone. The PIN can be changed by: • Using the Change Credentials service of a Cisco Unified IP Phone • Using the **ChangePIN** softkey on the Extension Mobility logout screen	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, Cisco Extension Mobility.
Cisco Extension Mobility Cross Cluster	Enables a user configured in a home cluster to log into a Cisco Unified IP Phone in another visiting cluster. Before you configure Extension Mobility Cross Cluster (EMCC), configure Cisco Extension Mobility on the Cisco Unified IP Phones. **Note** Even though the Intercom feature works with Cisco Extension Mobility (EM), it cannot be used with EMCC because the feature must be enabled with a real phone device. The Intercom feature cannot be enabled with EM profiles.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, Cisco Extension Mobility Cross Cluster.
Cisco Unified Communications Manager Assistant	Enables managers and their assistants to work together more effectively by providing a call-routing service, enhancements to phone capabilities for the manager, and desktop interfaces that are primarily used by the assistant.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, Cisco IP Manager Assistant With Proxy Line Support and Cisco IP Manager Assistant With Shared Line Support.
Client matter codes (CMC) (SCCP phones only)	Enables a user to specify that a call relates to a specific client matter. **Note** If you are using this feature, you must disable Enbloc dialing. See Enbloc Dialing for details.	For more information, see *Cisco Unified Communications Manager Features and Services Guide,* Client Matter Codes and Forced Authorization Codes.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Conference	• Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference, Join, cBarge, and Meet-Me. • Allows a non-initiator 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.	• For more information, see *Cisco Unified Communications Manager System Guide*, Cisco Unified IP Phones. • The service parameter, Advance Adhoc Conference, (disabled by default in Cisco Unified Communications Manager Administration) allows you to enable these features. For complete information, see the *Cisco Unified Communications Manager System Guide*, Conference Bridges. **Note** Be sure to inform your users whether these features are activated.
Configurable call forward 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,* Cisco Unified IP Phone Configuration. • *Cisco Unified Communications Manager System Guide*, Cisco Unified IP Phones.
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.
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 *Cisco Unified Communications Manager Features and Services Guide,* Call Park and Directed Call Park.
Directed Call Pickup	Allows a user to answer a call that is ringing on a particular directory number.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, Call Pickup.
Direct transfer	Allows users to connect two calls to each other (without remaining on the line).	For more information, see *Cisco Unified Communications Manager System Guide*, Cisco Unified IP Phones.
Distinctive ring	Users can customize how their phone indicates an incoming call and a new voice mail message. Users can customize up to six distinctive rings.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, Custom Phone Rings.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Do Not Disturb (DND)	When DND is turned on, either no audible rings occur during the ringing-in state of a call, or no audible or visual notifications of any type occur. You can configure the phone to have a softkey template with a DND softkey or 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. From Cisco Unified Communications Manager Administration, choose **Device > Phone > Phone Configuration**. • DND Option—Choose "Call Reject" (to turn off all audible and visual notifications), or "Ringer Off" (to turn off only the ringer). *DND Option* appears on both the Common Phone Profile window and the Phone Configuration window (Phone Configuration window value takes precedence). • 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 *Cisco Unified Communications Manager Features and Services Guide*, Do Not Disturb.
Enbloc Dialing (SCCP phones only)	Enbloc dialing enables SCCP to send all digits of a phone number simultaneously. This feature must be disabled if either Forced Authorization Codes (FAC) or Client Matter Codes (CMC) dialing is being used.	1. To disable enbloc dialing, in Cisco Unified Communications Manager Administration, go to **Device > Phone.** 2. On the Phone Configuration window, in the "Product Specific Configuration Layout" area, uncheck the "Enbloc Dialing" check box, then click **Apply Config**, then click **Save**.
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: • *Cisco Unified Communications Manager Administration Guide,* Cisco Unified IP Phone Services Configuration. • *Cisco Unified Communications Manager System Guide,* Cisco Unified IP Phone Services.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Forced authorization codes (FAC) (SCCP phones only)	Controls the types of calls that certain users can place. **Note** If you are using this feature, you must disable Enbloc dialing. See Enbloc Dialing for details.	For more information, see *Cisco Unified Communications Manager Features and Services Guide,* Client Matter Codes and Forced Authorization Codes.
Group call pickup	Allows a user to answer a call that is ringing on a directory number in another group.	For more information, see *Cisco Unified Communications Manager Features and Services Guide,* Call Pickup.
Headset Sidetone Level	Enables administrators to configure a higher sidetone level for user headsets on these Cisco Unified IP Phones 7941G, 7941G-GE, 7961G, and 7961G-GE: • High—Increases the voice level played back in the headset, which encourages a lower speaking voice and is desirable in environments such as call centers. • Use Phone Default—Maintains the existing voice level played back in the headset. While some users prefer the higher voice level in the headset, other users may find the level to be uncomfortable or they may hear an echo. In this case, administrators should return the setting to Use Phone Default. Typically, only call centers should use the High setting with the higher voice level played back in the headset.	To configure the parameter in the Cisco Unified CM Administration application, choose **Device > Phone**, select the appropriate IP Phones, and scroll to the Product Specific Configuration Layout pane.
Help system	Provides a comprehensive set of topics that appear on the phone screen	Requires no configuration.
Hold/Resume	Allows the user to move a connected call from an active state to a held state.	• Requires no configuration, unless you want to use music on hold. See Music-on-Hold in this table for information. • See Hold Reversion in this table.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Hold Reversion	Limits the amount of time that a call can be on hold before reverting back to the phone that put the call on hold and alerting the user. Reverting calls are distinguished from incoming calls by a single ring (or beep, depending on the new call indicator setting for the line). This notification repeats at intervals as long as the call is not resumed. A call that triggers Hold Reversion also displays an animated icon in the call bubble and a brief message on the status line. You can configure call focus priority to favor incoming or reverting calls.	For more information about configuring this feature, see *Cisco Unified Communications Manager Features and Services Guide,* Hold Reversion.
Hold Status	Enables phones with a shared line to distinguish between the local and remote lines that placed a call on hold.	No configuration is required.
Hunt Group Display	Provides load sharing for calls to a main directory number. A hunt group contains a series of directory numbers that can answer the incoming calls. When an incoming call is offered to a directory number that is part of the hunt group, this feature displays the main directory number in addition to the calling party.	For more information, see: • *Cisco Unified Communications Manager Administration Guide,* Hunt List Configuration. • *Cisco Unified Communications Manager System Guide,* Understanding Route Plans. • *Cisco Unified Communications Manager Administration Guide*, CTI Route Point Configuration.
Immediate 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 *Cisco Unified Communications Manager Features and Services Guide*, Immediate Divert.
Immediate Divert—Enhanced	Allows users to transfer incoming calls directly to their voice messaging system or to the voice messaging system of the original called party.	For more information, see *Cisco Unified Communications Manager System Guide,* Cisco Unified IP Phones.
Intelligent Session Control	Reroutes a direct call to a user's mobile phone to the enterprise number (desk phone). For an incoming call to a remote destination (mobile phone), only the remote destination rings; the desk phone does not ring. When the call is answered on the mobile phone, the desk phone displays a Remote in Use message. During these calls, a user can use the various features of the mobile phone.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, Cisco Unified Mobility.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Intercom	Allows users to place and receive intercom calls using programmable phone buttons. You can configure intercom line buttons to: • Directly dial a specific intercom extension. • Initiate an intercom call and then prompt the user to enter a valid intercom number. **Note** If your user logs into the same phone on a daily basis using their Cisco Extension Mobility profile, assign the phone button template that contains intercom information to their profile, and assign the phone as the default intercom device for the intercom line.	*Cisco Unified Communications Manager Feature and Services Guide*, Intercom.
Join/Select	Allows a user to join two or more calls that are on one line to create a conference call and remain on the call.	For more information: • See Configuring Softkey Templates, page 5-27. • See *Cisco Unified Communications Manager System Guide,* Cisco Unified IP Phones.
Join Across Lines/Select	Allows users to apply the Join feature to calls that are on multiple phone lines.	For more information: • See the Configuring Softkey Templates, page 5-27. • See *Cisco Unified Communications Manager System Guide*, Cisco Unified IP Phones.
Line select	If this feature is disabled (default), then the ringing line is selected. When enabled, the primary line is picked up even if a call is ringing on another line. The user must manually select the other line. **Note** This feature can also be enabled or disabled for Extension Mobility.	For more information, see the option "Always use prime line" in the following chapters of *Cisco Unified Communications Manager Administration Guide*: • Device Profile Configuration • Common Phone Profile Configuration • Cisco Unified IP Phone Configuration
Line select for voice messages	When disabled (default), pressing the Messages button selects the line that has a voice message. If more than one line has voice mail, then the first available line is selected. When enabled, the primary line is always used to retrieve voice messages. **Note** This feature can also be enabled or disabled for Extension Mobility.	For more information, see the option "Always use prime line for voice message" in the following chapters of *Cisco Unified Communications Manager Administration Guide*: • Device Profile Configuration • Common Phone Profile Configuration • Cisco Unified IP Phone Configuration

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Log out of hunt groups	Allows users to log out of a hunt group and temporarily block calls from ringing their phone when they are not available to take calls. Logging out of hunt groups does not prevent non-hunt group calls from ringing their phone.	For more information • See Configuring Softkey Templates, page 5-27. • *Cisco Communications Manager System Guide,* Understanding Route Plans.
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 Phones. • *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 *Cisco Unified Communications Manager Administration Guide*, Meet-Me Number/Pattern Configuration.
Message Waiting	Defines directory numbers for message-waiting on and message-waiting off indicator. A directly connected voice-messaging system uses the specified directory number to set or to clear a message-waiting indication for a particular Cisco Unified IP Phone.	For more information, 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.
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 *Cisco Unified Communications Manager Administration Guide*, Directory Number Configuration.
Mobile Connect	Enables users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and a remote device such as a mobile phone. Users can restrict the group of callers according to phone number and time of day.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, Cisco Unified Mobility.
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 *Cisco Unified Communications Manager Features and Services Guide*, Cisco Unified Mobility.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
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 *Cisco Unified Communications Manager Features and Services Guide,* Multilevel Precedence and Preemption.
Multiple calls per line appearance	Each line can support multiple calls. Only one call can be active at any time; other calls are automatically placed on hold.	For more information see *Cisco Unified Communications Manager System Guide*, Understanding Directory Numbers.
Music on hold	Plays music while callers are on hold.	For more information see *Cisco Unified Communications Manager Features and Services Guide*, Music On Hold.
Mute	Mutes the microphone located in the active handset or headset.	Requires no configuration.
Onhook call transfer	Allows a user to press a single Transfer softkey and then go on hook to complete a call transfer.	For more information see *Cisco Unified Communications Manager System Guide,* Cisco Unified IP Phones.
Onhook predialing	Allows a user to dial a number without going off hook. The user can then either pick up the handset or press the Dial softkey.	For more information, see *Cisco Unified IP Phone Guide*, Basic Call Handling.
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 *Cisco Unified Communications Manager Features and Services Guide*, Call Pickup.
Phone secure web access	Enables a user to securely access the web with the use of a phone trust store called “phone-trust.”	*Cisco Unified Communications Manager Security Guide*, Product Security Overview.
Plus Dialing	Allows the user to dial E.164 numbers prefixed with a “+” sign. To dial the + sign, the user needs to press and hold the “*” key for at least 1 second. This applies to dialing the first digit for an on-hook or off-hook call only.	Requires no configuration.
Presence-enabled directories	Allows a user to monitor the call state of another directory number (DN) listed in call logs, speed-dials, and corporate directories. The Busy Lamp Field (BLF) for the DN displays the call state.	For more information, see *Cisco Unified Communications Manager Features and Services Guide*, Presence.
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.	See the Configuring PLAR section in Directory Number Configuration in *Cisco Unified Communications Manager Administration Guide,* for instructions on how to configure PLAR.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Privacy	Prevents users who share a line from adding themselves to a call and from viewing information on their phone screens about the call of the other user.	For more information see: • *Cisco Unified Communications Manager Administration Guide*, Cisco Unified IP Phone Configuration. • *Cisco Unified Communications Manager System Guide,* Cisco Unified IP Phones. • *Cisco Unified Communications Manager Features and Services Guide* Barge and Privacy.
Programmable line keys (PLK)	The administrator can assign features to line buttons. Softkeys normally control these features; for example, New Call, Call Back, End Call, and Forward All. When the administrator configures these features on the line buttons, they always remain visible, so users can have a hard feature key (for example, a hard New Call key).	For more information, see: • *Cisco Unified Communications Manager System Guide,* Cisco Unified IP Phones. • *Cisco Unified Communications Manager Administration Guide*, Phone Button Template Configuration. • *Cisco Unified Communications Manager Administration Guide*, Modifying Phone Button Templates.
Protected calling	Provides a secure (encrypted) connection between two phones. A security tone plays at the beginning of the call to indicate that both phones are protected. Some features, such as conference calling, shared lines, Extension Mobility, and Join Across Lines are not available when protected calling is configured. Protected calls are not authenticated.	For more information about security, see Overview of Supported Security Features, page 1-13. For additional information, see *Cisco Unified Communications Manager Security Guide.*
Quality Reporting Tool (QRT)	Allows users to use the **QRT** softkey on a phone to submit information about problem phone calls. QRT can be configured for either of two user modes, depending upon the amount of user interaction desired with QRT.	For more information see: • *Cisco Unified Communications Manager System Guide,* Cisco Unified IP Phones. • *Cisco Unified Communications Manager Features and Services Guide,* Quality Report Tool.
Redial	Allows users to call the most recently dialed phone number by pressing a button.	Requires no configuration.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

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 CM Administration. This enhances the performance for large deployments with specific port settings. **Note** If the ports are configured for Remote Port Configuration in Cisco Unified CM, the data cannot be changed on the phone.	To configure the parameter in the Cisco Unified CM Administration application, choose **Device > Phone**, select the appropriate IP Phones, and scroll to the Product Specific Configuration Layout pane (Switch Port Remote Configuration or PC Port Remote Configuration). To configure the setting on multiple phones simultaneously, configure the Remote Port Configuration in the Enterprise Phone Configuration (**System > Enterprise Phone Configuration**).
Ring setting	Identifies the 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. • *Cisco Unified Communications Manager Features and Services Guide,* Custom Phone Rings. • Creating Custom Phone Rings, page 6-2.
Ringer Volume Control	Enables you to control the minimum ringer-volume setting and adjust the minimum volume level for the ringer. Individual users cannot make the changes to the minimum ringer-volume setting. The parameter, Minimum Ring Volume, exists in the Cisco Unified Communications Manager Administration, Product Configuration window. When a user presses the minus (–) side of the Volume button to reduce the ringer volume in an on-hook state, the volume decreases only to the configured minimum volume-level setting. When the minimum volume level is reached, no status message appears. After a system restart, the minimum ringer volume resets to the minimum ringer-volume setting that is received from the configuration file. If you configure a new minimum volume level after the last startup and the end user had previously set the minimum ringer volume lower, the ringer volume will be set to the minimum value from the configuration file, not to the level set by the user. This feature does not apply to handset, speaker, and headset volumes during calls.	To configure the parameter in the Cisco Unified CM Administration application, choose **Device > Phone**, select the appropriate IP Phones, and scroll to the Product Specific Configuration Layout pane.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Secure and Nonsecure Indication Tone	When a phone is configured as secure (encrypted and trusted) in Cisco Unified CM, it can be given a protected status. After that, if desired, the protected phone can be configured to play an indication tone at the beginning of a call. Only protected phones hear these secure or nonsecure indication tones. Nonprotected phones never hear tones. If the overall call status changes during the call, the indication tone changes accordingly. At that time, the protected phone plays the appropriate tone. A protected phone plays or does not play a tone under these circumstances: • When the Play Secure Indication Tone option is enabled (True): – When end-to-end secure media is established and the call status is secure, the phone plays the secure indication tone (three long beeps with pauses). – When end-to-end nonsecure media is established and the call status is nonsecure, the phone plays the nonsecure indication tone (six short beeps with brief pauses). • If the Play Secure Indication Tone option is disabled, no tone is played.	• Protected Device—To change the status of a secure phone to protected, check the "Protected Device" check box in **Cisco Unified Communications Manager Administration > Device > Phone > Phone Configuration.** • Play Secure Indication Tone—To enable the protected phone to play a secure or nonsecure indication tone, set the Play Secure Indication Tone to True. (The default is False.) You set this option in **Cisco Unified Communications Manager Administration > System > Service Parameters**. Select the server and then the Unified CM service. In the Service Parameter Configuration window, select the option in the Feature - Secure Tone area. (The default is False.)
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 non-secure participants from the Conference List. Non-initiators can add or remove conference participants if the Advanced Adhoc Conference Enabled parameter is set.	For more information about security, see Overview of Supported Security Features, page 1-13. For additional information, see: • *Cisco Unified Communications Manager System Guide,* Conference Bridges. • *Cisco Unified Communications Manager Administration Guide,* Conference Bridge Configuration. • *Cisco Unified Communications Manager Security Guide.*

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
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 see: • *Cisco Unified Communications Manager Administration Guide,* Cisco Unified IP Phone Configuration. • *Cisco Unified Communications Manager System Guide,* Cisco Unified IP Phone Services.
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: • *Cisco Unified Communications Manager Administration Guide,* Cisco Unified IP Phone Configuration. • *Cisco Unified Communications Manager System Guide,* Cisco Unified IP Phone Services.
Session Handoff	Allows users to switch calls from a mobile phone to Cisco Unified devices that share the same line. Handsets on all the devices on the shared line flash simultaneously. After a user answers the call from one of the Cisco Unified devices, the other Cisco Unified devices that share the same line display a Remote in Use message. However, if the call fails to switch from the mobile phone, the mobile phone may display a Cannot Move Conversation message.	For more information, see: *Cisco Unified Communications Manager Features and Services Guide*, Cisco Unified Mobility and Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator Integration.
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 *Cisco Unified Communications Manager System Guide,* Understanding Directory Numbers.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Silent Monitoring	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, 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 *Cisco Unified Communications Manager Features and Services Guide,* Monitoring and Recording.
Single Button Barge	Allows users to press a line key to Barge or cBarge into a remote-in-use call on a shared line.	For more information, see: • *Cisco Unified Communications Manager Administration Guide*, Device Pool Configuration. • *Cisco Unified Communications Manager System Guide*, Cisco Unified IP Phones. • *Cisco Unified Communications Manager Features and Services Guide*, Barge and Privacy.
Speed-dialing	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 Phones.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
SSH Access	Allows the administrator to enable or disable the SSH Access setting using the Cisco Unified CM Administration application. This option indicates whether the phone supports the SSH Access. Settings include: • Enabled • Disabled—default When enabled, it allows the phone to accept the SSH connections. Disabling the SSH server functionality of the phone blocks the SSH access to the phone.	To configure the parameter in the Cisco Unified CM Administration application, choose **Device > Phone**, select the appropriate IP Phones, scroll to the **Product Specific Configuration Layout** pane and select **Enable** from the **SSH Access** drop-down list box. If you set the same parameter in the Common Phone Profile window (**Device > Device Settings > Common Phone Profile**), the precedence order of the settings is: 3. Phone Configuration window settings 4. Common Phone Profile window settings
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 *Cisco Unified Communications Manager Administration Guide*, Date/Time Group Configuration.
Transfer	Allows users to redirect connected calls from their phones to another number.	Requires no configuration.
UCR 2008	The IP Phones using SCCP support Unified Capabilities Requirements (UCR) 2008 by providing the following functions: • Support for Federal Information Processing Standard (FIPS) 104-2 • Support for TVS IPv6 • Support for 80-bit SRTCP Tagging As an IP Phone administrator, some of these functions require you to set up specific parameters in Cisco Unified Communications Manager Administration.	See Setting up UCR 2008, page 5-34
Video mode (SCCP phones only)	Allows a user to select the video display mode for viewing a video conference, depending on the modes configured in the system.	For more information: • See *Cisco Unified Communications Manager Administration Guide,* Conference Bridge Configuration. • See *Cisco Unified Communications Manager System Guide,* Understanding Video Telephony.

