



Cisco Unified IP Phone 6901 and 6911 Administration Guide for Cisco Unified Communications Manager 8.5 (SCCP and SIP)

Americas Headquarters

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

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

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

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

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

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

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

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

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

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

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

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

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



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



CONTENTS

Preface vii

Overview	vii
Audience	vii
Organization	vii
Related Documentation	viii
Obtaining Documentation, Obtaining Support, and Security Guidelines	ix
Document Conventions	x

CHAPTER 1

An Overview of the Cisco Unified IP Phone 1-1

Understanding the Cisco Unified IP Phone 6901 and 6911	1-2
What Networking Protocols are Used?	1-6
What Features are Supported on the Cisco Unified IP Phone 6901 and 6911?	1-9
Feature Overview	1-9
Configuring Telephony Features	1-9
Configuring Network Parameters Using the Cisco Unified IP Phone	1-10
Providing Users with Feature Information	1-10
Understanding Security Features for Cisco Unified IP Phones	1-10
Overview of Supported Security Features	1-13
Understanding Security Profiles	1-15
Identifying Authenticated, Encrypted, and Protected Phone Calls	1-15
Establishing and Identifying Protected Calls	1-16
Call Security Interactions and Restrictions	1-16
Supporting 802.1X Authentication on Cisco Unified IP Phones	1-17
Overview	1-17
Required Network Components	1-18
Best Practices—Requirements and Recommendations	1-19
Overview of Configuring and Installing Cisco Unified IP Phones	1-19
Configuring Cisco Unified IP Phones in Cisco Unified Communications Manager	1-20
Checklist for Configuring the Cisco Unified IP Phone 6901 and 6911 in Cisco Unified Communications Manager	1-21
Installing Cisco Unified IP Phones	1-23
Checklist for Installing the Cisco Unified IP Phone 6901 and 6911	1-23
Terminology Differences	1-24

CHAPTER 2

Preparing to Install the Cisco Unified IP Phone on Your Network 2-1

- Understanding Interactions with Other Cisco Unified IP Telephony Products 2-1
 - Understanding How the Cisco Unified IP Phone Interacts with Cisco Unified Communications Manager 2-2
 - Understanding How the Cisco Unified IP Phone 6911 Interacts with the VLAN 2-2
- Providing Power to the Cisco Unified IP Phone 2-3
 - Power Guidelines 2-4
 - Power Outage 2-4
 - Obtaining Additional Information About Power 2-5
- Understanding Phone Configuration Files 2-5
- Understanding the Phone Startup Process 2-6
- Adding Phones to the Cisco Unified Communications Manager Database 2-7
 - Adding Phones with Auto-Registration 2-8
 - Adding Phones with Auto-Registration and TAPS 2-9
 - Adding Phones with Cisco Unified Communications Manager Administration 2-10
 - Adding Phones Using the BAT Phone Template 2-10
- Using Cisco Unified IP Phones with Different Protocols 2-11
 - Converting a New Phone from SCCP to SIP 2-11
 - Converting an In-Use Phone from One Protocol to the Other Protocol 2-11
 - Deploying a Phone in an SCCP and SIP Environment 2-12
- Determining the MAC Address for a Cisco Unified IP Phone 2-12

CHAPTER 3

Setting Up the Cisco Unified IP Phone 3-1

- Before You Begin 3-1
 - Network Requirements 3-1
 - Cisco Unified Communications Manager Configuration 3-2
- Understanding the Cisco Unified IP Phone 6901 and 6911 Components 3-2
 - Network and Access Ports 3-2
 - Handset 3-3
 - Speakerphone (Cisco Unified IP Phone 6911 Only) 3-3
- Installing the Cisco Unified IP Phone 3-4
 - Footstand 3-7
 - Higher Viewing Angle 3-8
 - Lower Viewing Angle 3-8
 - Mounting the Phone to the Wall 3-9
 - Verifying the Phone Startup Process 3-9
 - Configuring Startup Network Settings 3-9
 - Configuring Security on the Cisco Unified IP Phone 3-10

CHAPTER 4**Configuring Settings on the Cisco Unified IP Phone 4-1**

- Configuring Settings on the Cisco Unified IP Phone 4-1
 - Phone Settings Options 4-1
- Accessing the Phone Configuration Settings 4-2
 - Accessing the IVR and Configuring Your Phone Setting 4-2

CHAPTER 5**Configuring Features, Templates, Services, and Users 5-1**

- Telephony Features Available for the Cisco Unified IP Phone 5-1
- Adding Users to Cisco Unified Communications Manager 5-8
- Managing the User Options Web Pages 5-9
 - Giving Users Access to the User Options Web Pages 5-9
 - Specifying Options that Appear on the User Options Web Pages 5-11

CHAPTER 6**Monitoring the Cisco Unified IP Phone Remotely 6-1**

- Accessing the Web Page for a Phone 6-2
- Disabling and Enabling Web Page Access 6-3
- Device Information 6-3
- Network Setup 6-4
- Network Statistics 6-7
- Device Logs 6-9
 - Status Messages 6-10
- Streaming Statistics 6-13

CHAPTER 7**Troubleshooting and Maintenance 7-1**

- Resolving Startup Problems 7-1
 - Symptom: The Cisco Unified IP Phone Does Not Go Through its Normal Startup Process 7-2
 - Symptom: The Cisco Unified IP Phone Does Not Register with Cisco Unified Communications Manager 7-2
 - Identifying Error Messages 7-3
 - Checking Network Connectivity 7-3
 - Verifying TFTP Server Settings 7-3
 - Verifying IP Addressing and Routing 7-3
 - Cisco CallManager and TFTP Services Are Not Running 7-4
 - Creating a New Configuration File 7-4
 - Registering the Phone with Cisco Unified Communications Manager 7-5
 - Symptom: Cisco Unified IP Phone Unable to Obtain IP Address 7-5
- Cisco Unified IP Phone Resets Unexpectedly 7-6
 - Verifying the Physical Connection 7-6

- Identifying Intermittent Network Outages 7-6
- Verifying DHCP Settings 7-6
- Checking Static IP Address Settings 7-7
- Verifying the Voice VLAN Configuration 7-7
- Verifying that the Phones Have Not Been Intentionally Reset 7-7
- Eliminating DNS or Other Connectivity Errors 7-7
- Checking Power Connection 7-8
- General Troubleshooting Tips 7-8
- Resetting or Restoring the Cisco Unified IP Phone 7-10
 - Performing a Basic Reset 7-10
 - Performing a Factory Reset 7-10
- Monitoring the Voice Quality of Calls 7-11
- Using Voice Quality Metrics 7-11
 - Troubleshooting Tips 7-12
- Where to Go for More Troubleshooting Information 7-13
- Cleaning the Cisco Unified IP Phone 7-13

APPENDIX A

Providing Information to Users Via a Website A-1

- How Users Obtain Support for the Cisco Unified IP Phone A-1
- Giving Users Access to the User Options Web Pages A-1
- How Users Configure Phone Features A-2
- How Users Access a Voice Messaging System A-2

APPENDIX B

Supporting International Users B-1

- Installing the Cisco Unified Communications Manager Locale Installer B-1

APPENDIX C

Technical Specifications C-1

- Physical and Operating Environment Specifications C-1
- Cable Specifications C-2
- Network and Access Port Pinouts C-3

APPENDIX D

Basic Phone Administration Steps D-1

- Example User Information for These Procedures D-1
- Adding a User to Cisco Unified Communications Manager D-2
 - Adding a User From an External LDAP Directory D-2
 - Adding a User Directly to Cisco Unified Communications Manager D-2
- Configuring the Phone D-3

Performing Final End User Configuration Steps D-6

APPENDIX E

Installing the Wall Mount for the Cisco Unified IP Phone 6901 and 6911 E-1

Installing a Wall Mount for the Cisco Unified IP Phone 6901 E-1

Before You Begin E-2

Installing the Phone on Wall Mount Plate E-3

Installing a Wall Mount for the Cisco Unified IP Phone 6911 E-7

Before You Begin E-7

Installing the Bracket E-8

APPENDIX F

Cisco Unified IP Phone Non-Lockable Wall Mount F-1

ADA Non-Lockable Wall Mount Kit for 6900 Series F-1

Components F-2

Before You Begin F-3

Install Non-Lockable Wall Mount Kit for Phone F-3

Remove Phone from Non-Lockable Wall Mount F-6

APPENDIX G

Feature Support by Protocol for the Cisco Unified IP Phone 6901 and 6911 G-1

INDEX



Preface

Overview

Cisco Unified IP Phone 6901 and 6911 Administration Guide for Cisco Unified Communications Manager 8.5 (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 the [“Related Documentation” section on page viii](#).

Audience

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

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

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

Organization

This manual is organized as follows:

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

Chapter 4, “Configuring Settings on the Cisco Unified IP Phone”	Describes how to configure network settings, verify status, and make global changes to the Cisco Unified IP Phone.
Chapter 5, “Configuring Features, Templates, Services, and Users”	Provides an overview of procedures for configuring telephony features, configuring directories, configuring phone button, and adding users to Cisco Unified Communications Manager.
Chapter 6, “Monitoring the Cisco Unified IP Phone 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 7, “Troubleshooting and Maintenance”	Provides tips for troubleshooting the Cisco Unified IP Phone.
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, “Supporting International Users”	Provides information about setting up phones in non-English environments.
Appendix C, “Technical Specifications”	Provides technical specifications of the Cisco Unified IP Phone.
Appendix D, “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.
Appendix E, “Installing the Wall Mount for the Cisco Unified IP Phone 6901 and 6911”	Contains instructions for installing the wall mount for the Cisco Unified IP Phone.
Appendix F, “Cisco Unified IP Phone Non-Lockable Wall Mount”	Contains instructions for installing the Cisco Unified IP Phone Non-Lockable Wall Mount for the Cisco Unified IP Phone 6911.
Appendix G, “Feature Support by Protocol for the Cisco Unified IP Phone 6901 and 6911”	Describes the features supported by each protocol (SCCP and SIP).