Table 5-1 Telephony Features for the Cisco Unified IP Phone (continued)

Feature	Description	Configuration Reference
Video Support (SCCP phones only)	Enable video support on the phone.	For more information see: • *Cisco Unified Communications Manager Administration Guide,* Conference Bridge Configuration. • *Cisco Unified Communications Manager System Guide,* Understanding Video Telephony. • *Cisco VT Advantage Administration Guide*.
Voice messaging 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. • *Cisco Unified Communications Manager System Guide*, Voice Mail Connectivity to Cisco Unified Communications Manager.
VPN client	Provides a VPN connection using SSL on the Cisco Unified IP Phones 7942G and 7962G for situations in which a phone is located outside a trusted network or when network traffic between the phone and Cisco Unified Communications Manager must cross untrusted networks. (Supported only for the Cisco Unified IP Phones 7942G and 7962G.)	For more information, see the *Cisco Unified Communications Manager Security Guide*, Configuring Virtual Private Networks.

Configuring Product Specific Configuration Parameters

Cisco Unified Communications Manager Administration allows you to set some product specific configuration parameters for Cisco Unified IP Phones. Table 5-2 lists the configuration windows, their paths, and the parameters in Cisco Unified Communications Manager Administration.

Table 5-2 Configuration parameters for Cisco Unified IP Phones

Configuration Window	Path	Parameters
Enterprise Phone Configuration window	**System > Enterprise Phone Configuration**	You can set the following parameters in any of the three configuration windows: • Settings Access • Video Capabilities • Web Access • Load Server • RTCP • Peer Firmware Sharing • Cisco Discovery Protocol (CDP): Switch Port • Cisco Discovery Protocol (CDP): PC Port • Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port • Link Layer Discovery Protocol (LLDP): PC Port • IPv6 Load Server • 802.1x Authentication • Switch Port Remote Configuration • PC Port Remote Configuration • Automatic Port Synchronization When you set the parameters, select the Override Common Settings check box for each setting you wish to update. If you do not check this box, the corresponding parameter setting does not take effect. If you set the parameters at the three configuration windows, the setting takes precedence in the following order: • Phone Configuration window • Common Phone Profile window • Enterprise Phone Configuration window
Common Phone Profile window	**Device > Device Settings > Common Phone Profile**	
Phone Configuration window	**Device > Phone**; Product Specific Configuration portion of window	

Configuring Corporate and Personal Directories

The **Directories** button on the Cisco Unified IP Phones 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. See Configuring Corporate Directories, page 5-24 for more information.

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

  To support this feature, you must provide the user with software to configure the personal directory. See Configuring Personal Directory, page 5-24 for more information.

Configuring Corporate Directories

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

To install and set up these features, see LDAP System Configuration, LDAP Directory Configuration, and LDAP Authentication Configuration in *Cisco Unified Communications Manager Administration Guide*.

After the LDAP directory configuration completes, users can use the Corporate Directory service on their Cisco Unified IP Phones to look up users in the corporate directory.

Configuring Personal Directory

Personal Directory consists of the following features:

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

Users can access Personal Directory features by these methods:

- From a web browser—Users can access the PAB and Fast Dials features from the Cisco Unified Communications Manager User Options web pages
- From the Cisco Unified IP Phone—Users can choose **Directories > Personal Directory** to access the PAB and Fast Dials features from their phones
- From a Microsoft Windows application—Users can use the TABSynch tool to synchronize their PABs with Microsoft Windows Address Book (WAB). Customers who want to use the Microsoft Outlook Address Book (OAB) should begin by importing the data from the OAB into the Windows Address Book (WAB). TabSync can then be used to synchronize the WAB with Personal Directory.

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

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

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

Modifying Phone Button Templates

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** from 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. See *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager System Guide* for more information.

Cisco Unified IP Phone 7962G

The default Cisco Unified IP Phone 7962G template that ships with the phone uses buttons 1 and 2 for lines and assigns buttons 3 through 6 as speed dial.

The recommended standard Cisco Unified IP Phone 7962G template uses buttons 1 and 2 for lines, assigns button 3 as speed dial, and buttons 4 through 6 as Hold, Conference, and Transfer, respectively.

Cisco Unified IP Phone 7942G

The default Cisco Unified IP Phone 7942G template that ships with the phone uses buttons 1 and 2 for lines.

The recommended standard Cisco Unified IP Phone 7942G template uses buttons 1 and 2 for lines.

Cisco Unified IP Phone 7961G /7961G-GE

The default template that ships with the 7961G/7961G-GE uses buttons 1 and 2 for lines and buttons 3 through 8 as speed dial.

The recommended standard Cisco Unified IP Phone 7961G/7961G-GE template uses buttons 1 and 2 for lines, assigns button 3 as speed dial, and buttons 4 through 6 as Hold, Conference, and Transfer, respectively.

Cisco Unified IP Phone 7941G/7941G-GE

The default template that ships with the Cisco Unified IP Phone 7941G/7941G-GE uses buttons 1 and 2 for lines.

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

For more information about softkey templates, see Configuring Softkey Templates, page 5-27.

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

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

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

Procedure

Step 1 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.

Step 4 Click **Save**.

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

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

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

Procedure

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

Step 2 Click **Find**.

Step 3 Select the phone model.

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

The Phone Button Template Configuration window opens.

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

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

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

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

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

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

For additional information on IP Phone services, see the *Cisco Unified Communications Manager Administration Guide,* IP Phone Services Configuration. For additional information on configuring line buttons, see the *Cisco Unified Communications Manager Administration Guide*, Cisco Unified IP Phone Configuration.

Configuring Softkey Templates

Using Cisco Unified Communications Manager Administration, you can manage softkeys associated with applications that are supported by the Cisco Unified IP Phone 7962G and 7942G.
Cisco Unified Communications Manager supports two types of softkey templates: standard and nonstandard. Standard softkey templates include Standard User, Standard Feature, Standard Assistant, Standard Manager, and Standard Shared Mode Manager. 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, choose **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. See *Cisco Unified Communications Manager Administration Guide*, *Cisco Unified Communications Manager System Guide* for more information.

Note The Cisco Unified IP Phones support all the softkeys that are configurable in Cisco Unified Communications Manager Administration.

Setting Up Services

The **Services** button on the Cisco Unified IP Phones gives users access to Cisco Unified IP Phone Services. You can also assign services to the programmable buttons on the phone. 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 by using the Cisco Unified Communications Manager User Options application. This web-based application provides a graphical user interface (GUI) for limited, end user configuration of IP Phone applications.

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. See *Cisco Unified Communications Manager Administration Guide* and to *Cisco Unified Communications Manager System Guide* for more information.

After you configure these services, verify that your users have access to the Cisco Unified CM User Options web-based application, from which they can select and subscribe to configured services. See How Users Subscribe to Services and Configure Phone Features, page A-3 for a summary of the information that you must provide to end users.

Cisco Unified IP Phones can support up to four HTTP/HTTPS active client connections and up to four HTTP/HTTPS active server connections at one time. A few examples of HTTP/HTTPS services include:

- Extension Mobility
- Directories
- Messages

Note To configure extension mobility services for users, see *Cisco Unified Communications Manager Features and Services Guide*.

Adding Users to Cisco Unified Communications Manager

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

- Access the corporate directory and other customized directories from a Cisco Unified IP Phone.
- Create a personal directory.
- Set up speed dial and call forwarding numbers.
- Subscribe to services that are accessible from a Cisco Unified IP Phone.

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

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

See *Cisco Unified Communications Manager Administration Guide* for more information about adding users. See *Cisco Unified Communications Manager System Guide* for details about user information.

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

  See *Cisco Unified Communications Manager Bulk Administration Guide* for details.

Managing the User Options Web Pages

From the User Options web page, users can customize and control several phone features and settings. For detailed information about the User Options web pages, see *Cisco Unified IP Phone 7962G, 7942G, 7961G, 7961G-GE, 7941G, and 7941G-GE User Guide*.

Giving Users Access to the User Options Web Pages

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

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

Procedure

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

The Find and List Users window displays.

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

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

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

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

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

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

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

Step 8 Click **Add Selected**.

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

Procedure

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

The Find and List Users window displays.

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

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

Step 4 Click **Device Association.**

The User Device Association window displays.

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

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

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

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

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

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

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

  These settings correspond to the values you entered when you added the user to Cisco Unified Communications Manager (see Adding Users to Cisco Unified Communications Manager, page 5-28).

For additional information, see:

- *Cisco Unified Communications Manager Administration Guide*, User Group Configuration.
- *Cisco Unified Communications Manager Administration Guide*, End User Configuration.
- *Cisco Unified Communications Manager System Guide*, Roles and User Groups.

Specifying Options that Appear on the User Options Web Pages

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

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

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

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

Procedure

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

The Enterprise Parameters Configuration window appears.

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

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

Enabling EnergyWise on the Cisco Unified IP Phone

To reduce power consumption, you can configure the phone to sleep (power down) and wake (power up) if your system includes an EnergyWise controller (for example, a Cisco Switch with the EnergyWise feature enabled).

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 sends back either an acceptance or a rejection of the request. If the switch rejects the request or does not reply, the phone does not power down. If the switch accepts the request, the idle phone goes to sleep, reducing its power consumption to a predetermined level. A phone that is not idle sets an idle timer, and goes to sleep after the timer expires.

At the scheduled wake time, the system restores power to the phone, waking it up. To wake up the phone before the wake time, you must power on the phone from the switch. For more information, see the switch documentation.

Table 5-3 explains the Cisco Unified Communications Manager Administration fields that control the EnergyWise settings. You configure these fields in Cisco Unified Communications Manager Administration by choosing **Device > Phone**. You can also configure EnergyWise parameters in the Enterprise Phone Configuration and Common Phone Profile Configuration windows.

Table 5-3 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 the days for the schedule. By default, no days are selected. When Enable Power Save is checked, you receive a message to warn about emergency (e911) concerns. ⚠ **Caution** While power save plus mode (the mode) is in effect, endpoints 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 are taking 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 will 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 selected 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.
Phone Off Time	The time of day that the phone powers down for the days 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 range of the field is 20 to 1440 minutes. The default value is 60 minutes.

Field	Description
Enable Audible Alert	When enabled, instructs the phone to play an audible alert starting at 10 minutes before the time specified in the Phone Off Time field. 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's designated volume level. The audible alert schedule is: • 10 minutes before power down, play the ringtone four times • 7 minutes before power down, play the ringtone four times • 4 minutes before power down, play the ringtone four times • 30 seconds before power down, play the ringtone 15 times or until the phone powers down 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 is 127 characters.
EnergyWise Secret	The security secret password that is used to communicate with the endpoints in the Energywise domain. The maximum length is 127 characters.
Allow EnergyWise Overrides	This check box determines whether you will allow the EnergyWise domain controller policy to send power-level updates to the phones. The following conditions apply: 1. If the phone is in Power Save or at full power and the level is set to any standby level, the phone will go to Power Save when idle and remain there until the next Unified CM scheduled power-level change or user interaction. 2. If the phone is in Power Save or at full power and the level is set to any nonoperational level, the phone will power down when idle and remain powered down until the switch reapplies power or the user wakes the phone. For example, assume 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 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 will remain in effect (assuming no phone user intervention occurs) until the configured Phone On Time at 6:00 a.m. • At 6 a.m., the phone will turn on and resume receiving its power-level changes from the settings in Cisco 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. Leaving the Allow EnergyWise Overrides checked with no days selected in the Enable Power Save Plus field does not disable Power Save Plus.

Setting up UCR 2008

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 5-4 UCR 2008 parameter location

Parameter	Administration Path	Procedure
FIPS Mode	Device > Device Settings > Common Phone Profile	Configuring UCR 2008 in Common Phone Profile, page 5-35
	System > Enterprise Phone Configuration	Configuring UCR 2008 in Enterprise Phone Configuration, page 5-35
SSH Access	Device > Phone	Configuring UCR 2008 in Phone, page 5-34
	Device > Device Settings > Common Phone Profile	Configuring UCR 2008 in Common Phone Profile, page 5-35
Web Access	Device > Phone	Configuring UCR 2008 in Phone, page 5-34 Disabling and Enabling Web Page Access, page 7-3
HTTPS Server	Device > Phone	Configuring UCR 2008 in Phone, page 5-34
	System > Enterprise Phone Configuration	Configuring UCR 2008 in Enterprise Phone Configuration, page 5-35
80-bit SRTCP	Device > Device Settings > Common Phone Profile	Configuring UCR 2008 in Common Phone Profile, page 5-35
	System > Enterprise Phone Configuration	Configuring UCR 2008 in Enterprise Phone Configuration, page 5-35
IP Addressing Mode	Device > Device Settings > Common Device Configuration	Network Configuration Menu, page 4-34
IP Addressing Mode Preference for Signaling	Device > Device Settings > Common Device Configuration	Network Configuration Menu, page 4-34

Configuring UCR 2008 in Phone

Use the following procedure to set the following UCR 2008 parameters:

- SSH Access
- Web Access
- HTTPS Server

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 Set the HTTPS Service parameter to **https only**.

Step 5 Click **Save**.

Configuring UCR 2008 in Common Phone Profile

Use the following procedure to set the following UCR 2008 parameters:

- FIPS Mode
- SSH Access
- 80-bit SRTCP

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 Click **Save**.

Configuring UCR 2008 in Enterprise Phone Configuration

Use the following procedure to set the following UCR 2008 parameters:

- FIPS Mode
- HTTPS Server
- 80-bit SRTCP

Step 1 Choose **Device > Device Settings > Common Phone Profile**.

Step 2 Set the FIPS Mode parameter to **Enabled**.

Step 3 Set the HTTPS Server parameter to **https only**.

Step 4 Set the 80-bit SRTCP parameter to **Enabled**.

Step 5 Click **Save**.

CHAPTER 6

Customizing the Cisco Unified IP Phones

This chapter explains how you customize configuration files, phone ring sounds, and background images at your site. Ring sounds play when the phone receives a call. Background images appear on the phone LCD screen.

This chapter includes these topics:

Customizing and Modifying Configuration Files

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

You can obtain a copy of the Ringlist.xml and List.xml files from the system using the following admin command-line interface (CLI) “file” commands:

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

Creating Custom Phone Rings

The Cisco Unified IP Phone ships with two default ring types that are implemented in hardware: Chirp1 and Chirp2. Cisco Unified Communications Manager also provides a default set of additional phone ring sounds that are implemented in software as pulse code modulation (PCM) files. The PCM files, along with an XML file (named Ringlist.xml) that describes the ring list options that are available at your site, exist in the TFTP directory on each Cisco Unified Communications Manager server.

For more information, see Custom Phone Rings in *Cisco Unified Communications Manager Features and Services Guide* and Software Upgrades in *Cisco Unified Communications Operating System Administration Guide.*

The following sections describe how you can customize the phone rings that are available at your site by creating PCM files and editing the Ringlist.xml file:

- Ringlist.xml File Format Requirements, page 6-2
- PCM File Requirements for Custom Ring Types, page 6-3
- Configuring a Custom Phone Ring, page 6-3

Ringlist.xml File Format Requirements

The Ringlist.xml file defines an XML object that contains a list of phone ring types. This file can include up to 50 ring types. Each ring type contains a pointer to the PCM file that is used for that ring type and the text that will appear on the Ring Type menu on a Cisco Unified IP Phone for that ring. The Cisco TFTP server for each Cisco Unified Communications Manager contains this file.

The CiscoIPPhoneRinglist XML object uses the following simple tag set to describe the information:

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName/>
      <FileName/>
   </Ring>
</CiscoIPPhoneRingList>
```

The following characteristics apply to the definition names. You must include the required DisplayName and FileName for each phone ring type.

- DisplayName defines the name of the custom ring for the associated PCM file that will display on the Ring Type menu of the Cisco Unified IP Phone.
- FileName specifies the name of the PCM file for the custom ring to associate with DisplayName.

Note The DisplayName and FileName fields must not exceed 25 characters.

This example shows a Ringlist.xml file that defines two phone ring types:

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName>Analog Synth 1</DisplayName>
      <FileName>Analog1.raw</FileName>
   </Ring>
   <Ring>
      <DisplayName>Analog Synth 2</DisplayName>
      <FileName>Analog2.raw</FileName>
   </Ring>
</CiscoIPPhoneRingList>
```

PCM File Requirements for Custom Ring Types

The PCM files for the rings must meet the following requirements for proper playback on Cisco Unified IP Phones:

- Raw PCM (no header)
- 8000 samples per second
- 8 bits per sample
- uLaw compression
- Maximum ring size—16080 samples
- Minimum ring size—240 samples
- Number of samples in the ring is evenly divisible by 240.
- Ring starts and ends at the zero crossing.

To create PCM files for custom phone rings, you can use any standard audio editing packages that support these file format requirements.

Configuring a Custom Phone Ring

To create custom phone rings for the Cisco Unified IP Phone, follow these steps:

Procedure

Step 1 Create a PCM file for each custom ring (one ring per file). Ensure the PCM files comply with the format guidelines that are listed in PCM File Requirements for Custom Ring Types, page 6-3.

Step 2 Upload the new PCM files that you created to the Cisco TFTP server for each Cisco Unified Communications Manager in your cluster. For more information, see Software Upgrades in *Cisco Unified Communications Operating System Administration Guide.*

Step 3 Use an text editor to edit the Ringlist.xml file. See Ringlist.xml File Format Requirements, page 6-2 for information about how to format this file and for a sample Ringlist.xml file.

Step 4 Save your modifications and close the Ringlist.xml file.

Step 5 To cache the new Ringlist.xml file, stop and start the TFTP service by using Cisco Unified Serviceability or disable and re-enable the “Enable Caching of Constant and Bin Files at Startup” TFTP service parameter (located in the Advanced Service Parameters).

Creating Custom Background Images

You can provide users with a choice of background images for the LCD screen on their phones. Users can select a background image by choosing **Settings > User Preferences > Background Images** on the phone.

The image choices that users see come from PNG images and an XML file (called List.xml) that are stored on the TFTP server used by the phone. By storing your own PNG files and editing the XML file on the TFTP server, you can designate the background images from which users can choose. In this way, you can provide custom images, such as your company logo.

The following sections describe how you can customize the background images that are available at your site by creating your own PNG files and editing the List.xml file:

- List.xml File Format Requirements, page 6-4.
- PNG File Requirements for Custom Background Images, page 6-5.
- Configuring a Custom Background Image, page 6-5

Note The XSI Screen Width Enhancement feature, when implemented on Cisco Unified IP Phones, enhances the viewability of the Messages, Directories, and Services screens. These screens may appear in Normal mode or in Wide mode, depending on how the phone is set up. For information, see Cisco Unified IP Phone Services Application Development Notes.

List.xml File Format Requirements

The List.xml file defines an XML object that contains a list of background images. The List.xml file is stored in the following subdirectory on the TFTP server:

/Desktops/320x196x4

Tip If you are manually creating the directory structure and the List.xml file, you must ensure that the directories and files can be accessed by the user\CCMService, which is used by the TFTP service.

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

The List.xml file can include up to 50 background images. The images are in the order that they appear in the Background Images menu on the phone. For each image, the List.xml file contains one element type, called ImageItem. The ImageItem element includes these two attributes:

- Image—Uniform resource identifier (URI) that specifies where the phone obtains the thumbnail image that will appear on the Background Images menu on a phone.
- URL—URI that specifies where the phone obtains the full size image.

The following example shows a List.xml file that defines two images. The required Image and URL attributes must be included for each image. The TFTP URI that is shown in the example is the only supported method for linking to full size and thumbnail images. HTTP URL support is not provided.

List.xml Example

```
<CiscoIPPhoneImageList>
<ImageItem Image="TFTP:Desktops/320x196x4/TN-Fountain.png"
URL="TFTP:Desktops/320x196x4/Fountain.png"/>
<ImageItem Image="TFTP:Desktops/320x196x4/TN-FullMoon.png"
URL="TFTP:Desktops/320x196x4/FullMoon.png"/>
</CiscoIPPhoneImageList>
```

The Cisco Unified IP Phone firmware includes a default background image. This image is not defined in the List.xml file. The default image is always the first image that appears in the Background Images menu on the phone.

PNG File Requirements for Custom Background Images

Each background image requires two PNG files:

- Full size image—Version that appears on the on the phone.
- Thumbnail image—Version that appears on the Background Images screen from which users can select an image. The thumbnail image must be 25% of the size of the full size image.

Tip Many graphics programs provide a feature that will resize a graphic. An easy way to create a thumbnail image is to first create and save the full size image, then use the sizing feature in the graphics program to create a version of that image that is 25% of the original size. Save the thumbnail version with a different name than the full size image.

The PNG files for background images must meet the following requirements for proper display on the Cisco Unified IP Phone:

- Full size image—320 pixels (width) X 196 pixels (height)
- Thumbnail image—80 pixels (width) X 49 pixels (height)

Tip If you are using a graphics program that supports a posterize feature for grayscale, set the number of tonal levels per channel to 16, and the image will posterize to 16 shades of grayscale.

Configuring a Custom Background Image

To create custom background images for the Cisco Unified IP Phone, follow these steps:

Procedure

Step 1 Create two PNG files for each image (a full size version and a thumbnail version). Ensure the PNG files comply with the format guidelines that are listed in PNG File Requirements for Custom Background Images, page 6-5.

Step 2 Upload the new PNG files that you created to the following subdirectory in the TFTP server for the Cisco Unified Communications Manager:

/Desktops/320x196x4

Note The file name and subdirectory parameters are case sensitive. Be sure to use the forward slash "/" when you specify the subdirectory path.

To upload the files, choose **Software Upgrades > Upload TFTP Server File** in Cisco Unified Communications Operating System Administration. For more information, see Software Upgrades in *Cisco Unified Communications Operating System Administration Guide*.

Note If the folder does not exist, the folder gets created and the files get uploaded to the folder.

Step 3 You must also copy the customized images and files to the other TFTP servers that the phone may contact to obtain these files.

Note Cisco recommends that you also store backup copies of custom image files in another location. You can use these backup copies if the customized files are overwritten when you upgrade Cisco Unified Communications Manager.

Step 4 Use a text editor to edit the List.xml file. See List.xml File Format Requirements, page 6-4 for the location of this file, formatting requirements, and a sample file.

Step 5 Save your modifications and close the List.xml file.

Note When you upgrade Cisco Unified Communications Manager, a default List.xml file will replace your customized List.xml file. After you customize the List.xml file, make a copy of the file and store it in another location. After upgrading Cisco Unified Communications Manager, replace the default List.xml file with your stored copy.

Step 6 To cache the new List.xml file, stop and start the TFTP service by using Cisco Unified Communications Manager Serviceability or disable and re-enable the Enable Caching of Constant and Bin Files at Startup TFTP service parameter (located in the Advanced Service Parameters).

Configuring Wideband Codec

If Cisco Unified Communications Manager has been configured to use G.722 (G.722 is enabled by default for the Cisco Unified IP Phone 7962G and 7942G) and if the far endpoint supports G.722, the call can connect using the G.722 codec in place of G.711. This situation occurs regardless of whether the user has enabled a wideband headset or wideband handset, but if either the headset or handset is enabled, the user may notice greater audio sensitivity during the call. Greater sensitivity means improved audio clarity but also means that more background noise can be heard by the far endpoint—noise such as rustling papers or nearby conversations. Even without a wideband headset or handset, some users may prefer the additional sensitivity of G.722. Other users may be distracted by the additional sensitivity of G.722.

Two parameters in Cisco Unified Communications Manager Administration affect whether wideband is supported for this Cisco Unified Communications Manager server or a specific phone:

- Advertise G.722 Codec—From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**. The default value of this enterprise parameter is True, which means that all Cisco Unified IP Phone models that are described in this administration guide and are registered to this Cisco Unified Communications Manager will advertise G.722 to Cisco Unified Communications Manager. For more information, see the *Cisco Unified Communications Manager System Guide*, Cisco Unified IP Phones chapter.
- Advertise G.722 Codec—From Cisco Unified Communications Manager Administration, choose **Device > Phone**. The default value of this product-specific parameter is to use the value specified in the enterprise parameter. If you want to override this on a per-phone basis, choose Enabled or Disabled in the Advertise G.722 Codec parameter on the Product Specific Configuration area of the Phone Configuration window.

CHAPTER 7

Monitoring the Cisco Unified IP Phones Remotely

Each Cisco Unified IP Phone has a web page from which you can view a variety of information about the phone, including:

- Device information
- Network configuration information
- Network statistics
- Device logs
- Streaming statistics

Note The Cisco Unified IP Phones does not support web access on its IPv6 address.

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 Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phones.

For more information about troubleshooting the Cisco Unified IP Phone, see Troubleshooting and Maintenance.

This chapter includes these topics:

Accessing the Web Page for a Phone

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

Note If you cannot access the web page, it may be disabled. See Disabling and Enabling Web Page Access, page 7-3 for more information.

Procedure

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

- 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.
- On the Cisco Unified IP Phone, press the **Settings** button, choose **Network Configuration**, and then scroll to the IP Address option.

Step 2 Open a web browser and enter the following URL, where *IP_address* is the IP address of the Cisco Unified IP Phone:

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

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

- Device Information—Displays device settings and related information for the phone. For more information, see Device Information, page 7-4.
- Network Configuration—Displays network configuration information and information about other phone settings. For more information, see Network Configuration, page 7-5.
- Network Statistics—Includes the following hyperlinks, which provide information about network traffic:
  - Ethernet Information—Displays information about Ethernet traffic. For more information, see Network Statistics, page 7-9.
  - Access (Port)—Displays information about network traffic to and from the PC port on the phone. For more information, see Network Statistics, page 7-9.
  - Network (Port)—Displays information about network traffic to and from the network port on the phone. For more information, see Network Statistics, page 7-9.
- Device Logs—Includes the following hyperlinks, which provide information that you can use for troubleshooting:
  - Console Logs—Includes hyperlinks to individual log files. For more information, see Device Logs, page 7-11.
  - Core Dumps—Includes hyperlinks to individual dump files. For more information, see Device Logs, page 7-11.
  - Status Messages—Displays up to the 10 most recent status messages that the phone has generated since it was last powered up. For more information, see Device Logs, page 7-11.
  - Debug Display—Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting. For more information, see Device Logs, page 7-11.

- Streaming Statistics—Includes the following hyperlinks
  - Stream 1, Stream 2, Stream 3, Stream 4, or Stream 5—Display a variety of streaming statistics. For more information, see Streaming Statistics, page 7-11.

Disabling and Enabling Web Page Access

For security purposes, you may choose to prevent access to the web pages for a phone. If you do so, you will prevent access to the web pages that are described in this chapter and to the Cisco Unified Communications Manager User Options web pages.

You can enable or disable access to the web pages for an individual phone, a group of phones, or to all phones in the system.

To enable or disable access to the web pages for all phones on the system, choose **System > Enterprise Parameters** and select Enabled or Disabled from the Web Access drop-down menu.

To enable or disable access to the web pages for a group of phones, choose **Device > Device Settings > Common Phone Profile** to create a new phone profile or to update an existing phone profile, select Enabled or Disabled from the Web Access drop-down menu and select the common phone profile when you configure your phone.

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

Procedure

Step 1 Choose **Device > Phone**.

Step 2 Specify the criteria to find the phone and click **Find**, or click **Find** to display a list of all phones.

Step 3 Click the device name to open the Phone Configuration window for the device.

Step 4 Scroll down to the Product Specific Configuration section. From the Web Access drop-down list box, choose **Disabled** if you want to disable the phone and choose **Enabled** if you want to enable the phone.

Step 5 Click **Update**.

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.

Configuring the Cisco Unified IP Phone to use HTTP/HTTPS Protocols

The Cisco Unified IP Phone can be configured to use:

- The HTTPS protocol only—Phone web access uses https://IP_address
- The HTTP or HTTPS protocols—Phone web access uses http://IP_address or https://IP_address

Device Information

The Device Information area on a phone's web page displays device settings and related information for the phone. Table 7-1 describes these items.

To display the Device Information area, access the web page for the phone as described in the Accessing the Web Page for a Phone, page 7-2, and then click the **Device Information** hyperlink.

Table 7-1 Device Information Area Items

Item	Description
MAC Address	Media Access Control (MAC) address of the phone
Host Name	Unique, fixed name that is automatically assigned to the phone based on the 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
Version	Version of the firmware running on the phone
Expansion Module 1	Phone load ID for the first Cisco Unified IP Phone Expansion Module, if connected to the phone
Expansion Module 2	Phone load ID for the second Cisco Unified IP Phone Expansion Module, if connected to the phone
Hardware Revision	Revision value of the phone hardware
Serial Number	Serial number of the phone
Model Number	Model number of the phone
Message Waiting	Indicates if there is a voice message waiting on any 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 The Version Identifier field might display a blank screen if the user is using an older model Cisco Unified IP Phone, because the hardware does not provide this information. • 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

Table 7-1 Device Information Area Items (continued)

Item	Description
Time Zone	Time zone obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs
Date	Date obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs

Network Configuration

The Network Configuration area on a phone's web page displays network configuration information and information about other phone settings. Table 7-2 describes these items.

You can view and set many of these items from the Network Configuration Menu and the Device Configuration Menu on the Cisco Unified IP Phone. For more information, see Configuring Features, Templates, Services, and Users.

To display the Network Configuration area, access the web page for the phone as described in Accessing the Web Page for a Phone, page 7-2, and then click the **Network Configuration** hyperlink.

Table 7-2 Network Configuration Area Items

Item	Description
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address.
BOOTP Server	Indicates whether the phone obtains configuration from a Bootstrap Protocol (BootP) server.
MAC Address	Media Access Control (MAC) address of the phone.
Host Name	Host name that the DHCP server assigned to the phone.
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.
IP Address	Internet Protocol (IP) address of the phone.
Subnet Mask	Subnet mask used by the phone.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone.
Default Router 1–5	Default router used by the phone (Default Router 1) and optional backup routers (Default Router 2–5).
DNS Server 1–5	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.

Table 7-2 Network Configuration Area Items (continued)

Item	Description
Unified CM 1–5	Host names or IP addresses, in prioritized order, of the Cisco Unified Communications Manager servers with which the phone can register. An item can also show the IP address of an SRST router that is capable of providing limited Cisco Unified Communications Manager functionality, if such a router is available. For an available server, an item will show the Cisco Unified Communications Manager server IP address and one of the following states: • Active—Cisco Unified Communications Manager server from which the phone is currently receiving call-processing services. • Standby—Cisco Unified Communications Manager server to which the phone switches if the current server becomes unavailable. • Blank—No current connection to this Cisco Unified Communications Manager server. An item may also include the Survivable Remote Site Telephony (SRST) designation, which identifies an SRST router capable of providing Cisco Unified Communications Manager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communications Manager always appears last in the list of servers, even if it is active. You configure the SRST router address in the Device Pool section in Cisco Unified Communications Manager Configuration window.
Information URL	URL of the help text that appears on the phone.
Directories URL	URL of the server from which the phone obtains directory information.
Messages URL	URL of the server from which the phone obtains message services.
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.
DHCP Enabled	Indicates whether DHCP is being used by the phone.
DHCP Address Released	Indicates the setting of the DHCP Address Released option on the phone's Network Configuration menu.
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.
Idle URL	URL that the phone displays when the phone has not been used for the time specified by Idle URL Time, and no menu is open.
Idle URL Time	Number of seconds that the phone has not been used and no menu is open before the XML service specified by Idle URL is activated.
Proxy Server URL	URL of proxy server, which makes HTTP requests to non-local host addresses on behalf of the phone HTTP client and provides responses from the non-local host to the phone HTTP client.
Authentication URL	URL that the phone uses to validate requests made to the phone web server.

Table 7-2 Network Configuration Area Items (continued)

Item	Description
SW Port Configuration	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 • No Link—No connection to the switch port
PC Port Configuration	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 • No Link—No connection to the PC port To configure the setting on multiple phones simultaneously, configure the Remote Port Configuration in the Enterprise Phone Configuration (**System > Enterprise Phone Configuration**). **Note** If the ports are configured for Remote Port Configuration in Unified CM, the data cannot be changed on the phone.
TFTP Server 2	Backup TFTP server that the phone uses if the primary TFTP server is unavailable.
User Locale	User locale associated with the phone user. Identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
Network Locale	Network locale associated with the phone user. Identifies a set of detailed information to support the phone in a specific location, including definitions of the tones and cadences used by the phone.
Headset Enabled	Indicates whether the Headset button is enabled on the phone.
User Locale Version	Version of the user locale loaded on the phone.
Network Locale Version	Version of the network locale loaded on the phone.
PC Port Disabled	Indicates whether the PC port on the phone is enabled or disabled.
Speaker Enabled	Indicates whether the speakerphone is enabled on the phone.
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP (GARP) 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.
Auto Line Select	Indicates whether the phone shifts the call focus to incoming calls on all lines.