Related Documentation

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

Cisco Unified IP Phone 6900 Series

Related publications are available at the following URL:

http://www.cisco.com/en/US/products/ps10326/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>

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

Cisco Product Security Overview

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

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

Document Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[]	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 .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.



Note

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



Caution

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

Warnings use the following convention:



Warning

IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS



CHAPTER 1

An Overview of the Cisco Unified IP Phone

The Cisco Unified IP Phone 6901 and 6911 provide voice communication over an Internet Protocol (IP) network. The Cisco Unified IP Phone functions much like a digital business phone, allowing you to place and receive phone calls. In addition, the phone includes the following:

- The Cisco Unified IP Phone 6901 supports basic features such as hold, redial, transfer, and conference.
- The Cisco Unified IP Phone 6911 supports features such as mute, hold, transfer, conference, speed dial, call forward, and more.

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

This chapter includes the following topics:

- [Understanding the Cisco Unified IP Phone 6901 and 6911, page 1-2](#)
- [What Networking Protocols are Used?, page 1-6](#)
- [What Features are Supported on the Cisco Unified IP Phone 6901 and 6911?, page 1-9](#)
- [Overview of Configuring and Installing Cisco Unified IP Phones, page 1-19](#)
- [Terminology Differences, page 1-24](#)



Caution

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

Understanding the Cisco Unified IP Phone 6901 and 6911



Figure 1-1 shows the main components of the Cisco Unified IP Phone 6901.

Figure 1-1 Cisco Unified IP Phone 6901



Table 1-1 describes the buttons on the Cisco Unified IP Phone 6901.

Table 1-1 Features on the Cisco Unified IP Phone 6901

1	Hookswitch	Activates the features (hookflash) on your phone.
2	Hold button 	Places an active call on hold.
3	Redial button 	Dials the last dialed number.



4	<p>Line button</p> 	<p>Allows users to pick up second incoming call. The line button LED shows call status.</p> <p>The line button enables users to answer an incoming call and swap between two calls on the line. The LED associated with the line button lights up to reflect the line status.</p> <p>The line button illuminates to indicate status:</p> <ul style="list-style-type: none"> • Green, steady—Active call • Green, flashing—Held call • Amber, flashing—Incoming call • Amber, steady—Call Forward All activated • Red, steady—Remote line in use (shared line) • Red, flashing—Remote line on hold
5	<p>Volume button</p> 	<p>Controls the handset and the ringer volume (on-hook).</p>
6	<p>Keypad</p>	<p>Allows you to dial phone numbers, *, and #, and choose menu items (by entering the item number).</p>
7	<p>Handset light strip</p>	<p>Lights up to indicate a ringing call (flashing red) or a new voice message (steady red).</p>




Figure 1-2 shows the main components of the Cisco Unified IP Phone 6911.








Figure 1-2 Cisco Unified IP Phone 6911



Table 1-2 describes the buttons on the Cisco Unified IP Phone 6911.

Table 1-2 Features on the Cisco Unified IP Phone 6911

1	Handset light strip	Lights up to indicate a ringing call (flashing red) or a new voice message (steady red).
2	Phone Template	A paper strip where you can enter names and contact numbers.
3	Transfer button 	Transfers a call.
4	Conference button 	Creates a conference call.
5	Hold button 	Places an active call on hold.

6	<p>Line button</p> 	<p>Allows users to pick up an incoming call. The line button LED shows call status.</p> <p>The line button enables users to answer an incoming call and swap between two calls on the line. The LED associated with the line button lights up to reflect the line status.</p> <p>The line button illuminates to indicate status:</p> <ul style="list-style-type: none"> • Green, steady—Active call • Green, flashing—Held call • Amber, flashing—Incoming call • Amber, steady—Call Forward All activated • Red, steady—Remote line in use (shared line) • Red, flashing—Remote line on hold
7	<p>Speakerphone button</p> 	<p>Selects the speakerphone as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. The speakerphone audio path does not change until a new default audio path is selected (for example, by picking up the handset).</p>
8	<p>Keypad</p>	<p>Allows you to dial phone numbers, *, and #, and choose menu items (by entering the item number).</p>
9	<p>Mute button</p> 	<p>Toggles the microphone on or off. When the microphone is muted, the button is lit red.</p>
10	<p>Volume button</p> 	<p>Controls the handset and speakerphone volume (off-hook) and the ringer volume (on-hook).</p>
11	<p>Messages button</p> 	<p>Auto-dials your voice messaging service (varies by service).</p>
12	<p>Redial</p> 	<p>Dials the last dialed number.</p>
13	<p>Feature button</p> 	<p>Depending on how the phone is set up in Cisco Unified Communications Manager, the programmable feature button provides access to the Speed dialing, Call Forward, Pickup, Group Pickup, and Meet Me features. Users can configure up to nine items on the feature key. The user accesses each of these features by pressing the feature key followed by the number associated with the feature. The number must be pressed within five seconds of pressing the feature key. The number can only be a single digit number from 1-9.</p> <p>These features can be accessed off-hook or on-hook.</p> <ul style="list-style-type: none"> • Call Forward—Allows you to forward a call. • Pickup—Allows you to pickup a call on the third-party phone. • Group Pickup—Allows you to pick up a call within a group. • Meet Me—Allows you to setup a conference. • Speed Dial—Allows you to dial a specific number that has been previously stored.

14	Handset	Phone handset.
----	---------	----------------

What Networking Protocols are Used?

Cisco Unified IP Phones support several industry-standard and Cisco networking protocols required for voice communication. [Table 1-3](#) provides an overview of the networking protocols that the Cisco Unified IP Phone 6901 and 6911 support.

Table 1-3 Supported Networking Protocols on the Cisco Unified IP Phone

Networking Protocol	Purpose	Usage Notes
Cisco Audio Session Tunneling (CAST) (Cisco Unified IP Phone 6911 only)	The CAST protocol allows IP phones and associated applications behind the phone to discover and communicate with the remote endpoints without requiring changes to the traditional signaling components like Cisco Unified Communications Manager and gateways. The CAST protocol allows separate hardware devices to synchronize related media and it allows PC applications to augment non Video capable phones to become video enabled by using the PC as the video resource.	—
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.	The Cisco Unified IP Phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect an IP phone into the network and have the phone become operational without your needing to manually assign an IP address or to configure additional network parameters.	DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each phone locally. Cisco recommends that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, go to the Dynamic Host Configuration Protocol chapter and the Cisco TFTP chapter in the <i>Cisco Unified Communications Manager System Guide</i> . Note If you cannot use option 150, you may try using DHCP option 66.
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 troubleshooting purposes.

Table 1-3 Supported Networking Protocols on the Cisco Unified IP Phone (continued)

Networking Protocol	Purpose	Usage Notes
IEEE 802.1X	<p>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.</p> <p>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.</p>	<p>The Cisco Unified IP Phone implements the IEEE 802.1X standard by providing support for the following authentication methods: EAP-FAST and EAP-TLS.</p> <p>When 802.1X authentication is enabled on the phone, you should disable the voice VLAN. Refer to the “Supporting 802.1X Authentication on Cisco Unified IP Phones” section on page 1-17 for additional information.</p>
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	<p>To communicate using IP, network devices must have an assigned IP address, subnet, and gateway.</p> <p>IP addresses, subnets, and gateways identifications are automatically assigned if you are using the Cisco Unified IP Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally.</p>
Link Layer Discovery Protocol (LLDP) (Cisco Unified IP Phone 6911 only)	LLDP is a standardized network discovery protocol (similar to CDP) that is supported on some Cisco and third-party devices.	The Cisco Unified IP Phone supports LLDP on the switch and PC port.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard developed for voice products.	<p>The Cisco Unified IP Phone supports LLDP-MED on the SW port to communicate information such as:</p> <ul style="list-style-type: none"> • Voice VLAN configuration • Device discovery • Power management • Inventory management <p>For more information about LLDP-MED support, see the <i>LLDP-MED and Cisco Discovery Protocol</i> white paper: http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html</p>
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	Cisco Unified IP Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.
Real-Time Control Protocol (RTCP)	RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round trip delay) on RTP streams.	RTCP is disabled by default, but you can enable it on a per phone basis by using Cisco Unified Communications Manager.

Table 1-3 Supported Networking Protocols on the Cisco Unified IP Phone (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 Phone to use either SIP or Skinny Client Control Protocol (SCCP).
Skinnny Client Control Protocol (SCCP)	SCCP includes a messaging set that allows communications between call control servers and endpoint clients such as IP Phones. SCCP is proprietary to Cisco Systems.	Cisco Unified IP Phone 6901 and 6911 use SCCP, version 20 for call control.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Cisco Unified IP Phones use TCP to connect to Cisco Unified Communications Manager.
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, refer to the <i>Cisco Unified Communications Manager Security Guide</i> .
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the Cisco Unified IP Phone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server. If you want a phone to use a TFTP server other than the one specified by the DHCP server, you must manually assign the IP address of the TFTP server by using the Network Configuration menu on the phone. For more information, go to the Cisco TFTP chapter in the <i>Cisco Unified Communications Manager System Guide</i> .
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	Cisco Unified IP Phones transmit and receive RTP streams, which utilize UDP.