Table 7-2 Network Configuration Area Items (continued)

Item	Description
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.
Forwarding Delay	Indicates whether the internal switch begins forwarding packets between the PC port and switched port on the phone when the phone becomes active.
LLDP: PC Port	Indicates whether Link Layer Discovery Protocol (LLDP) is enabled on the PC port.
LLDP-MED: SW Port	Indicates whether Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is enabled on the switch port.
LLDP Asset ID	Identifies the asset ID assigned to the phone for inventory management.
Wireless Headset Hookswitch Control	Enables users to receive notifications of incoming calls and answer or end calls while working in a wireless environment.
LLDP Power Priority	Advertises the phone's power priority to the switch, enabling the switch to appropriately provide power to the phones. Settings include: • Unknown—default • Low • High • Critical
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. **Note** 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. **Note** The current PC and switch port CDP values display 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. **Note** 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. **Note** The current PC and switch port CDP values display on the Settings menu.
SSH Access Enabled	Indicates whether the phone accepts or blocks the SSH connections.

Network Statistics

The following network statistics hyperlinks on a phone's web page provide information about network traffic on the phone. To display a network statistics area, access the web page for the phone as described in the Accessing the Web Page for a Phone, page 7-2.

- Ethernet Information—Displays information about Ethernet traffic. Table 7-3 describes the items in this area.
- Access—Displays information about network traffic to and from the PC port on the phone. Table 7-4 describes the items in this area.
- Network—Displays information about network traffic to and from the network (SW) port on the phone. Table 7-4 describes the items in this area.

Table 7-3 Ethernet Information Items

Item	Description
Tx Frames	Total number of packets transmitted by the phone
Tx broadcast	Total number of broadcast packets transmitted by the phone
Tx multicast	Total number of multicast packets transmitted by the phone
Tx unicast	Total number of unicast packets transmitted by the phone
Rx Frames	Total number of packets received by the phone
Rx broadcast	Total number of broadcast packets received by the phone
Rx multicast	Total number of multicast packets received by the phone
Rx unicast	Total number of unicast packets received by the phone
RxPacketNoDes	Total number of shed packets caused by no Direct Memory Access (DMA) descriptor

Table 7-4 Access Area and Network Items

Item	Description
Rx totalPkt	Total number of packets received by the phone
Rx crcErr	Total number of packets received with CRC failed
Rx alignErr	Total number of packets received between 64 and 1522 bytes in length that have a bad Frame Check Sequence (FCS)
Rx multicast	Total number of multicast packets received by the phone
Rx broadcast	Total number of broadcast packets received by the phone
Rx unicast	Total number of unicast packets received by the phone
Rx shortErr	Total number of FCS error packets or Align error packets received that are less than 64 bytes in size
Rx shortGood	Total number of good packets received that are less than 64 bytes size
Rx longGood	Total number of good packets received that are greater than 1522 bytes in size
Rx longErr	Total number of FCS error packets or Align error packets received that are greater than 1522 bytes in size

Table 7-4 Access Area and Network Items (continued)

Item	Description
Rx size64	Total number of packets received, including bad packets, that are between 0 and 64 bytes in size
Rx size65 to127	Total number of packets received, including bad packets, that are between 65 and 127 bytes in size
Rx size128 to255	Total number of packets received, including bad packets, that are between 128 and 255 bytes in size
Rx size256 to511	Total number of packets received, including bad packets, that are between 256 and 511 bytes in size
Rx size512 to1023	Total number of packets received, including bad packets, that are between 512 and 1023 bytes in size
Rx size1024 to1518	Total number of packets received, including bad packets, that are between 1024 and 1518 bytes in size
Rx tokenDrop	Total number of packets dropped due to lack of resources (for example, FIFO overflow)
Tx excessDefer	Total number of packets delayed from transmitting due to medium being busy
Tx lateCollision	Number of times that collisions occurred later than 512 bit times after the start of packet transmission
Tx totalGoodPkt	Total number of good packets (multicast, broadcast, and unicast) received by the phone
Tx Collisions	Total number of collisions that occurred while a packet was being transmitted
Tx excessLength	Total number of packets not transmitted because the packet experienced 16 transmission attempts
Tx broadcast	Total number of broadcast packets transmitted by the phone
Tx multicast	Total number of multicast packets transmitted by the phone
LLDP FramesOutTotal	Total number of LLDP frames sent out from the phone
LLDP AgeoutsTotal	Total number of LLDP frames that have been time out in cache
LLDP FramesDiscardedTotal	Total number of LLDP frames that are discarded when any of the mandatory TLVs is missing or out of order or contains out of range string length.
LLDP FramesInErrorsTotal	Total number of LLDP frames that received with one or more detectable errors
LLDP FramesInTotal	Total number of LLDP frames received on the phone.
LLDP TLVDiscardedTotal	Total number of LLDP TLVs that are discarded.
LLDP TLVUnrecognizedTotal	Total number of LLDP TLVs that are not recognized on the phone.
CDP Neighbor Device ID	Identifier of a device connected to this port discovered by CDP protocol.
CDP Neighbor IP Address	IP address of the neighbor device discovered by CDP protocol.
CDP Neighbor Port	Neighbor device port to which the phone is connected discovered by CDP protocol.
LLDP Neighbor Device ID	Identifier of a device connected to this port discovered by LLDP protocol.
LLDP Neighbor IP Address	IP address of the neighbor device discovered by LLDP protocol.
LLDP Neighbor Port	Neighbor device port to which the phone is connected discovered by LLDP protocol.

Device Logs

The following device logs hyperlinks on a phone's web page provide information you can use to help monitor and troubleshoot the phone. To access a device log area, access the web page for the phone as described in the Accessing the Web Page for a Phone, page 7-2.

- Console Logs—Includes hyperlinks to individual log files. The console log files include debug and error messages received on the phone.
- Core Dumps—Includes hyperlinks to individual dump files. The core dump files include data from a phone crash.
- Status Messages—Displays up to the 10 most recent status messages that the phone has generated since it was last powered up. You can also see this information from the Status Messages screen on the phone. Table 8-2 describes the status messages that can appear.
- Debug Display—Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting.

Streaming Statistics

A Cisco Unified IP Phone can stream information to and from up to three devices simultaneously. A phone streams information when it is on a call or running a service that sends or receives audio or data.

The streaming statistics areas on a phone's web page provide information about the streams. Most calls use only one stream (Stream 1), but some calls use two or three streams. For example, a barged call uses Stream 1 and Stream 2.

To display a Streaming Statistics area, access the web page for the phone as described in the Accessing the Web Page for a Phone, page 7-2, and then click the **Stream 1**, the **Stream 2**, the **Stream 3**, the **Stream 4**, or the **Stream 5** hyperlink.

Table 7-5 describes the items in the Streaming Statistics areas.

Table 7-5 Streaming Statistics Area Items

Item	Description
Remote Address	IP address and UDP port of the destination of the stream.
Local Address	IP address and UPD port of the phone.
Start Time	Internal time stamp indicating when Cisco Unified Communications Manager requested that the phone start transmitting packets.
Stream Status	Indication of whether streaming is active or not.
Host Name	Unique, fixed name that is automatically assigned to the phone based on its MAC address.
Sender Packets	Total number of RTP data packets transmitted by the phone since starting this connection. The value is 0 if the connection is set to receive only mode.
Sender Octets	Total number of payload octets transmitted in RTP data packets by the phone since starting this connection. The value is 0 if the connection is set to receive only mode.
Sender Codec	Type of audio encoding used for the transmitted stream.
Sender Reports Sent[1]	Number of times the RTCP Sender Report have been sent.
Sender Report Time Sent[1]	Internal time stamp indication when the last RTCP Sender Report was sent.

Table 7-5 Streaming Statistics Area Items (continued)

Item	Description
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.
Avg Jitter	Estimate of mean deviation of the RTP data packet inter-arrival time, measured in milliseconds. The value displays as 0 if the connection was set to send-only mode.
Rcvr Codec	Type of audio encoding used for the received stream.
Rcvr Reports Sent[1]	Number of times the RTCP Receiver Reports have been sent.
Rcvr Report Time Sent[1]	Internal time stamp indication when a RTCP Receiver Report was sent.
Rcvr Packets	Total number of RTP data packets received by the phone since starting receiving data on this connection. Includes packets received from different sources if this is a multicast call. The value displays as 0 if the connection was set to send-only mode.
Rcvr Octets	Total number of payload octets received in RTP data packets by the device since starting reception on the connection. Includes packets received from different sources if this is a multicast call. The value displays as 0 if the connection was set to send-only mode.
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see Monitoring the Voice Quality of Calls, page 9-15. **Note** The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score observed from start of the voice stream. These codecs on the Cisco Unified IP Phones 7962G and 7942G provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 gives 4.5 • G.722 gives 4.5 • G.728/iLBC gives 3.9 • G.729 A/AB gives 3.8 These codecs on the Cisco Unified IP Phones 7961G/G-GE and 7941G/41G-GE provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 gives 4.5 • G.729 A /AB gives 3.7
MOS LQK Version	Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.

Table 7-5 Streaming Statistics Area Items (continued)

Item	Description
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[1]	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.
Max Jitter	Maximum value of instantaneous jitter, in milliseconds.
Sender Size	RTP packet size, in milliseconds, for the transmitted stream.
Sender Reports Received[1]	Number of times RTCP Sender Reports have been received.
Sender Report Time Received[1]	Last time at which an RTCP Sender Report was received.
Rcvr Size	RTP packet size, in milliseconds, for the received stream.
Rcvr Discarded	RTP packets received from network but discarded from jitter buffers.
Rcvr Reports Received[1]	Number of times RTCP Receiver Reports have been received.
Rcvr Report Time Received[1]	Last time at which an RTCP Receiver Report was received.
Voice Quality Metrics	
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see Monitoring the Voice Quality of Calls, page 9-15. The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score observed from start of the voice stream. These codecs for the Cisco Unified IP Phones 7962G and 7942G provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 gives 4.5 • G.722 gives 4.5 • G.728/iLBC gives 3.9 • G.729 A/AB gives 3.8 These codecs for the Cisco Unified IP Phones 7961G/G-GE and 7941G/G-GE provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 gives 4.5 • G.729 A /AB gives 3.7
MOS LQK Version	Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.
Cmltve Conceal Ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.

Table 7-5 Streaming Statistics Area Items (continued)

Item	Description
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.

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

Related Topics

- Configuring Settings on the Cisco Unified IP Phones
- Configuring Features, Templates, Services, and Users
- Call Statistics Screen, page 8-14
- Monitoring the Voice Quality of Calls, page 9-15

CHAPTER 8

Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phones

This chapter describes how to use the following menus on the Cisco Unified IP Phone 7962G and 7942G to view model information, status messages, and network statistics for the phone:

- Model Information screen—Displays hardware and software information about the phone. For more information, see Model Information Screen, page 8-2.
- Status menu—Provides access to screens that display the status messages, network statistics, firmware versions, and Expansion Module information. For more information, see Status Menu, page 8-2.
- Call Statistics screen—Displays counters and statistics for the current call. For more information, see Call Statistics Screen, page 8-14.

You can use the information on these screens to monitor the operation of a phone and to assist with troubleshooting.

You can also obtain much of this information, and obtain other related information, remotely through the phone's web page. For more information, see Chapter 7, Monitoring the Cisco Unified IP Phones Remotely.

For more information about troubleshooting the Cisco Unified IP Phone 7962G and 7942G, see Chapter 9, Troubleshooting and Maintenance.

This chapter includes these topics:

Model Information Screen

The Model Information screen includes the options described in Table 8-1.

To display the Model Information screen, press the **Settings** button and then select **Model Information**.

To exit the Model Information screen, press the **Exit** softkey.

Table 8-1 Model Information Settings

Option	Description	To Change
Model Number	Model number of the phone.	Display only—cannot configure.
MAC Address	MAC address of the phone.	Display only—cannot configure.
Load File	Identifier of the factory-installed load running on the phone.	Display only—cannot configure.
Boot Load ID	Identifier of the factory-installed load running on the phone.	Display only—cannot configure.
Serial Number	Serial number of the phone.	Display only—cannot configure.
MIC	Indicates whether a manufacturing installed certificate (used for the security features) is installed on the phone or is not installed on the phone.	For more information about how to manage the MIC for your phone, see Using the Certificate Authority Proxy Function in *Cisco Unified Communications Manager Security Guide*.
LSC	Indicates whether a locally significant certificate (used for the security features) is installed on the phone or is not installed on the phone.	For more information about how to manage the LSC for your phone, see Using the Certificate Authority Proxy Function in *Cisco Unified Communications Manager Security Guide*.
Call Control Protocol	Indicates the call processing protocol used by the phone.	See Using Cisco Unified IP Phones with Different Protocols, page 2-12.

Status Menu

To display the Status menu, press the **Settings** button and then select **Status**. To exit the Status menu, press the **Exit** softkey.

The Status menu includes theses options, which provide information about the phone and its operation:

- Status Messages—Displays the Status Messages screen, which shows a log of important system messages. For more information, see Status Messages Screen, page 8-3.
- Network Statistics—Displays the Network Statistics screen, which shows Ethernet traffic statistics. For more information, see Network Statistics Screen, page 8-9.
- Firmware Versions—Displays the Firmware Versions screen, which shows information about the firmware running on the phone. For more information, see Firmware Versions Screen, page 8-12.
- Expansion Modules—Displays the Expansion Modules screen, which shows information about the Cisco Unified IP Phone Expansion Module, if connected to the phone. For more information, see Expansion Module Status Screen, page 8-13.

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. Table 8-2 describes the status messages that might appear. This table also includes actions you can take to address errors.

To display the Status Messages screen, follow these steps:

Procedure

Step 1 Press the **Settings** button

Step 2 Select **Status**

Step 3 Select **Status Messages**

Step 4 To remove current status messages, press the **Clear** softkey.

Step 5 To exit the Status Messages screen, press the **Exit** softkey.

Table 8-2 Status Messages on the Cisco Unified IP Phone

Message	Description	Possible Explanation and Action
BootP server used	The phone obtained its IP address from a BootP server rather than a DHCP server.	None. This message is informational only.
CFG file not found	The name-based and default configuration file was not found on the TFTP Server.	The Cisco Unified Communications Manager creates a configuration file for the phone with the phone is added to the 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 Adding Phones with Cisco Unified Communications Manager Administration, page 2-11 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 Network Configuration Menu, page 4-5 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.

Table 8-2 Status Messages on the Cisco Unified IP Phone (continued)

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.
CTL and ITL installed	The CTL and ITL files are installed on the phone.	None. This message is informational only. Neither the CTL file nor the ITL file was installed previously. For more information about the CTL file, see *Cisco Unified Communications Manager Security Guide*.
CTL installed	The CTL file is installed in the phone.	None. This message is informational only. The CTL file was not installed previously. For more information about the CTL file, see *Cisco Unified Communications Manager Security Guide*.
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 Network Configuration Menu, page 4-5 for details on assigning a static IP address.
Dialplan Parsing Error (SIP Phones only)	The phone could not properly parse the dialplan XML file.	Problem with the TFTP downloaded dialplan XML file.
Disabled	802.1X Authentication is disabled on the phone.	You can enable 802.1X using the **Settings > Security Configuration > 802.1X Authentication** option on the phone. For more information, see 802.1X Authentication and Status, page 4-44.
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.

Table 8-2 Status Messages on the Cisco Unified IP Phone (continued)

Message	Description	Possible Explanation and Action
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 Network Configuration Menu, page 4-5 section for details. • If you are using DHCP, check the DHCP server configuration.
Erasing CTL and ITL files	Erasing CTL or ITL files.	None. This message is informational only. For more information about the CTL or ITL files, see *Cisco Unified Communications Manager Security Guide.*
Error update locale	One or more localization files could not be found in the TFTPPath directory or were not valid. The locale was not changed.	From Cisco Unified Operating System Administration, check that the following files are located within subdirectories in the TFTP File Management: • Located in subdirectory with same name as network locale: – tones.xml • Located in subdirectory with same name as user locale: – glyphs.xml – dictionary.xml – kate.xml
Failed	The phone attempted an 802.1X transaction but authentication failed.	Authentication typically fails for one of the following reasons: • No shared secret is configured in the phone or authentication server. • The shared secret configured in the phone and the authentication server do not match. • Phone has not been configured in the authentication server.
File auth error	An error occurred when the phone tried to validate the signature of a signed file. This message includes the name of the file that failed.	• The file is corrupted. If the file is a phone configuration file, delete the phone from the Cisco Unified Communications Manager database using Cisco Unified Communications Manager Administration. Then add the phone back to the Cisco Unified Communications Manager database using Cisco Unified Communications Manager Administration. • There is a problem with the CTL file and the key for the server from which files are obtained is bad. In this case, run the CTL client and update the CTL file, making sure that the proper TFTP servers are included in this file.

Table 8-2 Status Messages on the Cisco Unified IP Phone (continued)

Message	Description	Possible Explanation and Action
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 Network Configuration Menu, page 4-5 for details.
ITL installed	The ITL file is installed in the phone.	None. This message is informational only. The ITL file was not installed previously. For more information about the ITL file, see *Cisco Unified Communications Manager Security Guide.*
Load Auth Failed	The phone could not load a configuration file.	Check that: • A good version of the configuration file exists on the applicable server. • The phone load file being downloaded has not been altered or renamed. • The phone load type is compatible; for example, you cannot place a DEV load configuration file on a REL-signed phone.
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. See Firmware Versions Screen, page 8-12 to verify the phone setting.
Load Server is invalid	Indicates an invalid TFTP server IP address or name in the Load Server option.	The Load Server setting is not valid. The Load Server specifies a TFTP server IP address or name from which the phone firmware can be retrieved for upgrades on the phones. Check the Load Server entry (from Cisco Unified Communications Manager Administration, choose **Device > 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 Network Configuration Menu, page 4-34 for details. • If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.