Related Topics

- [Understanding Interactions with Other Cisco Unified IP Telephony Products, page 2-1](#)
- [Understanding the Phone Startup Process, page 2-6](#)

What Features are Supported on the Cisco Unified IP Phone 6901 and 6911?

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

This section includes the following topics:

- [Feature Overview, page 1-9](#)
- [Configuring Telephony Features, page 1-9](#)
- [Configuring Network Parameters Using the Cisco Unified IP Phone, page 1-10](#)
- [Providing Users with Feature Information, page 1-10](#)

Feature Overview

Cisco Unified IP Phones provide traditional telephony functionality, such as call forwarding and transferring, redialing, conference calling, and voice messaging system access. Cisco Unified IP phones also provide a variety of other features. For an overview of the telephony features that the Cisco Unified IP Phone supports and for tips on configuring them, see the [“Telephony Features Available for the Cisco Unified IP Phone” section on page 5-1](#).

As with other network devices, you must configure Cisco Unified IP Phones to prepare them to access Cisco Unified Communications Manager and the rest of the IP network. By using DHCP, you have fewer settings to configure on a phone, but if your network requires it, you can manually configure an IP address, TFTP server, subnet information, and so on. For instructions on configuring the network settings on the Cisco Unified IP Phones, see [Chapter 4, “Configuring Settings on the Cisco Unified IP Phone.”](#)

Finally, because the Cisco Unified IP Phone is a network device, you can obtain detailed status information from it directly. This information can assist you with troubleshooting any problems users might encounter when using their IP phones.

Related Topics

- [Configuring Settings on the Cisco Unified IP Phone, page 4-1](#)
- [Configuring Features, Templates, Services, and Users, page 5-1](#)
- [Troubleshooting and Maintenance, page 7-1](#)

Configuring Telephony Features

You can modify additional settings for the Cisco Unified IP Phone from Cisco Unified Communications Manager Administration. Use Cisco Unified Communications Manager Administration to set up phone registration criteria and calling search spaces, among other tasks. See the [“Telephony Features Available for the Cisco Unified IP Phone” section on page 5-1](#) and the Cisco Unified Communications Manager documentation for additional information.

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

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

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

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

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

Related Topic

- [Telephony Features Available for the Cisco Unified IP Phone, page 5-1](#)

Configuring Network Parameters Using the Cisco Unified IP Phone

You configure parameters such as DHCP, TFTP, and IP settings on the phone itself. For more information about configuring settings and viewing statistics from the phone, see [Chapter 4, “Configuring Settings on the Cisco Unified IP Phone”](#).

Providing Users with Feature Information

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

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

From this site, you can view various user documentation.

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

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 6901 and 6911 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, refer to the *Cisco Unified Communications Manager Security Guide*.

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

Table 1-4 shows where you can find additional information about security in this and other documents.

Table 1-4 Cisco Unified IP Phone and Cisco Unified Communications Manager Security Topics

Topic	Reference
Detailed explanation of security, including set up, configuration, and troubleshooting information for Cisco Unified Communications Manager and Cisco Unified IP Phones	Refer to the <i>Troubleshooting Guide for Cisco Unified Communications Manager</i>
Security features supported on the Cisco Unified IP Phone	See the “ Overview of Supported Security Features ” section on page 1-13
Viewing a security profile name	See the Table 1-5 for an overview of the security features supported by the Cisco Unified IP Phone 6901 and 6911. For more information about these features and about Cisco Unified Communications Manager and Cisco Unified IP Phone security, refer to the <i>Cisco Unified Communications Manager Security Guide</i> .
Identifying phone calls for which security is implemented	See the “ Identifying Authenticated, Encrypted, and Protected Phone Calls ” section on page 1-15
TLS connection	<ul style="list-style-type: none"> • See the “What Networking Protocols are Used?” section on page 1-6 • See the “Adding Phones to the Cisco Unified Communications Manager Database” section on page 2-7
Security and the phone startup process	See the “ Understanding the Phone Startup Process ” section on page 2-6
Security and phone configuration files	See the “ Adding Phones to the Cisco Unified Communications Manager Database ” section on page 2-7
Disabling access to a phone’s web pages	See the “ Disabling and Enabling Web Page Access ” section on page 6-3
Troubleshooting	<ul style="list-style-type: none"> • See the “Troubleshooting and Maintenance” section on page 7-1 • Refer to the <i>Troubleshooting Guide for Cisco Unified Communications Manager</i>
Deleting the CTL file from the phone	See the “ Resetting or Restoring the Cisco Unified IP Phone ” section on page 7-10
Resetting or restoring the phone	See the “ Resetting or Restoring the Cisco Unified IP Phone ” section on page 7-10
802.1X Authentication for Cisco Unified IP Phones	See these sections: <ul style="list-style-type: none"> • “Supporting 802.1X Authentication on Cisco Unified IP Phones” section on page 1-17 • “Troubleshooting and Maintenance” section on page 7-1

Overview of Supported Security Features

Table 1-5 provides an overview of the security features that the Cisco Unified IP Phone 6901 and 6911 support. For more information about these features and about Cisco Unified Communications Manager and Cisco Unified IP Phone security, refer to *Cisco Unified Communications Manager Security Guide*.


Note

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

Table 1-5 Overview of Security Features

Feature	Description
Image authentication	Signed binary files (with the extension .zz.sgn) prevent tampering with the firmware image before it is loaded on a phone. Tampering with the image causes a phone to fail the authentication process and reject the new image.
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). See the “ Configuring Security on the Cisco Unified IP Phone ” section on page 3-10 for more information.
Device authentication	Occurs between the Cisco Unified Communications Manager server and the phone when each entity accepts the certificate of the other entity. Determines whether a secure connection between the phone and a Cisco Unified Communications Manager should occur; and, if necessary, creates a secure signaling path between the entities by using TLS protocol. Cisco Unified Communications Manager will not register phones unless they can be authenticated by the Cisco Unified Communications Manager.
File authentication	Validates digitally signed files that the phone downloads. The phone validates the signature to make sure that file tampering did not occur after the file creation. Files that fail authentication are not written to Flash memory on the phone. The phone rejects such files without further processing.
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.

Table 1-5 Overview of Security Features (continued)

Feature	Description
Secure SRST reference	<p>After you configure a SRST reference for security and then reset the dependent devices in Cisco Unified Communications Manager Administration, the TFTP server adds the SRST certificate to the phone configuration file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router.</p> <p>The configuration file is with one of the following extensions:</p> <ul style="list-style-type: none"> • .cnf.xml • .cnf.xml.sgn • .cnf.xml.enc.sgn
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 the “Understanding Security Profiles” section on 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.
Phone hardening	<p>Additional security option, which you control from Cisco Unified Communications Manager Administration:</p> <ul style="list-style-type: none"> • Disabling access to web pages for a phone
802.1X Authentication	The Cisco Unified IP Phone can use 802.1X authentication to request and gain access to the network. See the “Supporting 802.1X Authentication on Cisco Unified IP Phones” section on page 1-17 for more information.
Voice Quality Metrics	
MOS LQK	<p>Objective estimate of the Mean Opinion Score (MOS) for Listening Quality (LQK) that ranks audio quality from 5 (excellent) to 1 (bad). This score is based on audible-concealment events due to a frame loss in the preceding 8 seconds of the voice stream.</p> <p>Note The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.</p>
Avg MOS LQK	Average MOS LQK score for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score from the start of the voice stream.

Table 1-5 Overview of Security Features (continued)

Feature	Description
Max MOS LQK	<p>Baseline or highest MOS LQK score from the start of the voice stream.</p> <p>The following codecs provide the corresponding maximum MOS LQK scores under normal conditions with no frame loss:</p> <ul style="list-style-type: none"> • G.711: 4.5 • G.728/iLBC: 3.9 • G729A/AB: 3.7
MOS LQK Version	Version of the Cisco-proprietary algorithm used to calculate the MOS LQK scores.

Related Topics

- [Understanding Security Features for Cisco Unified IP Phones, page 1-10](#)
- [Identifying Authenticated, Encrypted, and Protected Phone Calls, page 1-15](#)

Understanding Security Profiles

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

To view the security mode that is set for the phone, you can view the security profile in Cisco Unified Communications Manager Administration.

Related Topics

- [Identifying Authenticated, Encrypted, and Protected Phone Calls, page 1-15](#)

Identifying Authenticated, Encrypted, and Protected Phone Calls

In an authenticated call, all devices participating in the establishment of the call are trusted devices, and authenticated by Cisco Unified Communications Manager.

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.

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.

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 calling and shared lines are not available when protected calling is configured. Protected calls are not authenticated.

Related Topic

- [Understanding Security Features for Cisco Unified IP Phones, page 1-10](#)
- [Understanding Security Features for Cisco Unified IP Phones, page 1-10](#)

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 are not supported.

A protected call is established using this process:

1. A user initiates the call from a protected phone (protected security mode).
2. 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 is not played.

**Note**

Protected calling is supported for conversations between two phones. Some features, such as conference calling and shared 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 also security in the system.

[Table 1-6](#) provides information about changes to call security levels when using Barge for Cisco Unified IP Phone 6901 and 6911.