Table 8-2 Status Messages on the Cisco Unified IP Phone (continued)

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 Network Configuration Menu, page 4-5 for details. • If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.
No Trust List installed	Certificate Trust List (CTL) file or Identity Trust List (ITL) file is not installed in the phone.	Occurs if the CTL file is not configured on the Cisco Unified Communications Manager and the Cisco Unified Communications Manager does not support security by default. For more information about the CTL file or ITL file, see *Cisco Unified Communications Manager Security Guide.*
Programming Error	The phone failed during programming.	Attempt to resolve this error by power cycling the phone. If the problem persists, contact Cisco technical support for additional assistance.
Successful—MD5	The phone attempted an 802.1X transaction and authentication achieved.	The phone achieved 802.1X authentication.
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 Network Configuration Menu, page 4-5 for details on assigning a TFTP server.
TFTP error	The phone does not recognize an error code provided by the TFTP server.	Contact the Cisco TAC.
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 timeout	TFTP server did not respond.	• Network is busy—The errors should resolve themselves when the network load reduces. • No network connectivity between the TFTP server and the phone—Verify the network connections. • TFTP server is down—Check configuration of TFTP server.
Timed Out	Supplicant attempted 802.1X transaction but timed out to due the absence of an authenticator.	Authentication typically times out if 802.1X is not configured on the switch.

Table 8-2 Status Messages on the Cisco Unified IP Phone (continued)

Message	Description	Possible Explanation and Action
Trust List update failed	Updating CTL and ITL files failed.	Phone has CTL and ITL files installed and it failed to update the new CTL and ITL files. Possible reasons for failure: • Network failure. • TFTP server was down. • The new security token used to sign CTL file and the TFTP certificate used to sign ITL file are introduced, but are not available in the current CTL and ITL files in the phone. • Internal phone failure. Possible solutions: • Check the network connectivity. • Check if the TFTP server is active and functioning normally. • If the TVS server is supported on Cisco Unified Communications Manager, check if the TVS server is active and functioning normally. • Verify if the security token and the TFTP server are valid. • Manually delete the CTL and ITL files if all the above solutions fail, and reset the phone.
Trust List updated	The CTL file, the ITL file, or both files are updated.	None. This message is informational only. For more information about the Trust List, see *Cisco Unified Communications Manager Security Guide*.
No Trust List installed	The CTL file or the ITL file is not installed in the phone.	The Trust List is not configured on the Cisco Unified Communications Manager, which does not support security by default. For more information about the Trust List, see *Cisco Unified Communications Manager Security Guide*.
Version error	The name of the phone load file is incorrect.	Make sure that the phone load file has the correct name.
XmlDefault 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. Table 8-3 describes the information that appears in this screen.

To display the Network Statistics screen, follow these steps:

Procedure

Step 1 Press the **Settings** button

Step 2 Select **Status**

Step 3 Select **Status > Network Statistics**

Step 4 To reset the Rx Frames, Tx Frames, and Rx Broadcasts statistics to 0, press the **Clear** softkey.

Step 5 To exit the Network Statistics screen, press the **Exit** softkey.

Table 8-3 Network Statistics Message Information

Item	Description
Rx Frames	Number of packets received by the phone
Tx Frames	Number of packets sent by the phone
Rx Broadcasts	Number of broadcast packets received by the phone
One of the following values: • Initialized • TCP-timeout • CM-closed-TCP • TCP-Bad-ACK • CM-reset-TCP • CM-aborted-TCP • CM-NAKed • KeepaliveTO • Failback • Phone-Keypad • Phone-Re-IP • Reset-Reset • Reset-Restart • Phone-Reg-Rej • Load Rejected HC • CM-ICMP-Unreach • Phone-Abort	Cause of the last reset of the phone
Elapsed Time	Amount of time that has elapsed since the phone last rebooted

Table 8-3 Network Statistics Message Information (continued)

Item	Description
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

Table 8-3 Network Statistics Message Information (continued)

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

Table 8-3 Network Statistics Message Information (continued)

Item	Description
IPv6	Information on the DHCPv6 status. This includes the following states: • DHCP6 BOUND; • DHCP6 DISABLED • DHCP6 RENEW • DHCP6 REBIND • DHCP6 INIT • DHCP6 SOLICIT • DHCP6 REQUEST • DHCP6 RELEASING • DHCP6 RELEASED • DHCP6 DISABLING • DHCP6 DECLINING • DHCP6 DECLINED • DHCP6 INFOREQ • DHCP6 INFOREQ DONE • DHCP6 INVALID • DHCP6 DECLINED DUPLICATE IP • DHCP6 WAITING COLDBOOT TIMEOUT • DHCP6 TIMEOUT USING RESTORED VAL • DHCP6 TIMEOUT. CANNOT RESTORE • STACK TURNED OFF

Firmware Versions Screen

The Firmware Versions screen displays information about the firmware version that is running on the phone. Table 8-4 describes the information that is displayed on this screen.

To display the Firmware Version screen, follow these steps:

Procedure

Step 1 Press the **Settings** button

Step 2 Select **Status**

Step 3 Select **Firmware Versions**

Step 4 To exit the Firmware Version screen, press the Exit softkey.

Table 8-4 Firmware Version Information

Item	Description
Load File	Load file running on the phone
App Load ID	Identifies the JAR file running on the phone
JVM Load ID	Identifies the Java Virtual Machine (JVM) running on the phone
OS Load ID	Identifies the operating system running on the phone
Boot Load ID	Identifies the factory-installed load running on the phone
Expansion Module 1 Expansion Module 2	Identifies the load running on the Expansion Modules, if connected to a SIP or SCCP phone
DSP Load ID	Identifies the digital signal processor (DSP) software version used

Expansion Module Status Screen

The Expansion Module Status screen displays information about each Cisco Unified IP Phone Expansion Module that is connected to the phone.

Table 8-5 explains the information that is displayed on this screen for each connected expansion module. You can use this information to troubleshoot the expansion module, if necessary. In the Expansion Module Stats screen, a statistic preceded by “A” is for the first expansion module. A statistic preceded by “B” is for the second expansion module.

To display the Expansion Module Status screen, follow these steps:

Procedure

Step 1 Press the **Settings** button

Step 2 Select **Status**

Step 3 Select **Expansion Module**

Step 4 To exit the Expansion Module screen, press the Exit softkey.

Table 8-5 Expansion Module Statistics

Item	Description
Link State	Overall expansion module status
RX Discarded Bytes	Number of bytes discarded due to errors
RX Length Err	Number of packets discarded due to improper length
RX Checksum Err	Number of packets discarded due to invalid checksum information
RX Invalid Message	Number of packets that have been discarded because a message was invalid or unsupported

Table 8-5 Expansion Module Statistics (continued)

Item	Description
TX Retransmit	Number of packets that have been retransmitted to the expansion module
TX Buffer Full	Number of packets discarded because the expansion module was not able to accept new messages

Call Statistics Screen

You can access the Call Statistics screen on the phone to display counters, statistics, and voice-quality metrics in the following ways:

- During call—You can view the call information by rapidly pressing the ? button twice.
- After the call—You can view the call information captured during the last call by displaying the Call Statistics screen.

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 Monitoring the Cisco Unified IP Phones Remotely, page 7-1

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 last voice stream, follow these steps:

Procedure

Step 1 Press the **Settings** button.

Step 2 Select **Status**.

Step 3 Select **Call Statistics**.

Table 8-6 describes the items displayed on the Call Statistics screen:

Table 8-6 Call Statistics Items

Item	Description
Rcvr Codec	Type of voice stream received (RTP streaming audio from codec): G.729, G.728/iLBC, G.711 u-law, G.711 A-law, or Lin16k.
Sender Codec	Type of voice stream transmitted (RTP streaming audio from codec): G.729, G.728/iLBC, G.711 u-law, G.711 A-law, or Lin16k.
Rcvr Size	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).

Table 8-6 Call Statistics Items (continued)

Item	Description
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 discards payload type 19 comfort noise packets that are generated by Cisco Gateways, which increment this counter.
Rcvr Lost Packets	Missing RTP packets (lost in transit).
Voice Quality Metrics	
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see Monitoring the Voice Quality of Calls, page 9-15. **Note** The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score observed from start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 gives 4.5 • G.722 gives 4.5 • G.728/iLBC gives 3.9 • G.729 A/AB gives 3.8

Table 8-6 Call Statistics Items (continued)

Item	Description
MOS LQK Version	Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency[1]	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.
Network Protocol	Identifies the current Network Protocol.

1When the RTP Control Protocol is disabled, no data generates for this field and thus displays as 0.

Using Test Tone

The Cisco Unified IP Phone supports a “test tone,” which allows you to troubleshoot echo on a call as well as to test low volume levels.

To use a test tone you must:

- Enable the tone generator.
- Create a test tone.

To enable the tone generator, follow these steps:

Procedure

Step 1 Verify that the phone is unlocked.

When options are inaccessible for modification, a *locked* padlock icon appears on the configuration menus. When options are unlocked and accessible for modification, an *unlocked* padlock icon appears on these menus.

To unlock or lock options on the Settings menu, press ****#** on the phone keypad. This action either locks or unlocks the options, depending on the previous state.

Note If a Settings Menu password has been provisioned, SIP Phones present an "Enter password" prompt after you enter **#.

Make sure to lock options after you have made your changes.

Caution Do not press ****#** to unlock options and then immediately press ****#** again to lock options. The phone will interpret this sequence as ****#****, which will reset the phone. To lock options after unlocking them, wait at least 10 seconds before you press ****#** again.

Step 2 While offhook, press the Help button twice to invoke the Call Statistics screen, or press **Settings > Status > Call Statistics** to invoke the Call Statistics screen. Look for the Tone softkey.

When the Tone softkey is visible, the softkey remains enabled for as long as this Cisco Unified IP Phone is registered with Cisco Unified Communications Manager.

You can proceed to the procedure for using the tone generator.

Step 3 If the Tone softkey is not present, exit the Call Statistics screen and enter the Setting Menu. Press ****3** on the phone keypad to enable (toggle) the Tone softkey.

Note If you press ****# **3** consecutively, with no pause, you will inadvertently reset the phone because of the ****#**** sequence. Make sure that you wait at least 10 seconds after you press **# before you press **3.

While offhook, press the Help button twice to invoke the Call Statistics screen, or press **Settings > Status > Call Statistics** to invoke the Call Statistics screen. Verify that the Tone softkey is present.

When the Tone softkey is visible, the softkey remains enabled for as long as this Cisco Unified IP Phone is registered with Cisco Unified Communications Manager.

To use the tone, follow these steps:

Procedure

Note When measuring echo, make sure you first set the input and output levels to 0 dB gain/attenuation on the trunk. This is set for the gateway (in Cisco Unified Communications Manager for MGCP) or under IOS CLI for H.323 or SIP.

Step 1 Place a call.

Step 2 After the call is established, press the **Help** button twice, or press **Settings > Status > Call Statistics**.

The Call Statistics screen and Tone softkey appear.

Step 3 Press the **Tone** softkey.

The phone generates a 1004 Hz tone at –15 dBm. For a good network connection, the tone sounds at the call destination only. For a bad network connection, the phone generating the tone may receive echo from the destination phone.

Step 4 To stop the tone, end the call.

For information on interpreting the results of test tone for volume and echo, see the following document:

http://www.cisco.com/en/US/docs/ios/solutions_docs/voip_solutions/EA_ISD.html

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.

For additional troubleshooting information, see the *Using the 79xx Status Information For Troubleshooting* tech note. That document is available to registered Cisco.com users at this URL:

http://www.cisco.com/warp/customer/788/AVVID/telecaster_trouble.html

If you need additional assistance to resolve an issue, see Obtaining Documentation, Obtaining Support, and Security Guidelines, page -xiii.

This chapter includes these topics:

Resolving Startup Problems

After installing a Cisco Unified IP Phone into your network and adding it to Cisco Unified Communications Manager, the phone should start up as described in the Verifying the Phone Startup Process, page 3-14. If the phone does not start up properly, see the following sections for troubleshooting information:

- Symptom: The Cisco Unified IP Phone Displays the Message Security Error, page 9-6

Symptom: The Cisco Unified IP Phone Does Not Go Through its Normal Startup Process

When you connect a Cisco Unified IP Phone into the network port, the phone should go through its normal startup process as described in Verifying the Phone Startup Process, page 3-14 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:

1. Verify that the network port is functional:
   - Exchange the Ethernet cables with cables that you know are functional.
   - Disconnect a functioning Cisco Unified IP Phone from another port and connect it to this network port to verify the port is active.
   - Connect the Cisco Unified IP Phone that will not start up to a different network port that is known to be good.
   - Connect the Cisco Unified IP Phone that will not start up directly to the port on the switch, eliminating the patch panel connection in the office.
2. Verify that the phone is receiving power:
   - If you are using external power, verify that the electrical outlet is functional.
   - If you are using in-line power, use the external power supply instead.
   - If you are using the external power supply, switch with a unit that you know to be functional.
3. If the phone still does not start up properly, power up the phone with the handset off-hook. When the phone is powered up in this way, it attempts to launch a backup software image.
4. If the phone still does not start up properly, perform a factory reset of the phone. For instructions, see Performing a Factory Reset, page 9-14.

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.

Symptom: The Cisco Unified IP Phone Does Not Register with Cisco Unified Communications Manager

If the phone proceeds past the first stage of the startup process (LED buttons flashing on and off) but continues to cycle through the messages displaying on the 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.

These sections can assist you in determining the reason the phone is unable to start up properly:

- Identifying Error Messages, page 9-3
- Checking Network Connectivity, page 9-3

- Verifying TFTP Server Settings, page 9-3
- Verifying IP Addressing and Routing, page 9-3
- Verifying DNS Settings, page 9-4
- Verifying Cisco Unified Communications Manager Settings, page 9-4
- Cisco CallManager and TFTP Services Are Not Running, page 9-4
- Creating a New Configuration File, page 9-5
- Checking Network Connectivity, page 9-3

In addition, problems with security may prevent the phone from starting up properly. See Troubleshooting Cisco Unified IP Phone Security, page 9-9 for more information.

Identifying Error Messages

As the phone cycles through the startup process, you can access status messages that might provide you with information about the cause of a problem. See Status Messages Screen, page 8-3 for instructions about accessing status messages and for a list of potential errors, their explanations, and their solutions.

Checking Network Connectivity

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

Verifying TFTP Server Settings

You can determine the IP address of the TFTP server used by the phone by pressing the **Settings** button on the phone, choosing **Network Configuration > IPv4** and scrolling to the **TFTP Server 1** option.

If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option. See Network Configuration Menu, page 4-5.

If you are using DHCP, the phone obtains the address for the TFTP server from the DHCP server. Check the IP address configured in Option 150.

You can also enable the phone to use an alternate TFTP server. Such a setting is particularly useful if the phone was recently moved from one location to another. See Network Configuration Menu, page 4-5 for instructions.

Verifying IP Addressing and Routing

You should verify the IP addressing and routing settings on the phone. If you are using DHCP, the DHCP server should provide these values. If you have assigned a static IP address to the phone, you must enter these values manually.

On the Cisco Unified IP Phone, choose **Settings > Network Configuration > IPv4 Configuration**, and look at the following options:

- DHCP Server—If you have assigned a static IP address to the phone, you do not need to enter a value for the DHCP Server option. However, if you are using a DHCP server, this option must have a value. If it does not, check your IP routing and VLAN configuration. See the *Troubleshooting Switch Port and Interface Problems* document, available at this URL: http://www.cisco.com/warp/customer/473/53.shtml

- IP Address, Subnet Mask, Default Router—If you have assigned a static IP address to the phone, you must manually enter settings for these options. See Network Configuration Menu, page 4-5 for instructions.

If you are using DHCP, check the IP addresses distributed by your DHCP server. See the *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* document, available at this URL: http://www.cisco.com/warp/customer/473/100.html#41

Verifying DNS Settings

If you are using DNS to see the TFTP server or to Cisco Unified Communications Manager, you must ensure that you have specified a DNS server. Verify this setting by pressing the **Settings** button on the phone, choosing **Network Configuration,** and scrolling to the **DNS Server 1** option. You should also verify that there is a CNAME entry in the DNS server for the TFTP server and for the Cisco Unified Communications Manager system.

You must also ensure that DNS is configured to do reverse look-ups.

Verifying Cisco Unified Communications Manager Settings

On the Cisco Unified IP Phone, press the **Settings** button, choose **Device Configuration**, and look at the **Unified CM Configuration** options. The Cisco Unified IP Phone attempts to open a TCP connection to all the Cisco Unified Communications Manager servers that are part of the assigned Cisco Unified Communications Manager group. If none of these options contain IP addresses or show Active or Standby, the phone is not properly registered with Cisco Unified Communications Manager. See Checking Network Connectivity, page 9-3 for tips on resolving this problem.

Cisco CallManager and TFTP Services Are Not Running

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

If the Cisco CallManager service is not running, all devices on the network that rely on it to make phone calls will be affected. If the TFTP service is not running, many devices will not be able to start up successfully.

To start a service, follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Cisco Unified Serviceability** from the Navigation drop-down list and click **Go**.

Step 2 Choose **Tools > Control Center - Feature Services**.

Step 3 Choose the primary Cisco Unified Communications Manager server from the Server drop-down list.

The window displays the service names for the server that you chose, the status of the services, and a service control panel to start or stop a service.

Step 4 If a service has stopped, click its radio button and then click the **Start** button.

The Service Status symbol changes from a square to an arrow.

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

Creating a New Configuration File

If you continue to have problems with a particular phone that other suggestions in this chapter do not resolve, the configuration file may be corrupted.

To create a new configuration file, follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager, choose **Device > Phone > Find** to locate the phone experiencing problems.

Step 2 Choose **Delete** to remove the phone from the Cisco Unified Communications Manager database.

Step 3 Add the phone back to the Cisco Unified Communications Manager database. See Adding Phones to the Cisco Unified Communications Manager Database, page 2-8 for details.

Step 4 Power cycle the phone.

Note

- When you remove a phone from the Cisco Unified Communications Manager database, its configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone's directory number or numbers remain in the Cisco Unified Communications Manager database. They are called "unassigned DNs" and can be used for other devices. If unassigned DNs are not used by other devices, delete them from the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers. See *Cisco Unified Communications Manager Administration Guide* for more information.
- Changing the buttons on a phone button template, or assigning a different phone button template to a phone, may result in directory numbers that are no longer accessible from the phone. The directory numbers are still assigned to the phone in the Cisco Unified Communications Manager database, but there is no button on the phone with which calls can be answered. These directory numbers should be removed from the phone and deleted if necessary.

Registering the Phone with Cisco Unified Communications Manager

A Cisco Unified IP Phone can register with a Cisco Unified Communications Manager server only if the phone has been added to the server or if auto-registration is enabled. Review the information and procedures in Adding Phones to the Cisco Unified Communications Manager Database, page 2-8 to ensure that the phone has been added to the Cisco Unified Communications Manager database.

To verify that the phone is in the Cisco Unified Communications Manager database, choose **Device > Phone > Find** from Cisco Unified Communications Manager Administration to search for the phone based on its MAC Address. For information about determining a MAC address, see Determining the MAC Address for a Cisco Unified IP Phones, page 2-13.

If the phone is already in the Cisco Unified Communications Manager database, its configuration file may be damaged. See Creating a New Configuration File, page 9-5 for assistance.

Symptom: Cisco Unified IP Phone Unable to Obtain IP Address

If a phone is unable to obtain an IP address when it starts up, the phone may be not be on the same network or VLAN as the DHCP server, or the switch port to which the phone is connected may be disabled. Make sure that the network or VLAN to which the phone is connected has access to the DHCP server, and make sure that the switch port is enabled.

Symptom: The Cisco Unified IP Phone Displays the Message Security Error

When a Cisco Unified IP Phone boots, it performs an internal Power On Self Test (POST). POST checks for existing encryption functionality. If POST detects that encryption functionality is missing, the phone fails to boot, and the message "Security Error" appears on the screen.

To correct the problem, perform the following steps:

1. Reset the phone manually.
2. If the phone 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.
3. If the phone still does not start up properly, perform a factory reset of the phone. For instructions, see Performing a Factory Reset, page 9-14.

Cisco Unified IP Phone Resets Unexpectedly

If users report that their phones are resetting during calls or while idle on their desk, you should investigate the cause. If the network connection and Cisco Unified Communications Manager connection are stable, a Cisco Unified IP Phone should not reset on its own.

Typically, a phone resets if it has problems connecting to the Ethernet network or to Cisco Unified Communications Manager. These sections can help you identify the cause of a phone resetting in your network:

Verifying the Physical Connection

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

Identifying Intermittent Network Outages

Intermittent network outages affect data and voice traffic differently. Your network might have been experiencing intermittent outages without detection. If so, data traffic can resend lost packets and verify that packets are received and transmitted. However, voice traffic cannot recapture lost packets. Rather than retransmitting a lost network connection, the phone resets and attempts to reconnect its network connection.

If you are experiencing problems with the voice network, you should investigate whether an existing problem is simply being exposed.

Verifying DHCP Settings

The following suggestions can help you determine if the phone has been properly configured to use DHCP:

1. Verify that you have properly configured the phone to use DHCP. See Network Configuration Menu, page 4-5 for more information.
2. Verify that the DHCP server has been set up properly.
3. Verify the DHCP lease duration. We recommend that you set the lease duration to 8 days.

Cisco Unified IP Phones send messages with request type 151 to renew their DHCP address leases. If the DHCP server expects messages with request type 150, the lease renewal is denied, forcing the phone to restart and request a new IP address from the DHCP server.

Checking Static IP Address Settings

If the phone has been assigned a static IP address, verify that you have entered the correct settings. See Network Configuration Menu, page 4-5 for more information.

Verifying the Voice VLAN Configuration

If the Cisco Unified IP Phone appears to reset during heavy network usage (for example, following extensive web surfing on a computer connected to the same switch as the phone), it is likely that you do not have a voice VLAN configured.

Isolating the phones on a separate auxiliary VLAN increases the quality of the voice traffic. See Understanding How the Cisco Unified IP Phones Interact with the VLAN, page 2-2 for details.

Verifying that the Phones Have Not Been Intentionally Reset

If you are not the only administrator with access to Cisco Unified Communications Manager, you should verify that no one else has intentionally reset the phones.

You can check whether a Cisco Unified IP Phone received a command from Cisco Unified Communications Manager to reset by pressing the **Settings** button on the phone and choosing **Status > Network Statistics**. If the phone was recently reset one of these messages appears:

- Reset-Reset—Phone received a Reset/Reset request from Cisco Unified Communications Manager Administration.

- Reset-Restart—Phone received a Reset/Restart request from Cisco Unified Communications Manager Administration.

Eliminating DNS or Other Connectivity Errors

If the phone continues to reset, follow these steps to eliminate DNS or other connectivity errors:

Procedure

Step 1 Use the **Erase** softkey to reset phone settings to their default values. See Resetting or Restoring the Cisco Unified IP Phones, page 9-13 for details.

Step 2 Modify DHCP and IP settings:

a. Disable DHCP. See Network Configuration Menu, page 4-5 for instructions.

b. Assign static IP values to the phone. See Network Configuration Menu, page 4-5 for instructions. Use the same default router setting used for other functioning Cisco Unified IP Phones.

c. Assign a TFTP server. See Network Configuration Menu, page 4-5 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 Determining the MAC Address for a Cisco Unified IP Phones, page 2-13.

Step 6 Power cycle the phone.

Checking Power Connection

In most cases, a phone will restart if it powers up by using external power but loses that connection and switches to Power over Ethernet (PoE). Similarly, a phone may restart if it powers up by using PoE and then gets connected to an external power supply.

Troubleshooting Cisco Unified IP Phone Security

Table 9-1 provides troubleshooting information for the security features on the Cisco Unified IP Phone. For information relating to the solutions for any of these issues, and for additional troubleshooting information about security and encryption, see *Cisco Unified Communications Manager Security Guide*.

Table 9-1 Cisco Unified IP Phone Security Troubleshooting

Problem	Possible Cause
Device authentication error.	CTL file does not have a Cisco Unified Communications Manager certificate or has an incorrect certificate.
Phone cannot authenticate CTL file.	The security token that signed the updated CTL file does not exist in the CTL file on the phone.
Phone cannot authenticate any of the configuration files other than the ITL file.	The configuration file may not be signed by the corresponding certificate in the phone's Trust List.
Phone cannot authenticate any of the configuration files other than the CTL file.	The configuration file may not be signed by the corresponding certificate in the phone's Trust List.
Phone does not register with Cisco Unified Communications Manager.	The CTL file does not contain the correct information for the Cisco Unified Communications Manager server.
Phone does not request signed configuration files.	The CTL file does not contain any TFTP entries with certificates.
802.1X Enabled on Phone but Not Authenticating	
Phone cannot obtain a DHCP-assigned IP address	These errors typically indicate that 802.1X is enabled on the phone, but the phone is unable to authenticate. 1. Verify that you have properly configured the required components Supporting 802.1X Authentication on Cisco Unified IP Phones, page 1-19. 2. Confirm that the shared secret is configured on the phone. See Security Configuration Menu, page 4-32 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 shared secret on the authentication server.
Phone does not register with Cisco Unified Communications Manager	
Phone status display as Configuring IP or Registering	
802.1X Authentication Status displays as Held (see 802.1X Authentication and Status, page 4-44).	
Status menu displays 802.1x status as Failed (see Call Statistics Screen, page 8-14).	
802.1X Not Enabled	
Phone cannot obtain a DHCP-assigned IP address	These errors typically indicate that 802.1X is not enabled on the phone. To enable it, see Security Configuration Menu, page 4-32 for information on enabling 802.1X on the phone.
Phone does not register with Cisco Unified Communications Manager	
Phone status display as Configuring IP or Registering	
802.1X Authentication Status displays as Disabled (see 802.1X Authentication and Status, page 4-44).	
Status menu displays DHCP status as timing out (see Call Statistics Screen, page 8-14).	

Table 9-1 Cisco Unified IP Phone Security Troubleshooting (continued)

Problem	Possible Cause
Factory Reset Deleted 802.1X Shared Secret	
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	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. 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.

General Troubleshooting Tips

Table 9-2 provides general troubleshooting information for the Cisco Unified IP Phone.

Table 9-2 Cisco Unified IP Phone Troubleshooting

Summary	Explanation
Connecting a Cisco Unified IP Phone to another Cisco Unified IP Phone	Cisco does not support connecting an IP Phone to another IP Phone through the PC port. Each IP Phone should directly connect to a switch port. If phones are connected together in a line (by using the PC port), the phones will not work.
Poor quality 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.
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 network card in the computer cannot receive power through the network connection; if power comes through the connection, the network card can be destroyed. To protect a network card, wait 10 seconds or longer after unplugging the cable from the phone before plugging it into a computer. This delay gives the switch enough time to recognize that there is no longer a phone on the line and to stop providing power to the cable.
Changing the telephone configuration	By default, the network configuration options are locked to prevent users from making changes that could impact their network connectivity. You must unlock the network configuration options before you can configure them. See Unlocking and Locking Options, page 4-2 for details.

Table 9-2 Cisco Unified IP Phone Troubleshooting (continued)

Summary	Explanation
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.
LCD display issues	If the display appears to have rolling lines or a wavy pattern, it might be interacting with certain types of older fluorescent lights in the building. Moving the phone away from the lights, or replacing the lights, should resolve the problem.
Dual-Tone Multi-Frequency (DTMF) delay	When you are on a call that requires keypad input, if you press the keys too quickly, some of them might not be recognized.
Codec mismatch between the phone and another device	The RxType and the TxType statistics show the codec that is being used for a conversation between this Cisco Unified IP phone and the other device. The values of these statistics should match. If they do not, verify that the other device can handle the codec conversation, or that a transcoder is in place to handle the service. See Call Statistics Screen, page 8-14 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 Call Statistics Screen, page 8-14 for information about displaying these statistics.
Gaps in voice calls	Check the AvgJtr and the MaxJtr statistics. A large variance between these statistics might indicate a problem with jitter on the network or periodic high rates of network activity. See Call Statistics Screen, page 8-14 for information about displaying these statistics.
Loopback condition	A loopback condition can occur when the following conditions are met: • The SW Port Configuration option in the Network Configuration menu on the phone is set to **10 Half** (10-BaseT / half duplex) • The phone receives power from an external power supply • The phone is powered down or the power supply is disconnected In this case, the switch port on the phone can become disabled and the following message appears in the switch console log: HALF_DUX_COLLISION_EXCEED_THRESHOLD To resolve this problem, re-enable the port from the switch.
One-way audio	When at least one person in a call does not receive audio, IP connectivity between phones is not established. Check the configurations in routers and switches to ensure that IP connectivity is properly configured.

Table 9-2 Cisco Unified IP Phone Troubleshooting (continued)

Summary	Explanation
Peer Firmware Sharing fails.	If the Peer Firmware Sharing fails, the phone will default to using the TFTP server to download firmware. Access the log messages stored on the remote logging machine to help debug the Peer Firmware Sharing feature. **Note** These log messages are different from the log messages sent to the phone log.
Cisco VT Advantage/Unified Video Advantage (CVTA)	If you are having problems getting CVTA to work, make sure that the PC Port is enabled, and that CDP is enabled on the PC port. See Network Configuration Menu, page 4-5 for more information.
Phone call cannot be established	The phone does not have a DHCP IP address, is unable to register to Cisco Unified Communications Manager, and shows a Configuring IP or Registering message. Verify the following: 1. The Ethernet cable is attached. 2. The Cisco CallManager service is running on the Cisco Unified Communications Manager server. 3. Both phones are registered to the same Cisco Unified Communications Manager. 4. Audio server debug and capture logs are enabled for both phones. If needed, enable Java debug.
Call established with the iLBC protocol does not show that the iLBC codec is being used	Call statistics display does not show iLBC as the receiver/sender codec. 1. Check the following by using Cisco Unified Communications Manager Administration: – Both phones are in the iLBC device pool. – The iLBC device pool is configured with the iLBC region. – The iLBC region is configured with the iLBC codec. 2. Capture a sniffer trace between the phone and Cisco Unified Communications Manager and verify that SCCP messages, OpenReceiveChannel, and StationMediaTransmit messages have media payload type value equal to 86. If so, the problem is with the phone; otherwise, the problem is with the Cisco Unified Communications Manager configuration. 3. Enable audio server debug and capture logs from both phones. If needed, enable Java debug.

General Troubleshooting Tips for the Cisco Unified IP Phone Expansion Module

Table 9-3 provides general troubleshooting information for the Cisco Unified IP Phone Expansion Module.

Table 9-3 Cisco Unified IP Phone Expansion Module Troubleshooting

Problem	Solution
No display on the Cisco Unified IP Phone Expansion Module.	Verify that all of the cable connections are correct. Verify that you have power to the Cisco Unified IP Phone Expansion Module.
Lighted buttons on the first Cisco Unified IP Phone Expansion Module are all red.	Verify that the Cisco Unified IP Phone Expansion Module is configured in Cisco Unified Communications Manager.
Lighted buttons on the second Cisco Unified IP Phone Expansion Module are all amber.	Verify that the Cisco Unified IP Phone Expansion Module is configured in Cisco Unified Communications Manager.

Resetting or Restoring the Cisco Unified IP Phones

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

- Performing a Basic Reset, page 9-13
- Performing a Factory Reset, page 9-14

Performing a 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.

Table 9-4 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 9-4 Basic Reset Methods

Operation	Performing	Explanation
Restart phone	Press the **Services**, **Settings, or Directories** button and then press **#**.	Resets any user and network configuration changes that you have made, but that the phone has not written to its Flash memory, to previously saved settings, then restarts the phone.

Table 9-4 Basic Reset Methods (continued)

Operation	Performing	Explanation
Erase softkey	From the Settings menu, unlock phone options (see Unlocking and Locking Options, page 4-2). Then press the **Erase** softkey.	Resets user and network configuration settings to their default values, deletes the CTL file from the phone, and restarts the phone.
	From the Network Configuration menu, unlock phone options (see Unlocking and Locking Options, page 4-2). Then press the **Erase** softkey.	Resets network configuration settings to their default values and resets the phone. This method causes DHCP to reconfigure the IP address of the phone.
	From the Security Configuration menu, unlock phone options (see Unlocking and Locking Options, page 4-2). Then press the **Erase** softkey.	Deletes the CTL file from the phone and restarts the phone.

Performing a 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:

- CTL file—Erased
- LSC—Erased
- User configuration settings—Reset to default values
- Network configuration settings—Reset to default values
- Call histories—Erased
- Locale information—Reset to default values
- Phone application—Erased. The phone recovers by loading the appropriate default load file (term62.default.loads, term61.default.loads, term42.default.loads, or term41.defaults.loads) depending on the phone model.

Before you perform a factory reset, ensure that the following conditions are met:

- The phone must be on a DHCP-enabled network.
- A valid TFTP server must be set in DHCP option 150 or option 66 on the DHCP server.
- The default load file for your phone model and the files specified in that file should be available on the TFTP server that is specified by the DHCP packet.

To perform a factory reset of a phone, perform the following steps:

Procedure

Step 1 Unplug the power cable from the phone and then plug the cable back in.

The phone begins its power-up cycle.

Step 2 While the phone is powering up, and before the Speaker button flashes on and off, press and hold **#**.

Continue to hold **#** until each line button flashes on and off in sequence in amber.

Step 3 Release **#** and press **123456789*0#**.

You can press a key twice in a row, but if you press the keys out of sequence, the factory reset will not take place.

After you press these keys, the line buttons on the phone flash red, and the phone goes through the factory reset process.

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

Using the Quality Report Tool

The Quality Report Tool (QRT) is a voice quality and general problem-reporting tool for the Cisco Unified IP Phone. The QRT feature is installed as part of the Cisco Unified Communications Manager installation.

You can configure users' Cisco Unified IP Phones with QRT. When you do so, users can report problems with phone calls by pressing the QRT softkey. This softkey is available only when the Cisco Unified IP Phone is in the Connected, Connected Conference, Connected Transfer, or OnHook states.

When a user presses the **QRT** softkey, a list of problem categories appears. The user selects the appropriate problem category, and this feedback is logged in an XML file. Actual information logged depends on the user selection, and whether the destination device is a Cisco Unified IP Phone.

For more information about using QRT, see *Cisco Unified Communications Manager Features and Services Guide*.

Monitoring the Voice Quality of Calls

To measure the voice quality of calls that are sent and received within the network, Cisco Unified IP Phones use the following 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—Shows the ratio of concealment frames over total speech frames. The phone calculates an interval conceal ratio every 3 seconds.
- Concealed Second metrics—Shows 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.
- MOS-LQK metrics—Uses a numeric score to estimate the relative voice listening quality. The Cisco Unified IP Phone calculates the mean opinion score (MOS) for listening quality (LQK) based audible concealment events due to frame loss in the preceding 8 seconds, and includes perceptual weighting factors such as codec type and frame size.

  The phone uses the Cisco proprietary algorithm, Cisco Voice Transmission Quality (CVTQ) index, to produce MOS LQK scores. Depending on the MOS LQK version number, these scores might be compliant 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 while MOS LQK scores project a "human-weighted" version of the same information on a scale from 5 (excellent) to 1 (bad) for measuring listening quality.