Table 1-6 Call Security Interactions When Using Barge (Cisco Unified IP Phone 6911 only)

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

[Table 1-7](#) 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 1-7 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	Non-secure conference
Secure (encrypted)	Conference	All participants are encrypted	Secure encrypted level conference
Secure (authenticated)	Conference	All participants are encrypted or authenticated	Secure authenticated level conference
Non-secure	cBarge	All participants are encrypted	Conference changes to non-secure
Non-secure	Meet Me	Minimum security level is encrypted	Initiator receives message "Does not meet Security Level", call rejected.
Secure (encrypted)	Meet Me	Minimum security level is authenticated	Conference accepts encrypted and authenticated calls
Secure (encrypted)	Meet Me	Minimum security level is non-secure	Only secure conference bridge available and used Conference accepts all calls

Supporting 802.1X Authentication on Cisco Unified IP Phones

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

- [Overview, page 1-17](#)
- [Required Network Components, page 1-18](#)
- [Best Practices—Requirements and Recommendations, page 1-19](#)

Overview

Cisco Unified IP phones and Cisco Catalyst switches have traditionally used Cisco Discovery Protocol (CDP) to identify each other and determine parameters such as VLAN allocation and inline power requirements. However, CDP is not used to identify any locally attached PCs; therefore, Cisco Unified IP Phones provide an EAPOL pass-through mechanism, whereby a PC locally attached to the IP phone, may pass through EAPOL messages to the 802.1X authenticator in the LAN switch. This prevents the IP phone from having to act as the authenticator, yet allows the LAN switch to authenticate a data 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 is disconnected from the IP phone, the LAN switch would not see the physical link fail, because the link between the LAN switch and the IP phone is maintained. To avoid compromising network integrity, the IP phone sends an EAPOL-Logoff message to the switch, on behalf of the downstream PC, which triggers the LAN switch to clear the authentication entry for the downstream PC.

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

Required Network Components

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

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

Best Practices—Requirements and Recommendations

- Enable 802.1X Authentication—If you want to use the 802.1X standard to authenticate Cisco Unified IP Phones, be sure that you have properly configured the other components before enabling it on the phone.
- Configure PC Port—The 802.1X standard does not take into account the use of VLANs and thus recommends that only a single device should be authenticated to a specific switch port. However, some switches (including Cisco Catalyst switches) support multi-domain authentication. The switch configuration determines whether you can connect a PC to the phone's PC port.



Note Only Cisco Unified IP Phone 6911 has PC ports.

- Enabled—If you are using a switch that supports multi-domain authentication, you can enable the PC port and connect a PC to it. In this case, Cisco Unified IP Phones support proxy EAPOL-Logoff to monitor the authentication exchanges between the switch and the attached PC. For more information about IEEE 802.1X support on the Cisco Catalyst switches, refer to the Cisco Catalyst switch configuration guides at:
http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
- Disabled—If the switch does not support multiple 802.1X-compliant devices on the same port, you should disable the PC Port when 802.1X authentication is enabled. 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.

Overview of Configuring and Installing Cisco Unified IP Phones

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

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

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

- [Configuring Cisco Unified IP Phones in Cisco Unified Communications Manager, page 1-20](#)
- [Installing Cisco Unified IP Phones, page 1-23](#)

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—Not supported if Cisco Unified Communications Manager is operating in mixed mode.
- Cisco Unified Communications Manager Administration
- Bulk Administration Tool (BAT)
- BAT and the Tool for Auto-Registered Phones Support (TAPS)

For more information about these choices, see the [“Adding Phones to the Cisco Unified Communications Manager Database”](#) section on page 2-7.

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

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

Checklist for Configuring the Cisco Unified IP Phone 6901 and 6911 in Cisco Unified Communications Manager

Table 1-8 provides an overview and checklist of configuration tasks for the Cisco Unified IP Phone 6901 and 6911 in Cisco Unified Communications Manager Administration. The list presents a suggested order to guide you through the phone configuration process. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, refer to the sources in the list.

Table 1-8 Checklist for Configuring the Cisco Unified IP Phone 6901 and 6911 in Cisco Unified Communications Manager

Task	Purpose	For More Information
1.	<p>Gather the following information about the phone:</p> <ul style="list-style-type: none"> • Phone Model • MAC address • Physical location of the phone • Name or user ID of phone user • Device pool • Partition, calling search space, and location information • Associated directory number (DN) to assign to the phone • Cisco Unified Communications Manager user to associate with the phone <p>Provides list of configuration requirements for setting up phones.</p>	<p>For more information, go to the “Cisco Unified IP Phones” chapter in the <i>Cisco Unified Communications Manager System Guide</i>.</p> <p>See the “Telephony Features Available for the Cisco Unified IP Phone” section on page 5-1.</p>
2.	<p>Verify that you have sufficient unit licenses for your phone.</p>	<p>For more information, go to the License Unit Report chapter in the <i>Cisco Communications Manager Administration Guide</i>.</p>
3.	<p>Add and configure the phone by completing the required fields in the Phone Configuration window. Required fields are indicated by an asterisk (*) next to the field name; for example, MAC address and device pool.</p> <p>The device with its default settings gets added to the Cisco Unified Communications Manager database.</p>	<p>For more information, go to the Cisco Unified IP Phone Configuration chapter in the <i>Cisco Communications Manager Administration Guide</i>.</p> <p>For information about Product Specific Configuration fields, refer to “?” Button Help in the Phone Configuration window.</p> <p>Note If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, go to the User/Phone Add Configuration chapter in the <i>Cisco Communications Manager Administration Guide</i>.</p>

Table 1-8 Checklist for Configuring the Cisco Unified IP Phone 6901 and 6911 in Cisco Unified Communications Manager (continued)

Task	Purpose	For More Information
4.	Add and configure directory numbers (line) 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.	For more information, go to the “Directory Number Configuration” chapter in the <i>Cisco Unified Communications Manager Administration Guide</i> . See the “Telephony Features Available for the Cisco Unified IP Phone” section on page 5-1.
5.	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 accessing the Network Menu via the IVR). Adds user information to the global directory for Cisco Unified Communications Manager.	For more information, go to the End User Configuration chapter in the <i>Cisco Unified Communications Manager Administration Guide</i> . See the “Adding Users to Cisco Unified Communications Manager” section on page 5-8. Note If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, go to the User/Phone Add Configurations chapter in the <i>Cisco Unified Communications Manager Administration Guide</i> .
6.	Associate a user to a user group. Assigns users a common list of roles and permissions that apply to all users in a user group. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users. Note In order for end users to access Cisco Unified CM User Options, you must add users to the standard Cisco CCM End Users group.	Refer to the following sections in the <i>Cisco Unified Communications Manager Administration Guide</i> : <ul style="list-style-type: none"> • “End User Configuration Settings” section in the “End User Configuration” chapter. • “Adding Users to a User Group” section in the “User Group Configuration” chapter.
7.	Associate a user with a phone (optional). Provides users with control over their phone such a forwarding calls or adding speed-dial numbers or services. Note Some phones, such as those in conference rooms, do not have an associated user.	For more information, go to the “Associating Devices to an End User” section in the End User Configuration chapter in the <i>Cisco Unified Communications Manager Administration Guide</i> .

Installing Cisco Unified IP Phones

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



Note

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

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

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

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

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

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

Checklist for Installing the Cisco Unified IP Phone 6901 and 6911

Table 1-9 provides an overview and checklist of installation tasks for the Cisco Unified IP Phone 6901 and 6911. The list presents a suggested order to guide you through the phone installation. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, refer to the sources in the list.

Table 1-9 Installation Checklist for the Cisco Unified IP Phone 6901 and 6911

Task	Purpose	For More Information
1.	Choose the power source for the phone: <ul style="list-style-type: none"> • Power over Ethernet (PoE) • External power supply Determines how the phone receives power.	See the “ Providing Power to the Cisco Unified IP Phone ” section on page 2-3.
2.	Assemble the phone, adjust phone placement, and connect the network cable. Locates and installs the phone in the network.	See the “ Installing the Cisco Unified IP Phone ” section on page 3-4. See the “ Footstand ” section on page 3-7.
3.	Monitor the phone startup process. Associates directory numbers to the phone. Verifies that phone is configured properly.	See the “ Verifying the Phone Startup Process ” section on page 3-9.

Table 1-9 Installation Checklist for the Cisco Unified IP Phone 6901 and 6911 (continued)

Task	Purpose	For More Information
4.	<p>If you are configuring the network settings on the phone, you can set up an IP address for the phone by either using DHCP or manually entering an IP address.</p> <p>Using DHCP—Verify that DHCP is enabled with the IVR. You can set an alternate TFTP by entering the IP address for the TFTP when prompted by the IVR.</p> <p>Note Consult with the network administrator to determine whether you need to assign an alternative TFTP server instead of using the TFTP server assigned by DHCP.</p> <p>Without DHCP—Verify that DHCP is disabled with the IVR. You must then configure the IP address, subnet mask, TFTP server, and default router locally by using the phone’s IVR.</p>	<p>See the “Configuring Startup Network Settings” section on page 3-9.</p> <p>See the “Configuring Settings on the Cisco Unified IP Phone” section on page 4-1.</p>
5.	<p>Set up security on the phone.</p> <p>Provides protection against data tampering threats and identity theft of phones.</p>	See the “ Configuring Security on the Cisco Unified IP Phone ” section on page 3-10.
6.	<p>Make calls with the Cisco Unified IP Phone.</p> <p>Verifies that the phone and features work correctly.</p>	Refer to <i>Cisco Unified IP Phone 6901 and 6911 User Guide</i> for more information.
7.	<p>Provide information to end users about how to use their phones and how to configure their phone options.</p> <p>Ensures that users have adequate information to successfully use their Cisco Unified IP Phones.</p>	See Appendix A, “Providing Information to Users Via a Website.”

Terminology Differences

[Table 1-10](#) highlights some of the important differences in terminology that is used in these documents:

- *Cisco Unified IP Phone 6901 and 6911 User Guide for Cisco Unified Communications Manager 8.5 (SCCP)*
- *Cisco Unified IP Phone 6901 and 6911 Administration Guide for Cisco Unified Communications Manager 8.5 (SCCP)*
- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager System Guide*

Table 1-10 Terminology Differences

User Guide	Administration and System Guides
Auto Barge	cBarge
Message Indicators	Message Waiting Indicator (MWI) or Message Waiting Lamp
Voicemail System	Voice Messaging System



CHAPTER 2

Preparing to Install the Cisco Unified IP Phone on Your Network

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

This chapter focuses on the interactions between the Cisco Unified IP Phone 6901 and 6911 and Cisco Unified Communications Manager, DNS and DHCP servers, TFTP servers, and switches. It also describes options for powering phones.

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

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

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

- [Understanding Interactions with Other Cisco Unified IP Telephony Products, page 2-1](#)
- [Providing Power to the Cisco Unified IP Phone, page 2-3](#)
- [Understanding Phone Configuration Files, page 2-5](#)
- [Understanding the Phone Startup Process, page 2-6](#)
- [Adding Phones to the Cisco Unified Communications Manager Database, page 2-7](#)
- [Using Cisco Unified IP Phones with Different Protocols, page 2-11](#)
- [Determining the MAC Address for a Cisco Unified IP Phone, page 2-12](#)

Understanding Interactions with Other Cisco Unified IP Telephony Products

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

This section includes the following topics:

- [Understanding How the Cisco Unified IP Phone Interacts with Cisco Unified Communications Manager, page 2-2](#)
- [Understanding How the Cisco Unified IP Phone 6911 Interacts with the VLAN, page 2-2](#)

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

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

- Firmware for phones
- Configuration file via TFTP service
- Phone registration
- Call preservation, so that a media session continues if signaling is lost between the primary Communications Manager and a phone

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

For an overview of security functionality for the Cisco Unified IP Phone, see the “[Understanding Security Features for Cisco Unified IP Phones](#)” section on page 1-10.



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

For more information, refer to “Software Upgrades” chapter in the *Cisco Unified Communications Operating System Administration Guide*.

Related Topic

- [Telephony Features Available for the Cisco Unified IP Phone, page 5-1](#)

Understanding How the Cisco Unified IP Phone 6911 Interacts with the VLAN

The Cisco Unified IP Phone 6911 has 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.



Note

Cisco Unified IP Phone 6901 does not support PC port.

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

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

- Data traffic present on the VLAN supporting phones might reduce the quality of Voice-over-IP traffic.
- Network security may indicate a need to isolate the VLAN voice traffic from the VLAN data traffic.

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

- Voice traffic to and from the IP phone (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 IP phone (native VLAN)

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

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

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

Related Topics

- [Understanding the Phone Startup Process, page 2-6](#)
- [Configuring Settings on the Cisco Unified IP Phone, page 4-1](#)

Providing Power to the Cisco Unified IP Phone

The Cisco Unified IP Phone 6901 and 6911 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 Phone 6901 and 6911.

Table 2-1 Guidelines for Powering the Cisco Unified IP Phone 6901 and 6911

Power Type	Guidelines
External power—Provided through the CP-PWR-CUBE-3 external power supply.	The Cisco Unified IP Phone 6901 and 6911 use the CP-PWR-CUBE-3 power supply.
External power—Provided through the Cisco Unified IP Phone Power Injector.	The Cisco Unified IP Phone Power Injector may be used with any Cisco Unified IP Phone. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco Unified IP Phone Power Injector is connected between a switch port and the IP Phone, and supports a maximum cable length of 100m between the unpowered switch and the IP Phone.
PoE power—Provided by a switch through the Ethernet cable attached to the phone.	<ul style="list-style-type: none"> • The Cisco Unified IP Phone 6901 and 6911 support Cisco inline PoE. • The Cisco Unified IP Phone 6901 and 6911 support IEEE 802.3af Class 1 power on signal pairs and spare pairs. • To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply. • Make sure that the CatOS or IOS version running on your switch supports your intended phone deployment. Refer to the documentation for your switch for operating system version information.
External power—Provided through inline power patch panel WS-PWR-PANEL	The inline power patch panel WS-PWR-PANEL is compatible with the Cisco Unified IP Phone 6901 and 6911.

Power Outage

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

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 Phone 6901 and 6911
- The Cisco IOS releases that support bidirectional power negotiation
- Other requirements and restrictions regarding power

Table 2-2 *Related Documentation for Power*

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

Understanding Phone Configuration Files

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

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

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



Note

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

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file will contain sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For detailed information, refer to the “[Configuring Encrypted Phone Configuration Files](#)” chapter in *Cisco Unified Communications Manager Security Guide*. 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` from the TFTP server when the following conditions exist:

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

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

If the phone is registered and working in encrypted mode, the phone accesses the configuration file named SEPmac_address.cnf.xml.enc.sgn. If the SEPmac_address.cnf.xml.enc.sgn does not exist on the TFTP server, the phone requests for the file SEPmac_address.cnf.xml.sgn. That is, if phone works in encrypted mode with TFTP Encrypted Config selected, the phone accesses the configuration file named SEPMac_addr.cnf.xml.enc.sgn if it is not chosen, SEPMac_addr.cnf.xml.sgn is chosen. To enable TFTP Encrypted Configuration, select the **TFTP Encrypted Config** check box Phone Security Profile Configuration page. You can access this page from the Cisco Unified CM Administration UI by selecting **System > Security > Phone Security Profile** and then clicking **Add New**.

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

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

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 on phone configuration settings, go to the [Cisco Unified IP Phone Configuration](#) chapter in the *Cisco Communications Manager Administration Guide*.

Understanding the Phone Startup Process

When connecting to the VoIP network, the Cisco Unified IP Phone 6901 and 6911 go through a standard startup process that is described in [Table 2-3](#). Depending on your specific network configuration, not all of these steps may occur on your Cisco Unified IP Phone.

Table 2-3 Cisco Unified IP Phone Startup Process

Task	Purpose	Related Topics
1.	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.	<ul style="list-style-type: none"> • Adding Phones to the Cisco Unified Communications Manager Database, page 2-7. • Resolving Startup Problems, page 7-1.
2.	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.	<ul style="list-style-type: none"> • Configuring Settings on the Cisco Unified IP Phone, page 4-1. • Resolving Startup Problems, page 7-1.

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

Task	Purpose	Related Topics
3.	<p>Obtaining an IP Address</p> <p>If the Cisco Unified IP Phone is using DHCP to obtain an IP address, the phone queries the DHCP server to obtain one. If you are not using DHCP in your network, you must assign static IP addresses to each phone locally.</p>	<ul style="list-style-type: none"> • Configuring Settings on the Cisco Unified IP Phone, page 4-1. • Resolving Startup Problems, page 7-1.
4.	<p>Accessing a TFTP Server</p> <p>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.</p> <p>Note You can also assign an alternative TFTP server to use instead of the one assigned by DHCP.</p>	<ul style="list-style-type: none"> • Configuring Settings on the Cisco Unified IP Phone, page 4-1. • Resolving Startup Problems, page 7-1.
5.	<p>Requesting the Configuration File</p> <p>The TFTP server has configuration files, which define parameters for connecting to Cisco Unified Communications Manager and other information for the phone.</p>	<ul style="list-style-type: none"> • Adding Phones to the Cisco Unified Communications Manager Database, page 2-7. • Resolving Startup Problems, page 7-1.
6.	<p>Loading the Stored Phone Image</p> <p>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.</p>	Resolving Startup Problems , page 7-1.
7.	<p>Contacting Cisco Unified Communications Manager</p> <p>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.</p> <p>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.</p>	Resolving Startup Problems , page 7-1.

Adding Phones to the Cisco Unified Communications Manager Database

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

These sections describe the methods:

- [Adding Phones with Auto-Registration, page 2-8](#)
- [Adding Phones with Auto-Registration and TAPS, page 2-9](#)
- [Adding Phones with Cisco Unified Communications Manager Administration, page 2-10](#)
- [Adding Phones Using the BAT Phone Template, page 2-10](#)

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	<ul style="list-style-type: none"> • 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

Cisco recommends you use auto-registration to add less than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT). See the [“Adding Phones Using the BAT Phone Template”](#) section on page 2-10.

Auto-registration is disabled by default. In some cases, you might not want to use auto-registration; for example, if you want to assign a specific directory number to the phone. For information about enabling auto-registration, go to the “[Enabling Auto-Registration](#)” section 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 automatically enabled.

Related Topics

- [Adding Phones with Auto-Registration and TAPS, page 2-9](#)
- [Adding Phones with Cisco Unified Communications Manager Administration, page 2-10](#)
- [Adding Phones Using the BAT Phone Template, page 2-10](#)

Adding Phones with Auto-Registration and TAPS

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

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

**Note**

Cisco recommends you use auto-registration and TAPS to add less than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT). See the “[Adding Phones Using the BAT Phone Template](#)” section on page 2-10.

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

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

**Note**

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

For more information, go to the “[Bulk Administration](#)” chapter in *Cisco Unified Communications Manager Administration Guide*.

Related Topics

- [Adding Phones with Auto-Registration, page 2-8](#)
- [Adding Phones with Cisco Unified Communications Manager Administration, page 2-10](#)
- [Adding Phones Using the BAT Phone Template, page 2-10](#)

Adding Phones with Cisco Unified Communications Manager Administration

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

For information about determining a MAC address, see the [“Using Cisco Unified IP Phones with Different Protocols” section on page 2-11](#).