Listening quality scores (MOS LQK) relate to the clarity or sound of the received voice signal. Conversational quality scores (MOS CQ, such as G.107) include impairment factors, such as delay, that degrade the natural flow of conversation.

You can access voice quality metrics from the Cisco Unified IP Phone by using the Call Statistics screen (see Call Statistics Screen, page 8-14) or remotely by using Streaming Statistics (see Monitoring the Cisco Unified IP Phones Remotely).

Using Voice Quality Metrics

To use 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 important to distinguish significant changes from random changes in metrics. Significant changes are scores that change about 0.2 MOS or greater and persist in calls that last longer than 30 seconds. Conceal Ratio changes should indicate greater than 3 percent frame loss.

MOS LQK scores can vary based on the codec that the Cisco Unified IP Phone uses.

The following codecs on the Cisco Unified IP Phones 7962G and 7942G provide these maximum MOS LQK scores under normal conditions with zero frame loss:

- G.711 gives 4.5
- G.722 gives 4.5
- G.728/iLBC gives 3.9
- G.729 A/AB gives 3.8

The following codecs on the Cisco Unified IP Phones 7961G/G-GE and 7941G/G-GE provide these maximum MOS LQK scores under normal conditions with zero frame loss:

- G.711 codec gives 4.5 score
- G.729A/ AB gives 3.7

Note

- CVTQ does not support wideband (7 kHz) speech codecs, because ITU has not defined the extension of the technique to wideband. Therefore, MOS 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/low packet loss, and lower scores (approximately 3.5) indicate low quality/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.

Troubleshooting Tips

When you observe significant and persistent changes to metrics, use Table 9-5 for general troubleshooting information:

Table 9-5 Changes to Voice Quality Metrics

Metric Change	Condition
MOS LQK scores decrease significantly	Network impairment from packet loss or high jitter: • Average MOS LQK decreases could indicate widespread and uniform impairment. • Individual MOS LQK decreases indicate bursty impairment. Cross-check with Conceal Ratio and Conceal Seconds for evidence of packet loss and jitter.
MOS LQK scores decrease 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.
Conceal Ratio and Conceal Seconds increase significantly	• Network impairment from packet loss or high jitter.
Conceal Ratio is near or at zero, but the voice quality is poor.	• Noise or distortion in the audio channel such as echo or audio levels. • Tandem calls that undergo multiple encode/decode such as calls to a cellular network or calling card network. • Acoustic problems coming from a speakerphone, handsfree cellular phone or wireless headset. Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.

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

Where to Go for More Troubleshooting Information

If you have additional questions about troubleshooting the Cisco Unified IP Phones, 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_series_home.html

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

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

Cleaning the Cisco Unified IP Phone

To clean your Cisco Unified IP Phone, use only a dry soft cloth to gently wipe the phone and the LCD screen. Do not apply liquids or powders directly on the phone. As with all non-weather-proof electronics, liquids and powders can damage the components and cause failures.

APPENDIX A

Providing Information to Users Via a Website

If you are a system administrator, you are likely the primary source of information for Cisco Unified IP Phone users in your network or company. It is important to provide current and thorough information to end users.

Cisco recommends that you create a web page on your internal support site that provides end users with important information about their Cisco Unified IP Phones.

Consider including the following types of information on this site:

How Users Obtain Support for the Cisco Unified IP Phones

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

Giving Users Access to the User Options Web Pages

Before a user can access the User Options web pages, you must use Cisco Unified Communications Manager Administration to add the user to a standard Cisco Unified Communications Manager end user group. From the Cisco Unified Communications Manager Administration, choose **User Management > User Groups**. For additional information, see:

- *Cisco Unified Communications Manager Administration Guide*, User Group Configuration
- *Cisco Unified Communications Manager System Guide*, Roles and User Groups

How Users Access the Online Help System on the Cisco Unified IP Phone

The Cisco Unified IP Phones provide access to a comprehensive online help system. To view the main help menu on a phone, press the **?** button. If you are already in Help, press **Main**.

Main menu topics include:

- About Your Cisco Unified IP Phone—Descriptive information about the phone model
- How do I...?—Procedures and information about commonly used phone tasks
- Calling Features—Descriptions and procedures for using calling features, such as conference and transfer
- Help—Tips on using and accessing Help

You can also use the ? button to obtain information about softkeys, menu items, and the help system itself. See your Cisco Unified IP Phone User Guide for more information.

How Users Get Copies of Cisco Unified IP Phone Manuals

You should provide end users with access to user documentation for the Cisco Unified IP Phones. Each user guide includes detailed user instructions for key phone features.

There are several Cisco Unified IP Phone models available, so to assist users in finding the appropriate documentation on the Cisco website, Cisco recommends that you provide links to the current documentation. If you do not want to or cannot send users to the Cisco website, Cisco suggests that you download the PDF files and provide them to end users on your website.

For a list of available documentation for Cisco Unified IP Phones, go to this URL:

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

For a list of available documentation for Cisco Unified Communications Manager, go to this URL:

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

For more information about viewing or ordering documentation, see Obtaining Documentation, Obtaining Support, and Security Guidelines, page -xiii.

Accessing Cisco 7900 Series Unified IP Phone eLearning Tutorials for SCCP Phones Only

Cisco 7900 Series Unified IP Phone eLearning tutorials use audio and animation to demonstrate basic calling features for SCCP phones. The eLearning tutorials are currently available for the Cisco Unified IP Phone 7970 Series (7970G/7971G-GE), and the Cisco Unified IP Phone models 7961G/G-GE, 7941G/G-GE, 7960G, 7940G, 7912G, and 7905G.

End users can access runtime versions of the eLearning tutorials (English only) from Cisco.com by looking for tutorials under relevant phone models at this site:

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

Administrators can download customizable versions of the eLearning tutorials (English only) from the phone product pages on Cisco.com

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

See the tutorial Read Me file that is included with the relevant eLearning tutorial for specific instructions, including how to link to the most recent user guide PDF.

Note The eLearning tutorials are updated periodically and therefore might not contain the latest feature information for end users. For the latest feature information, end users should see the Cisco Unified IP Phone end users user guide specific to their phone model and Cisco Unified Communications Manager version.

How Users Subscribe to Services and Configure Phone Features

End users can perform a variety of activities by using the Cisco Unified Communications Manager User Options web pages. These activities include subscribing to services, setting up speed dial and call forwarding numbers, configuring ring settings, and creating a personal address book. Keep in mind that configuring settings on a phone by using a website might be new for your end users. You need to provide as much information as possible to ensure that they can successfully access and use the User Options web pages.

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

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

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

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

  These settings correspond to the values you entered when you added the user to Cisco Unified Communications Manager (see Adding Users to Cisco Unified Communications Manager, page 5-28).

- A brief description of what a web-based, graphical user interface application is, and how to access it with a web browser.
- An overview of the tasks that users can accomplish by using the web page.

How Users Access a Voice Messaging System

Cisco Unified Communications Manager lets you integrate with many different voice messaging systems, including the Cisco Unity voice messaging system. Because you can integrate with a variety of systems, you must provide users with information about how to use your specific system.

You should provide this information to each user:

- How to access the voice messaging system account.

  Make sure that you have used Cisco Unified Communications Manager to configure the **Messages** button on the Cisco Unified IP Phone.

- Initial password for accessing the voice messaging system.

  Make sure that you have configured a default voice messaging system password for all users.

- How the phone indicates that voice messages are waiting.

Make sure that you have used Cisco Unified Communications Manager to set up a message waiting indicator (MWI) method.

How Users Configure Personal Directory Entries

Users can configure personal directory entries on the Cisco Unified IP Phone. To configure a personal directory, users must have access to the following:

- User Options web pages—Make sure that users know how to access their User Options web pages. See How Users Subscribe to Services and Configure Phone Features, page A-3 for details.
- Cisco Unified IP Phone Address Book Synchronizer—Make sure to provide users with the installer for this application. To obtain the installer, choose **Application > Plugins** from Cisco Unified Communications Manager Administration and click **Download**, which is located next to the **Cisco Unified IP Phone Address Book Synchronizer** plugin name. When the file download dialog box displays, click **Save**. Send the TabSyncInstall.exe file to all users who require this application.

See Installing and Configuring the Cisco Unified IP Phone Address Book Synchronizer, page A-4 for information about installing the Cisco Unified IP Phone Address Book Synchronizer.

Installing and Configuring the Cisco Unified IP Phone Address Book Synchronizer

Use this tool to synchronize data stored in your Microsoft Windows address book with the Cisco Unified Communications Manager directory and the User Options Personal Address Book.

Tip To successfully synchronize the Windows address book with the Personal Address Book, all Windows address book users should be entered in the Windows address book before performing the following procedures.

Installing the Synchronizer

Step 1 Get the Cisco Unified IP Phone Address Book Synchronizer installer file from your system administrator.

Step 2 Double-click the TabSyncInstall.exe file provided by your system administrator.

The publisher dialog box displays.

Step 3 Click **Run**.

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

Step 4 Click **Next**.

The License Agreement window displays.

Step 5 Read the license agreement information, and click the I Accept radio button. Click **Next**.

The Destination Location window displays.

Step 6 Choose the directory in which you want to install the application and click **Next**.

The Ready to Install window displays.

Step 7 Click **Install**.

The installation wizard installs the application to your computer. When the installation is complete, the InstallShield Wizard Complete window displays.

Step 8 Click **Finish**.

Step 9 To complete the process, follow the steps in Configuring the Synchronizer, page A-5.

Configuring the Synchronizer

Step 1 Open the Cisco Unified IP Phone Address Book Synchronizer.

If you accepted the default installation directory, you can open the application by choosing **Start > All Programs > Cisco Systems > TabSync**.

Step 2 To configure user information, click the **User** button.

The Cisco Unified CallManager User Information window displays.

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

Step 4 To configure Cisco Unified Communications Manager server information, click the **Server** button.

The Configure Cisco Unified CallManager Server Information window displays.

Step 5 Enter the IP address or host name and the port number of the Cisco Unified Communications Manager server and click **OK**.

If you do not have this information, contact your system administrator.

Step 6 To start the directory synchronization process, click the **Synchronize** button.

The Synchronization Status window provides information on the status of the address book synchronization. If you chose the user intervention for duplicate entries rule and you have duplicate address book entries, the Duplicate Selection window displays. Choose the entry that you want to include in your Personal Address Book and click **OK**.

Step 7 When synchronization completes, click **Exit** to close the Cisco Unified CallManager Address Book Synchronizer.

Step 8 To verify if the synchronization worked, log in to your User Options web pages and choose Personal Address Book. The users from your Windows address book should be listed.

APPENDIX B

Feature Support by Protocol for Cisco Unified IP Phone

This appendix provides information about feature support for the Cisco Unified IP Phones using the SCCP or SIP protocol with Cisco Unified Communications Manager Release 8.6.

Table B-1 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 *Cisco Unified IP Phone 7962G, 7942G, 7961G, 7961G-GE, 7941G, and 7941G-GE User Guide.*

This guide is available at this URL:

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

The specific sections that describe the features in the phone guide are referenced in Table B-1.

Table B-1 Cisco Unified IP Phone Feature Support by Protocol

Features	Cisco Unified IP Phones 7962G, 7942G, 7961G, 7961G-GE, 7941G, and 7941G-GE		For More Information
	SCCP	SIP	
Calling Features			
Abbreviated Dialing	Supported	Supported	Basic Call Handling—Placing a Call: Additional Options
Agent Greeting	Supported	Supported	Basic Call Handling—Answering a Call
Assisted Directed Call Park	Not supported	Supported	Advanced Call Handling—Storing and Retrieving Parked Calls
Audible Message Waiting Indicator	Supported	Supported	Accessing Voice Messages
Auto Answer	Supported	Supported	Using a Handset, Headset, and Speakerphone—Using Auto Answer
Auto Dial	Supported	Supported	Basic Call Handling—Placing a Call: Basic Options
Barge (and cBarge)	Supported	Supported	Advanced Call Handling—Using a Shared Line
Busy Lamp Field (BLF)	Supported	Supported	Advanced Call Handling—Using BLF to Determine a Line State
Busy Lamp Field (BLF) Pickup	Supported	Supported	Advanced Call Handling—Using BLF to Determine a Line State

Table B-1 Cisco Unified IP Phone Feature Support by Protocol (continued)

Features	Cisco Unified IP Phones 7962G, 7942G, 7961G, 7961G-GE, 7941G, and 7941G-GE		For More Information
	SCCP	SIP	
Calling Features			
Busy Lamp Field (BLF) Speed Dial	Supported	Supported	Advanced Call Handling—Using BLF to Determine a Line State
Call Back	Supported	Supported	Basic Call Handling—Placing a Call: Additional Options
Call Chaperone	Supported	Supported	
Call Display Restrictions	Supported	Supported	
Call Forward All	Supported	Supported	Basic Call Handling—Forwarding Calls to Another Number
Call Forward All Breakout	Supported	Supported	Basic Call Handling—Forwarding Calls to Another Number
Call Forward All Loop Prevention	Supported	Supported	Basic Call Handling—Forwarding Calls to Another Number
Call Forward Busy	Supported	Supported	Basic Call Handling—Forwarding Calls to Another Number
Call Forward Configurable Display	Supported	Supported	
Call Forward Destination Override	Supported	Supported	
Call Forward No Answer	Supported	Supported	Basic Call Handling—Forwarding Calls to Another Number
Call Park	Supported	Supported	Advanced Call Handling—Storing and Receiving Parked Calls
Call Pickup/Group Call Pickup/Directed Call Pickup	Supported	Supported	Advanced Call Handling—Picking Up a Redirected Call on Your Phone
Call Waiting	Supported	Supported	Basic Call Handling—Answering a Call
Caller ID	Supported	Supported	An Overview of Your Phone—Understanding Touch Screen Features or An Overview of Your Phone—Understanding Phone Screen Features
Client Matter Codes (CMC)	Supported	Not supported	Basic Call Handling—Placing a Call: Additional Options
Conference	Supported	Supported	Basic Call Handling—Making Conference Calls
Computer Telephony Integration (CTI) Applications	Supported	Some support (such as Call Park, MWI)	Users do not interact with this feature directly. It is configured on Cisco Unified Communications Manager
Directed Call Park	Supported	Supported	Advanced Call Handling—Storing and Receiving Parked Calls
Distinctive Ring	Supported	Supported	Using Phone Settings—Customizing Rings and Message Indicators

Table B-1 Cisco Unified IP Phone Feature Support by Protocol (continued)

Features	Cisco Unified IP Phones 7962G, 7942G, 7961G, 7961G-GE, 7941G, and 7941G-GE		For More Information
	SCCP	SIP	
Calling Features			
Do Not Disturb (DND)	Supported	Supported	Basic Call Handling—Using Do Not Disturb
Enbloc Dialing	Supported	Not Supported	
Extension Mobility	Supported	Supported	Advanced Call Handling—Using Cisco Extension Mobility
Extension Mobility ChangePIN	Supported	Supported	Advanced Call Handling—Using Cisco Extension Mobility
Extension Mobility Cross Cluster	Supported	Supported	
Fast Dial Service	Supported	Supported	Advanced Call Handling—Speed Dialing
Forced Authorization Codes (FAC)	Supported	Not supported	Basic Call Handling—Placing a Call: Additional Options
Help System	Supported	Supported	An Overview of Your Phone—Understanding Feature Buttons and Menus
Hold/Resume	Supported	Supported	Basic Call Handling—Using Hold and Resume
Hold Reversion	Supported	Supported	Basic Call Handling—Using Hold and Resume
Hold Status	Supported	Supported	Using Hold and Resume
Hunt Group	Supported	Supported	
Immediate Divert	Supported	Supported	Basic Call Handling—Answering a Call
Immediate Divert—Enhanced	Supported	Supported	Basic Call Handling—Sending a Call to a Voice Messaging System
Intelligent Session Control	Supported	Supported	
Inter-Cluster Trust (Bulk Certificate Replication)	Supported	Supported	
Intercom	Supported	Supported	Basic Call Handling—Placing or Receiving Intercom Calls
Intra-Cluster Trust (Bulk Certificate Replication)	Supported	Supported	
Join/Select	Supported	Supported	Basic Call Handling—Making Conference Calls
Join Across Lines/Select	Supported	Supported	Basic Call Handling—Making Conference Calls
Line select	Supported	Supported	Configuring Features, Templates, Services, and Users—Telephony Features Available for the Phone
Line select for voice messages	Supported	Supported	Configuring Features, Templates, Services, and Users—Telephony Features Available for the Phone
Log Out of Hunt Groups	Supported	Supported	Advanced Call Handling—Logging Out of Hunt Groups
Malicious Call ID	Supported	Supported	Advanced Call Handling—Tracing Suspicious Calls
Meet-Me Conference	Supported	Supported	Basic Call Handling—Making Conference Calls

Table B-1 Cisco Unified IP Phone Feature Support by Protocol (continued)