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

For complete instructions and conceptual information about Cisco Unified Communications Manager, go to the [“Cisco Unified Communications Manager Overview” chapter in the *Cisco Unified Communications Manager System Guide*](#).

Related Topics

- [Adding Phones with Auto-Registration, page 2-8](#)
- [Adding Phones with Auto-Registration and TAPS, page 2-9](#)
- [Adding Phones Using the BAT Phone Template, page 2-10](#)

Adding Phones Using the BAT Phone Template

The Cisco Unified Communications Manager Bulk Administration Tool (BAT) enables you to perform batch operations, including registration, on multiple phones. To access BAT, choose **Bulk Administration** in Cisco Unified Communications Manager Administration,

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

For information about determining a MAC address, see the [“Using Cisco Unified IP Phones with Different Protocols” section on page 2-11](#).

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

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

Procedure

-
- Step 1** From Cisco Unified Communications Manager, choose **Bulk Administration > Phones > Phone Template**.
 - Step 2** Click **Add New**.
 - Step 3** Choose a Phone Type and click **Next**.
 - Step 4** Enter the details of phone specific parameters like Device Pool, Phone Button Template, Device Security Profile and so on.
 - Step 5** Click **Save**.
 - Step 6** From Cisco Unified Communications Manager, choose **Device > Phone > Add New** to add a phone using an existing BAT phone template.
-

Related Topics

- [Adding Phones with Auto-Registration, page 2-8](#)
- [Adding Phones with Auto-Registration and TAPS, page 2-9](#)
- [Adding Phones with Cisco Unified Communications Manager Administration, page 2-10](#)

Using Cisco Unified IP Phones with Different Protocols

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

This section includes these topics:

- [Converting a New Phone from SCCP to SIP, page 2-11](#)
- [Converting an In-Use Phone from One Protocol to the Other Protocol, page 2-11](#)
- [Deploying a Phone in an SCCP and SIP Environment, page 2-12](#)

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 parameter in Cisco Unified Communications Manager Administration to SIP.
 - To provision the phone using the Bulk Administration Tool (BAT), choose the appropriate phone model and choose SIP from the BAT.
 - To provision the phone manually, make the appropriate changes for SIP on the Phone configuration window in Cisco Unified Communications Manager Administration.
- Refer to *Cisco Unified Communications Manager Administration Guide* for detailed information about Cisco Unified Communications Manager configuration.
- Refer to *Cisco Unified Communications Manager Bulk Administration Guide* for detailed information about using the BAT.
- Step 2** If you are not using DHCP in your network, configure the network parameters for the phone. See [Configuring Startup Network Settings, page 3-9](#).
- Step 3** Save the configuration updates, click **Apply Config**, click **OK** when the Apply Configuration Information dialog displays, then have the user power cycle the phone.
-

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

If Cisco Unified IP phones presently connected to Cisco Unified CM are using the SCCP protocol to receive and place calls and you now want some or all of these phones to use the SIP protocol, the phone firmware for each phone type must be upgraded from SCCP to the recommended SIP version before the

phones can register. If Cisco Unified IP phones to be connected to Cisco Unified CM are brand new, out-of-the-box, the SCCP phone firmware preloaded at the factory must be upgraded to the recommended SIP version before your SIP phones can complete registration.

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

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:

Procedure

- Step 1** Set the Cisco Unified Communications Manager `auto_registration_protocol` parameter to SCCP. From Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.
- Step 2** Install the phones.
- Step 3** Change the Auto Registration Protocol enterprise parameter to SIP.
- Step 4** Auto-register the SIP phones.

Determining the MAC Address for a Cisco Unified IP Phone

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

- Look at the MAC label on the back of the phone.
- Display the web page for the phone and click the **Device Information** hyperlink.
For information about accessing the web page, see the [“Accessing the Web Page for a Phone” section on page 6-2](#).



CHAPTER 3

Setting Up the Cisco Unified IP Phone

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

- [Before You Begin, page 3-1](#)
- [Understanding the Cisco Unified IP Phone 6901 and 6911 Components, page 3-2](#)
- [Installing the Cisco Unified IP Phone, page 3-4](#)
- [Footstand, page 3-7](#)
- [Verifying the Phone Startup Process, page 3-9](#)
- [Configuring Startup Network Settings, page 3-9](#)



Note

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

Before You Begin

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

- [Network Requirements, page 3-1](#)
- [Cisco Unified Communications Manager Configuration, page 3-2](#)

Network Requirements

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

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

Cisco Unified Communications Manager Configuration

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

If you plan to use auto-registration, verify that it is enabled and properly configured in Cisco Unified Communications Manager Administration before connecting any Cisco Unified IP Phone to the network. For information about enabling and configuring auto-registration, refer to *Cisco Unified Communications Manager Administration Guide*. Also, see the “[Adding Phones to the Cisco Unified Communications Manager Database](#)” section on page 2-7.

You must use Cisco Unified Communications Manager Administration to configure and assign telephony features to the Cisco Unified IP Phones. See the “[Telephony Features Available for the Cisco Unified IP Phone](#)” section on page 5-1 for details.

In Cisco Unified Communications Manager Administration, you can add users to the database, add users to user groups, and associate users to specific phones. In this way, users gain access their Cisco Unified CM User Option page to configure items such as call forwarding, speed dialing, and voice messaging system options. See the “[Adding Users to Cisco Unified Communications Manager](#)” section on page 5-8 for details.

Understanding the Cisco Unified IP Phone 6901 and 6911 Components

The Cisco Unified IP Phone 6901 and 6911 include these components on the phone or as accessories for the phone:

- [Network and Access Ports](#), page 3-2
- [Handset](#), page 3-3
- [Speakerphone \(Cisco Unified IP Phone 6911 Only\)](#), page 3-3

Network and Access Ports

The back of the Cisco Unified IP Phone 6901 includes a network port, which the phone uses to connect to the network. The port supports 10/100 Mbps half- or full-duplex connections to external devices. You can use either Category 3/5/5e cabling for 10-Mbps connections, but you must use Category 5/5e for 100 Mbps connections.

The back of the Cisco Unified IP Phone 6911 includes these ports:

- Network port—Labeled Network.
- Access port—Labeled Computer.

**Note**

Only the Cisco Unified IP Phone 6911 has a PC port. The Cisco Unified IP Phone 6901 does not have a PC port.

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

Use the network port to connect the phone to the network. You must use a straight-through cable on this port. The phone can also obtain inline power from a switch over this connection. See the [“Adding Phones to the Cisco Unified Communications Manager Database” section on page 2-7](#) 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 handset is designed especially for use with a Cisco Unified IP Phone. It includes a light strip that indicates incoming calls and voice messages waiting.

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

Speakerphone (Cisco Unified IP Phone 6911 Only)

By default, the 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.

Installing the Cisco Unified IP Phone

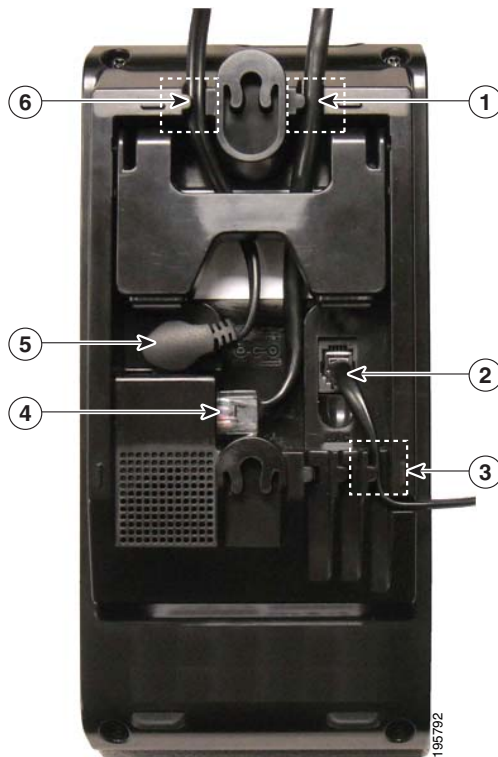
You must connect the Cisco Unified IP Phone to the network and to a power source before using it. See [Figure 3-1](#) for a graphical representation of the connections for a Cisco Unified IP Phone 6901 and [Figure 3-2](#) for a graphical representation of the connections for a Cisco Unified IP Phone 6911.

To install a Cisco Unified IP Phone, perform the tasks described in [Table 3-1](#).

Table 3-1 *Installing the Cisco Unified IP Phone 6901 and 6911*

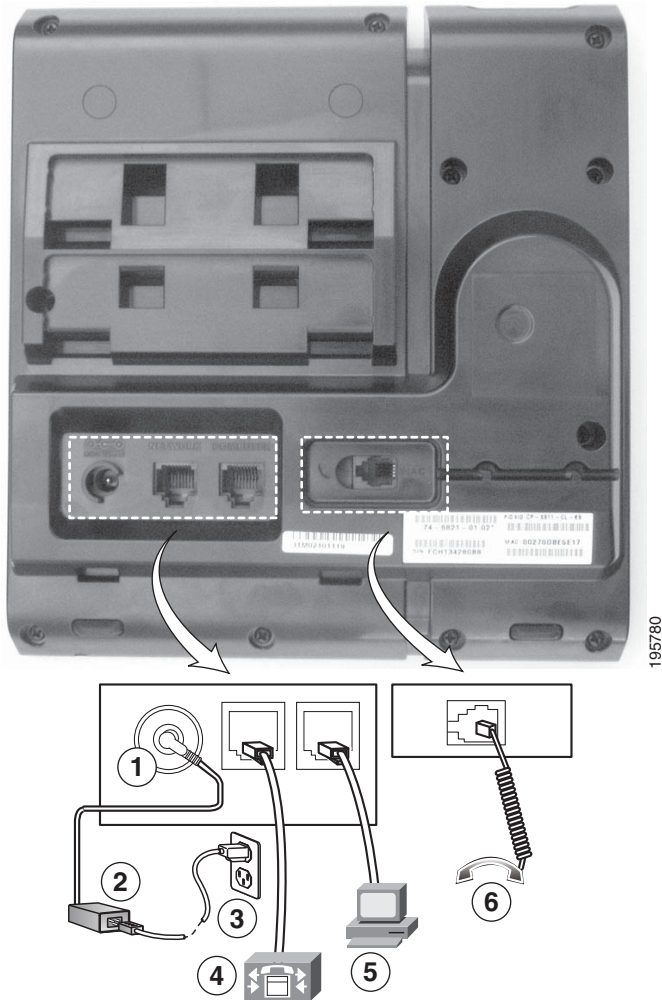
Task	Purpose	Related Topics
1.	Connect the handset to the Handset port.	—
2.	Optional. Connect the power supply to the Cisco DC Adapter port.	See the “Adding Phones to the Cisco Unified Communications Manager Database” section on page 2-7 for guidelines.
3.	<p>Connect a straight-through Ethernet cable from the switch to the network port labeled Network on the Cisco Unified IP Phone 6901 and 6911.</p> <p>Each Cisco Unified IP Phone ships with one Ethernet cable in the box.</p> <p>You can use either Category 3/5/5e cabling for 10-Mbps connections, but you must use Category 5/5e for 100 Mbps connections.</p>	See the “Network and Access Ports” section on page 3-2 for guidelines.
4.	<p>(Cisco Unified IP Phone 6911)</p> <p>Connect a straight-through Ethernet cable from another network device, such as a desktop computer, to the access port labeled Computer.</p> <p>Optional. You can connect another network device later if you do not connect one now.</p> <p>You can use either Category 3/5/5e cabling for 10-Mbps connections, but you must use Category 5/5e for 100 Mbps connections.</p>	See the “Network and Access Ports” section on page 3-2 for guidelines.

Figure 3-1 Cisco Unified IP Phone 6901 Cable Connections



1	Slot for Ethernet cable	4	Network port (10/100 SW) connection IEEE 802.3af power enabled
2	Handset connection	5	DC adaptor port (DC48V)
3	Slot for handset cable	6	Slot for DC adaptor cable

Figure 3-2 Cisco Unified IP Phone 6911 Cable Connections



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

Related Topics

- [Footstand, page 3-7](#)
- [Verifying the Phone Startup Process, page 3-9](#)
- [Configuring Startup Network Settings, page 3-9](#)

Footstand

The Cisco Unified IP Phone 6901 has a foldable footstand. When the footstand is unfolded, it gives the phone an elevated viewing angle.

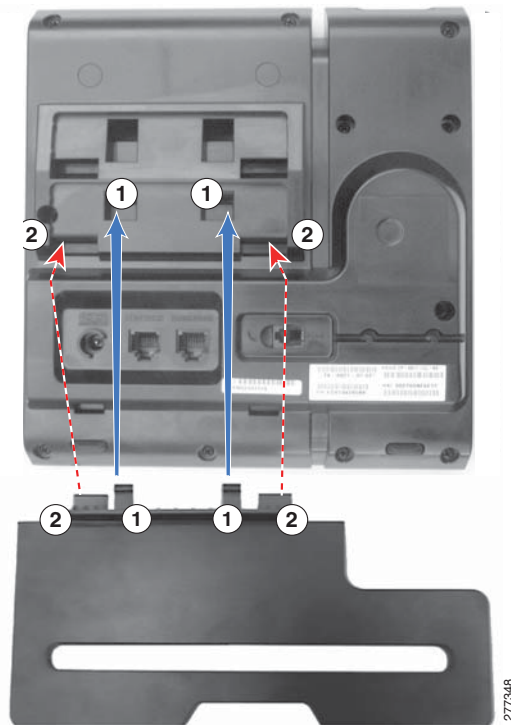
Figure 3-3 illustrates the footstand on the Cisco Unified IP Phone 6901.

Figure 3-3 Cisco Unified IP Phone 6901



Figure 3-4 illustrates attaching the footstand at a higher angle on the Cisco Unified IP Phone 6911.

Figure 3-4 Cisco Unified IP Phone 6911



- | | | | |
|----------|--|----------|---|
| 1 | Insert the connectors into the lower slots | 2 | Lift the footstand until the connectors snap into the upper slots |
|----------|--|----------|---|

Higher Viewing Angle

Connect the footstand to the lower slots for a higher viewing angle.



Lower Viewing Angle

Connect the footstand to the upper slots for a higher viewing angle.



Mounting the Phone to the Wall

You can mount the Cisco Unified IP Phone 6901 on the wall by using a standard telephone wall plate with an opening for an RJ-45 connector. Cisco recommends that you use Leviton Wall Mount plate (Leviton type number: 4108W-0SP) to wall mount the Cisco Unified IP Phone 6901. For information on installing the wall mount kit for Cisco Unified IP Phone 6901, see [Appendix E, “Installing the Wall Mount for the Cisco Unified IP Phone 6901 and 6911.”](#)

You can mount the Cisco Unified IP Phone 6911 on the wall by using special brackets available in a Cisco Unified IP Phone wall mount kit. For information on installing the wall mount kit, see [Appendix E, “Installing the Wall Mount for the Cisco Unified IP Phone 6901 and 6911”](#) or [Appendix F, “Cisco Unified IP Phone Non-Lockable Wall Mount.”](#)

**Note**

Wall mount kits are not included with the phone and must be ordered separately.

Verifying the Phone Startup Process

The LEDs on the MWI on the handset, and the LEDs on the Mute button light up during bootup. Upon successful completion of the bootup process, the LEDs turn off, and the phone is ready for calls. If the phone successfully boots up, it has started up properly. If the phone does not start up properly, the user receives a reorder tone. For more information, see the [“Resolving Startup Problems”](#) section on [page 7-1](#).

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
- Default Router
- TFTP server IP address

Collect this information and see the instructions in [Chapter 4, “Configuring Settings on the Cisco Unified IP Phone.”](#)

Configuring Security on the Cisco Unified IP Phone

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

For more information about the security features, see the [“Understanding Security Features for Cisco Unified IP Phones” section on page 1-10](#). Also, refer to *Cisco Unified Communications Manager Security Guide*.

You can initiate the installation of an 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 file should have a CAPF certificate.
- On Cisco Unified Communications Operating System Administration, verify that the CAPF certificate has been installed
- The CAPF is running and configured.

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

Related Topic

- [Understanding Security Features for Cisco Unified IP Phones, page 1-10](#)



CHAPTER 4

Configuring Settings on the Cisco Unified IP Phone

The Cisco Unified IP Phone includes configurable network settings that you may need to modify before the phone is functional for your users. You can access, view, and change the network settings on the phone by accessing the Interactive Voice Response (IVR). Other configuration settings may be configured in Cisco Unified Communications Manager Administration

This chapter includes the following topics:

- [Configuring Settings on the Cisco Unified IP Phone, page 4-1](#)
- [Accessing the Phone Configuration Settings, page 4-2](#)

Configuring Settings on the Cisco Unified IP Phone

Before the Cisco Unified IP Phone can function, you must configure the network setting on the phone. You can review the phone's configuration settings by using the phone's IVR. When the phone is connected to a network with a DHCP server, you can use the DHCP server to configure the network settings. You can also manually configure the phone by accessing the IVR.

Phone Settings Options

[Table 4-1](#) describes the Phone Settings Options that can be configured on the IVR.

Table 4-1 *Network Menu Options*

Option	Description
DHCP	Indicates whether the phone has DHCP enabled or disabled. When DHCP is enabled, the DHCP server assigns the phone an IP address, the subnet mask, default router, and TFTP Server. When DHCP is disabled, the administrator must manually assign the IP address, subnet mask, default router, and TFTP server on the phone.
IP Address	Internet Protocol (IP) address of the phone. If you assign an IP address with this option, you must also assign a subnet mask and default router. See the Subnet Mask and Default Router options in this table.

Table 4-1 Network Menu Options (continued)

Option	Description
Subnet Mask	Subnet mask used by the phone.
Default Router 1	Default router used by the phone (Default Router 1).
TFTP Server	Primary Trivial File Transfer Protocol (TFTP) server used by the phone. If you are not using DHCP in your network or you want to change this server, you must assign the TFTP Server.
802.1 xSecurity	Indicates whether the phone has 802.1x security enabled or disabled.

Accessing the Phone Configuration Settings

You can change the PIN of the IVR by navigating to **Device > Device Settings > Common Phone Profile**, and specifying a password for the **Local Phone Unlock Password** field in the Common Phone Profile Configuration page.

**Note**

When there is no User ID and/or PIN associated with a phone, the phone uses a default PIN of 24726.

Related Topics

- [Configuring Settings on the Cisco Unified IP Phone, page 4-1](#)

Accessing the IVR and Configuring Your Phone Setting

To access the IVR and configure your phone settings, follow these steps:

**Note**

You can change the PIN by using the **Local Phone Unlock Password** in the Common Phone Profile Configuration page of the Cisco Unified CM Administration web page.