Features	Cisco Unified IP Phones 7962G, 7942G, 7961G, 7961G-GE, 7941G, and 7941G-GE		For More Information
	SCCP	SIP	
Calling Features			
Missed call logging	Supported	Supported	Using Call Logs and Directories
Mobile Connect	Supported	Supported	Advanced Call Handling—Answering a Call
Multilevel Precedence and Preemption (MLPP)	Supported	Not supported	Advanced Call Handling—Prioritizing Critical Calls
Multiple Calls per Line Appearance	200	50	An Overview of Your Phone—Understanding Lines vs. Calls
Mute	Supported	Supported	Basic Call Handling—Using Mute
On-hook Dialing/Pre-Dial	Supported	Supported	Basic Call Handling—Placing a Call: Basic Options
Other Group Pickup	Supported	Supported	
Phone Secure Web Access	Supported	Supported	
Plus Dialing	Supported	Supported	Using Call Logs
Privacy	Supported	Supported	Advanced Call Handling—Using a Shared Line
Programmable Line Keys	Supported	Supported	Feature descriptions throughout phone guide
Protected Calling	Supported	Supported	An Overview of the Cisco Unified IP Phone—Understanding Security Features for Cisco Unified IP Phones
Quality Reporting Tool (QRT)	Supported	Supported	Troubleshooting—Using the Quality Reporting Tool
Redial	Supported	Supported	Basic Call Handling—Placing a Call: Basic Options
Ringer Volume Control	Supported	Supported	Changing Phone Settings—Customizing Rings and Message Indicators
Secure and Nonsecure Indication Tone	Supported	Supported	Advanced Call Handling—Making and Receiving Secure Calls
Secure Conference	Supported	Supported	Basic Call Handling—Making Conference Calls
Session Handoff	Supported	Supported	Advanced Call Handling—Using a Shared Line
Shared Line	Supported	Supported	Advanced Call Handling—Using a Shared Line
Sidetone Level	Supported	Supported (7941G and 7961G only)	
Single Button Barge	Supported	Supported	Advanced Call-Handling—Using Barge to Add Yourself to a Shared-Line Call
Speed Dialing	Supported	Supported	Advanced Call Handling—Speed Dialing
SSH Access	Supported	Supported	
Transfer	Supported	Supported	Basic Call Handling—Transferring Calls
Time Zone Update	Supported	Supported	
URL Dialing	Not supported	Supported	Using Call Logs and Directories—Using Call Logs
Video Support	Supported	Not supported	Understanding Additional Configuration Options

Table B-1 Cisco Unified IP Phone Feature Support by Protocol (continued)

Features	Cisco Unified IP Phones 7962G, 7942G, 7961G, 7961G-GE, 7941G, and 7941G-GE		For More Information
	SCCP	SIP	
Calling Features			
VPN Client	Supported (7942G and 7962G only)	Not supported	Advanced Call Handling—Making and Receiving Secure Calls
VPN Support in Phones	Supported	Supported	
Voice Mail	Supported	Supported	Accessing Voice Messages section of the Phone Guide
WebDialer	Supported	Supported	Customizing Your Phone on the Web—Configuring Features and Services on the Web
Settings			
Automatic Port Synchronization	Supported	Supported	
Call Statistics	Supported	Supported	Troubleshooting Your Phone—Viewing Phone Administrative Data
Power Save Plus (EnergyWise)	Supported	Not supported	An Overview of the Cisco Unified IP Phone—Reducing Power Consumption on the Phone
Remote Port Configuration	Supported	Supported	
SSH Disable	Supported	Supported	Configuring Features, Templates, Services, and Users—Telephony Features Available for the Cisco Unified IP Phone
UCR 2008	Supported	Not supported	Configuring Features, Templates, Services, and Users—Telephony Features Available for the Cisco Unified IP Phone
Voice Quality Metrics	Supported	Supported	Troubleshooting Your Phone—Viewing Phone Administrative Data
Services			
SDK Compliance	Supported	Supported	*Cisco Unified IP Phone Service Application Development Notes*
Directories			
Call Logs	Supported	Supported	Using Call Logs and Directories—Directory Dialing
Corporate Directories	Supported	Supported	Using Call Logs and Directories—Directory Dialing
Personal Directory Enhancements	Supported	Supported	Using Call Logs and Directories—Directory Dialing

Table B-1 Cisco Unified IP Phone Feature Support by Protocol (continued)

Features	Cisco Unified IP Phones 7962G, 7942G, 7961G, 7961G-GE, 7941G, and 7941G-GE		For More Information
	SCCP	SIP	
Calling Features			
Supplemental Features and Applications			
Cisco Unified Communications Manager Assistant	Supported	Supported	*Cisco Unified Communications Manager Assistant User Guide*
Cisco Unified Communications Manager Auto-Attendant	Supported	Not supported	*Cisco Unified Communications Manager Features and Services Guide*
Cisco Unified Business Attendant Console, Cisco Unified Department Attendant Console, or Cisco Unified Enterprise Attendant Console	Supported	Supported	These are third-party products. See http://www.cisco.com/en/US/products/ps7282/prod_maintenance_guides_list.html
Cisco Unified IP Phone Expansion Module 7914	Supported (7962G only)	Supported (7962G only)	*Cisco Unified IP Phone Expansion Module 7914 Phone Guide*
Cisco Unified IP Phone Expansion Module 7915	Supported (7962G only)	Supported (7962G only)	*Cisco Unified IP Phone Expansion Module 7915 Phone Guide*
Cisco Unified IP Phone Expansion Module 7916	Supported (7962G only)	Supported (7962G only)	*Cisco Unified IP Phone Expansion Module 7916 Phone Guide*
Cisco VT Advantage	Supported	Not supported	*Cisco VT Advantage User Guide*

APPENDIX C

Supporting International Users

Translated and localized versions of the Cisco Unified IP Phones are available in several languages. If you are supporting Cisco Unified IP Phones in a non-English environment, see the following sections to ensure that the phones are set up properly for your users:

Adding Language Overlays to Phone Buttons

To support the needs of international users, the button labels on the Cisco Unified IP Phones exhibit icons rather than text to indicate the purposes of the buttons. You can purchase language-specific text overlays to add to a phone. To order these language-specific overlays, go to this website:

http://www.overlaypro.com/cisco_systems?b=1

Note Phone overlays are available only for languages in which the Cisco Unified IP Phone software has been localized. All languages may not be immediately available, so continue to check the website for updates.

Installing the Cisco Unified Communications Manager Locale Installer

If you are using Cisco Unified IP Phones in a locale other than English (United States), you must install the locale-specific version of the Cisco Unified Communications Manager Locale Installer on every Cisco Unified Communications Manager server in the cluster. Installing the locale installer ensures that you have the latest translated text, user and network locales, and country-specific phone tones available for the Cisco Unified IP Phones. You can find locale-specific versions of the Cisco Unified Communications Manager Locale Installer at http://www.cisco.com/kobayashi/sw-center/telephony/callmgr/locale-installer.shtml.

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

Note All languages may not be immediately available, so continue to check the website for updates.

Support for International Call Logging

If your phone system is configured for international call logging, the call logs, redial, or call directory entries may display a "+" symbol to represent the international escape code for your location. Depending on the configuration for your phone system, the "+" may be replaced with the correct international dialing code, or you may need to edit the number before dialing to manually replace the "+" with the international escape code for your location. In addition, while the call log or directory entry may display the full international number for the received call, the phone display may show the shortened local version of the number, without international or country codes.

APPENDIX D

Technical Specifications

The following sections describe the technical specifications for the Cisco Unified IP Phones.

Physical and Operating Environment Specifications

Table D-1 shows the physical and operating environment specifications for the Cisco Unified IP Phones.

Table D-1 Physical and Operating Specifications

Specification	Value or Range
Operating temperature	32° to 104°F (0° to 40°C)
Operating relative humidity	10% to 95% (non-condensing)
Storage temperature	14° to 140°F (–10° to 60°C)
Height	8 in. (20.32 cm)
Width	10.5 in. (26.67 cm)
Depth	6 in. (15.24 cm)
Weight	3.5 lb (1.6 kg)
Power	**Cisco Unified IP Phone 7962G and 7942G** • 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 **Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE** • The phone can receive power from IEEE 802.3af-compliant data switches (Class III) • The phone can be powered locally with a power adapter (Cisco part number CP-PWR-CUBE-3=) and the appropriate power cord (power requirements for the power adapter: 100-240 VAC, 50-60 Hz, 0.5 A)

Table D-1 Physical and Operating Specifications (continued)

Specification	Value or Range
Cables	Category 3/5/5e for 10-Mbps cables with 4 pairs Category 5/5e for 100-Mbps cables with 4 pairs Category 5e/6 for 1000-Mbps cables with 4 pairs **Note** Cables have 4 pairs of wires for a total of 8 conductors.
Distance Requirements	As supported by the Ethernet Specification, it is assumed that the maximum cable length between each Cisco Unified IP Phone and the switch is 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 Phones 7962G, 7942G, 7961G and 7941G
  - labeled 10/100/1000 SW on the Cisco Unified IP Phones 7961G-GE and 7941G-GE).
- RJ-45 jack for a second 10/100BaseT compliant connection
  - (labeled 10/100 PC on the Cisco Unified IP Phones 7962G, 7941G, 7961G and 7941G
  - labeled 10/100/1000 PC on the Cisco Unified IP Phones 7961G-GE and 7941G-GE).
- 48-volt power connector.

Network and Access 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 `10/100 SW or 10/100/1000 SW` on the Cisco Unified IP Phone.
- The access port is labeled `10/100 PC or 10/100/1000 PC` on the Cisco Unified IP Phone.

Network Port Connector

Table D-2 describes the network port connector pinouts.

Table D-2 Network Port Connector Pinouts

Pin Number	Function
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+

Table D-2 Network Port Connector Pinouts (continued)

Pin Number	Function
8	BI_DD-
"BI" stands for bi-directional, while DA, DB, DC and DD stand for "Data A", "Data B", "Data C" and "Data D," respectively.	

Access Port Connector

Table D-3 describes the access port connector pinouts.

Table D-3 Access Port Connector Pinouts

Pin Number	Function
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-

Note "BI" stands for bi-directional, while DA, DB, DC and DD stand for "Data A", "Data B", "Data C" and "Data D", respectively.

APPENDIX E

Basic Phone Administration Steps

This appendix provides minimum, basic configuration steps for you to perform the following actions:

- Add a new user to Cisco Unified Communications Manager Administration
- Configure a new phone for that user
- Associate that user to that phone
- Complete other basic end user configuration tasks

The procedures provide one method for performing these tasks and are not the only way to perform these tasks. They are a streamlined approach to get a new user and corresponding phone running on the system.

These procedures are designed to be used on a mature Cisco Unified Communications Manager system where calling search spaces, partitions, and other complicated configuration have already been done and are in place for existing users.

This section contains these topics:

Example User Information for these Procedures

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

- User's Name: John Doe
- User ID: johndoe
- Phone model: 7961G
- Protocol: SCCP
- MAC address listed on phone: 00127F576611
- Five-digit internal telephone number: 26640

Adding a User to Cisco Unified Communications Manager

This section describes steps for adding a user to Cisco Unified Communications Manager. Follow one of the procedures in this section, depending on your operating system and the manner in which you are adding the user:

- Adding a User From an External LDAP Directory, page E-2
- Adding a User Directly to Cisco Unified Communications Manager, page E-3

Adding a User From an External LDAP Directory

If you added a user to an LDAP Directory (a non-Cisco Unified Communications Server directory), you can immediately synchronize that directory to the Cisco Unified Communications Manager on which you are adding this same user and the user's phone by following these steps:

Note Before you perform the following procedure, you must check the Enable Synchronizing from LDAP Server check box in the LDAP System Configuration window of Cisco Unified Communications Manager Administration (**System > LDAP > LDAP System**).

Procedure

Step 1 Log onto Cisco Unified Communications Manager Administration.

Step 2 Choose **System > LDAP > LDAP Directory**.

Step 3 Use the **Find** button to locate your LDAP directory.

Step 4 Click on the LDAP directory name.

Step 5 Click **Perform Full Sync Now**.

Note If you do not need to immediately synchronize the LDAP Directory to the Cisco Unified Communications Manager, the LDAP Directory Synchronization Schedule on the LDAP Directory window determines when the next auto-synchronization is scheduled. However, the synchronization must occur before you can associate a new user to a device.

Step 6 Proceed to Configuring the Phone, page E-3.

For more information and limitations on configuring LDAP system, see *Cisco Unified Communications Manager Administration Guide*, LDAP System Configuration, LDAP Directory Configuration, and LDAP Authentication Configuration and *Cisco Unified Communications Manager System Guide, Cisco Systems, Inc.* Understanding the Directory.

Adding a User Directly to Cisco Unified Communications Manager

If you are not using an LDAP directory, you can add a user directly to Cisco Unified Communications Manager Administration by following these steps:

Procedure

Step 1 Choose **User Management > End User**, then click **Add New.** The End User Configuration window appears.

Step 2 In the User Information pane of this window, enter the following:

- User ID—Enter the end user identification name. Cisco Unified Communications Manager does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.

  Example: *johndoe*

- Password and Confirm Password—Enter five or more alphanumeric or special characters for the end user password. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.

- Last Name—Enter the end user last name. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.

  Example: *doe*

- Telephone Number—Enter the primary directory number for the end user. End users can have multiple lines on their phones.

  Example: 26640 (John Doe's internal company telephone number)

Step 3 Click **Save**.

Step 4 Proceed to the section Configuring the Phone, page E-3.

Configuring the Phone

First, perform the following procedure to identify the user's phone model and protocol:

Procedure

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

Step 2 Click **Add New**.

Step 3 Select the user's phone model from the Phone Type drop-down list, then click **Next**.

Step 4 Select the device protocol (SCCP or SIP) from the drop-down list, then click **Next**. The Phone Configuration window appears.

On the Phone Configuration window, you can use the default values for most of the fields.

To configure the required fields and some key additional fields, follow these steps:

Procedure

Step 1 For the required fields, possible values, some of which are based on the example of user *johndoe*, can be configured as follows:

a. In the Device Information pane of this window:

- MAC Address—Enter the MAC address of the phone, which is listed on a sticker on the phone.

  Make sure that the value comprises 12 hexadecimal characters.

  Example: 00127F576611 (MAC address on john doe's phone)

- Description—This is an optional field in which you can enter a useful description, such as *john doe's phone*. This will help you if you need to search on information about this user.

- Device Pool—Choose the device pool to which you want this phone assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, softkey template, and MLPP information.

  Note Device Pools are defined on the Device Pool Configuration window of Cisco Unified Communications Server Administration (**System > Device Pool**).

- Phone Button Template—Choose the appropriate phone button template from the drop-down list. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.

  Note Phone button templates are defined on the Phone Button Template Configuration window of Cisco Unified Communications Manager Administration (**Device > Device Settings > Phone Button Template**). You can use the search 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.

  Note 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.

  Note Common Phone Profiles are defined on the Common Phone Profile Configuration window of Cisco Unified Communications Manager Administration (**Device > Device Settings > Common Phone Profile**). You can use the search 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.

  Note Calling Search Spaces are defined on the Calling Search Space Configuration window of Cisco Unified Communications Manager Administration (**Calling routing > Class of Control> Calling Search Space**). You can use the search 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 non-secure profile.

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

Note The security profile chosen should be based on the overall security strategy of the company.

c. (For SIP Phones only) Also in the Protocol Specific Information pane of this window, choose the applicable SIP Profile from the drop-down list.

d. In the Extension Information pane of this window, check the Enable Extension Mobility box if this phone supports Cisco Extension Mobility.

e. In the Product Specific Configuration Layout pane of this window, enable the Video Capabilities field if this field appears on your window.

f. Click **Save**.

Step 2 Configure line settings:

a. On the Phone Configuration window, click Line 1 on the left pane of the window. The Directory Number Configuration window appears.

b. In the Directory Number field, enter a valid number that can be dialed.

Note This field should contain the same number that appears in the Telephone Number field on the User Configuration window.

Example: 26640 is the directory number of user John Doe in the example above.

c. From the Route Partition drop-down list, choose the partition to which the directory number belongs. If you do not want to restrict access to the directory number, choose <None> for the partition.

d. From the Calling Search Space drop-down list (Directory Number Settings pane of the Directory Number Configuration window), choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. The value that you choose applies to all devices that are using this directory number.

e. In the Call Pickup and Call Forward Settings pane of the Directory Number Configuration window, choose the items (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 the Directory Number Configuration window, configure the following fields:

   - Display (Internal Caller ID field)—You can enter the first name and last name of the user of this device so that this name will be displayed for all internal calls. You can also leave this field blank to have the system display the phone extension.
   - External Phone Number Mask—Indicate phone number (or mask) that is used to send Caller ID information when a call is placed from this line.

     You can enter a maximum of 24 number and "X" characters. The Xs represent the directory number and must appear at the end of the pattern.

     Example: Using the john doe extension in the example above, if you specify a mask of 408902XXXX, an external call from extension 6640 displays a caller ID number of 4089026640.

     Note This setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the **Propagate Selected** button. The check box at right displays only if other devices share this directory number.

g. Click **Save**.

h. Click **Associate End Users** at the bottom of the window to associate a user to the line being configured. Use the **Find** button in conjunction with the Search fields to locate the user, then check the box next to the user's name, and then click **Add Selected**. The user's name and user ID should now appear in the "Users Associated With Line" pane of the Directory Number Configuration window.

i. Click **Save**. The user is now associated with Line 1 on the phone.

j. If the 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).
   - Click on the user ID (for example, *johndoe*). The End User Configuration window appears.
   - Click **Device Associations**.
   - Use the Search fields and the Find button to locate the device with which you want to associate to the user.

- Select the device, then click **Save Selected/Changes**. The user is now associated with the device.
- Click the **Go** button next to the "Back to User" Related link in the upper-right corner of the screen.

l. Proceed to Performing Final End User Configuration Steps, page E-7.

Performing Final End User Configuration Steps

If you are not already on the End User Configuration page, choose **User Management > End User** to perform some final configuration tasks. Use the Search fields and the Find button to locate the user (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, do the following:

Procedure

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

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

Step 3 In the Permissions Information pane, use the User Group buttons to add this user to any user groups. For example, you may want to add the user to a group that has been defined as a Standard CCM End User Group.

To view all configured user groups, choose **User Management > User Group**.

Step 4 Click **Save**.

INDEX

Symbols

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W