Procedure

- Step 1** To access the IVR, go off-hook and press the *, #, and 0 buttons simultaneously. Alternatively on the Cisco Unified IP Phone 6911, you can toggle the speaker button and press the *, #, and 0 buttons simultaneously.

The IVR prompts for a password.

**Note**


The Cisco Unified IP Phone 6901 and 6911 allow you to enter only numerical values for password.

- Step 2** Enter the PIN by pressing the number keypad, followed by # button.
You are at the IVR main configuration menu.
- Step 3** Follow the voice prompts on the IVR. Refer to [Table 4-2](#) for information on navigating the IVR.
- Step 4** To return to the main configuration menu, press #.

Step 5 To exit the IVR, end the call.

Table 4-2 describes the various options in the IVR Configuration Menu.

Table 4-2 Navigating the IVR Configuration Menu

Action	IVR Code	Navigating Notes
Review or Set Network Settings	1	<p>If DHCP is enabled, the IVR announces each network parameter.</p> <p>If DHCP is disabled, the IVR announces each network parameter, pausing in between to allow you to enter a new value.</p> <ol style="list-style-type: none"> 1. IVR announces the IP Address. To change the IP address for the phone, use the keypad to enter a new IP address, followed by the #. To retain the current IP address, press #. 2. IVR announces the subnet mask. To change the subnet mask use the keypad to enter a new IP address, followed by the #. To retain the current subnet mask, press #. <p> Note To enter the dot “.” that separates each octet in the IP address, press *.</p> <ol style="list-style-type: none"> 3. IVR announces the default gateway. To change the default gateway, use the keypad to enter a new IP address, followed by the #. To retain the current default gateway, press #.
Review or Set TFTP Server	2	<p>IVR announces the current TFTP setting.</p> <p>To change the TFTP server, use the keypad to enter a new IP address, followed by the #. To retain the current TFTP server, press #.</p> <p>To reset a TFTP server back to the TFTP server set by the DHCP server from a manually configured TFTP server, press *.</p> <p>Note To enter the dot “.” that separates each octet in the IP address, press *.</p>
Enable or Disable DHCP	3	Press 3 to toggle DHCP to enable or disable.
Enable or Disable 802.1X	4	Press 4 to toggle 802.1X to enable or disable security.
Reset to factory settings	0	<p>—</p> <p>Note All configuration settings will reset to default factory settings, the and phone will reset. It will take some time for the phone to re-register. Select this option only when needed.</p>



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 the Cisco Unified Communications Manager Administration application to configure telephony features, optionally modify phone templates, set up services, and assign users.

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

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

For suggestions about how to provide users with information about features, and what information to provide, see [Appendix A, “Providing Information to Users Via a Website.”](#)

For information about setting up phones in non-English environments, see [Appendix C, “Technical Specifications.”](#)

This chapter includes following topics:

- [Telephony Features Available for the Cisco Unified IP Phone, page 5-1](#)
- [Adding Users to Cisco Unified Communications Manager, page 5-8](#)
- [Managing the User Options Web Pages, page 5-9](#)

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, refer to *Cisco Unified IP Phone 6901 and 6911 User Guide for Cisco Unified Communications Manager*.



Note

Cisco Unified Communications Manager Administration also provides several service parameters that you can use to configure various telephony functions. For more information on accessing and configuring service parameters, refer to *Cisco Unified Communications Manager Administration Guide*.

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

Table 5-1 *Telephony Features for the Cisco Unified IP Phone*

Feature	Description	Configuration Reference
Agent Greeting	<p>Allows an agent to create and update a prerecorded greeting that plays at the beginning of a call, such as a customer call, before the agent begins the conversation with the caller. The agent can record greetings and update them, as required.</p> <p>When a customer calls, both the agent and the customer can hear the prerecorded greeting. The agent can remain on mute until the greeting ends or answer the call over the greeting.</p> <p>All codecs supported for the phone are supported for Agent Greeting calls.</p> <p>To enable Agent Greeting in the Cisco Unified CM Administration application, choose Device > Phone, and locate the IP Phone that you want to configure. Scroll to the Device Information Layout pane and set the Built In Bridge field to On or Default.</p> <p>If Built In Bridge is set to Default, choose System > Service Parameter and select the appropriate Server and Service. Scroll to the Clusterwide Parameters (Device - Phone) pane and set Built In Bridge Enable to On.</p>	<p>For more information, see:</p> <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Features and Services Guide</i>, Barge and Privacy. • <i>Cisco Unified Communications Manager System Guide</i>, <i>Cisco Unified IP Phones</i>.
Audible Message Waiting Indicator (AMWI)	<p>A stutter tone from the handset or speakerphone indicates that a user has one or more new voice messages on a line.</p>	<p>For more information, go to the “Cisco Unified IP Phone” chapter in the <i>Cisco Unified Communications Manager System Guide</i>.</p>
Auto Answer (Cisco Unified IP Phone 6911 only)	<p>Connects incoming calls automatically after a ring or two.</p> <p>Auto Answer works with the speakerphone.</p>	<p>For more information, go to the “Directory Number Configuration” chapter in the <i>Cisco Unified Communications Manager Administration Guide</i>.</p>

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

Feature	Description	Configuration Reference
Automatic Port Synchronization (Cisco Unified IP Phone 6911 only)	<p>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.</p> <p>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.</p> <p>Note If both the ports are configured for fixed speed, the Automatic Port Synchronization feature is ineffective.</p> <p>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.</p>	<p>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.</p> <p>To configure the setting on multiple phones simultaneously, enable Automatic Port Synchronization in either the Enterprise Phone Configuration (System > Enterprise Phone Configuration) or the Common Phone Profile Configuration (Device > Device Settings > Common Phone Profile).</p>
Auto Barge	Allows user to charge into a shared line call automatically.	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Features and Services Guide</i> “Barge and Privacy” chapter.
Block External to External Transfer	Prevents users from transferring an external call to another external number.	For more information, go to the “ External Call Transfer Restrictions ” chapter in the <i>Cisco Unified Communications Manager Features and Services Guide</i> .
Call Forward	<p>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.</p> <p>You will hear a stutter tone after off-hook if Call Forward All feature is configured on your phone.</p>	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Administration Guide</i>, “Directory Number Configuration” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone” chapter. • “Specifying Options that Appear on the User Options Web Pages” section on page 5-11

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

Feature	Description	Configuration Reference
Call Forward All Loop Breakout	Detects and prevents Call Forward All loops. When a Call Forward All loop is detected, the Call Forward All configuration is ignored and the call rings through.	For more information, go to the “ Cisco Unified IP Phone ” chapter in the <i>Cisco Unified Communications Manager System Guide</i> .
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 <i>Forward Maximum Hop Count</i> service parameter allows.	For more information, go to the “ Cisco Unified IP Phone ” chapter in the <i>Cisco Unified Communications Manager System Guide</i> .
Call Forward Destination Override	Allows you to override Call Forward All (CFA) in cases where the CFA target places a call to the CFA initiator. This feature allows the CFA target to reach the CFA initiator for important calls. The override works whether the CFA target phone number is internal or external.	For more information, go to the “ Understanding Directory Numbers ” chapter in the <i>Cisco Unified Communications Manager System Guide</i> .
Call Pickup (Cisco Unified IP Phone 6911 only)	Allows users to answer a call that is ringing on a co-worker's phone by redirecting the call to their phone You can configure an audio alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group.	For more information, go to the “ Call Pickup ” chapter in the <i>Cisco Unified Communications Manager Features and Services Guide</i> .
Call Waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. The phone sounds the call waiting tone (single beep) and the line button flashes amber.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Directory Numbers” chapter.
cBarge	Allows a user to join a non-private call on a shared phone line. cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Barge and Privacy” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone” chapter. • <i>Cisco Unified Communications Manager Features and Services Guide</i> “Barge and Privacy” chapter.
Cisco Unified Video Advantage (CUVA) (Cisco Unified IP Phone 6911 only)	Allows users to make video calls by using your Cisco Unified IP Phone, your personal computer, and an external video camera.	Configure Video Capabilities and Auto Line Select parameter in the Product Specific Configuration Layout section in Phone Configuration.
Cisco Web Dialer	Allows users to make calls from web and desktop applications.	For more information go to the “ Cisco Web Dialer ” chapter in the <i>Cisco Unified Communications Manager Features and Services Guide</i> .

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

Feature	Description	Configuration Reference
Client Matter Codes (CMC)	Enables a user to specify that a call relates to a specific client matter.	For more information, go to the “ Client Matter Codes and Forced Authorization Codes ” chapter in the <i>Cisco Unified Communications Manager Features and Services Guide</i> .
Conference	<ul style="list-style-type: none"> Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference and Meet Me. Allows a non-initiator in a standard (ad hoc) conference to add participants; also allows any conference participant to join together two standard conferences on the same line. Allows a conference host on the Cisco Unified IP Phone 6901 to remove the last participant that joined the conference by using the hookflash feature. 	<p>The service parameter, Advance Adhoc Conference, (disabled by default in Cisco Unified Communications Manager Administration) allows you to enable these features.</p> <p>For information on conferences, go to the “Conference Bridges” chapter in the <i>Cisco Unified Communications Manager System Guide</i>.</p> <p>For more information, go to the “Cisco Unified IP Phone” chapter in the <i>Cisco Unified Communications Manager System Guide</i>.</p> <p>Note Be sure to inform your users whether these features are activated.</p>
CTI Applications	A computer telephony integration (CTI) route point can designate a virtual device to receive multiple, simultaneous calls for application-controlled redirection.	For more information, go to the “ CTI Route Point Configuration ” chapter in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Forced Authorization Codes (FAC)	Controls the types of calls that certain users can place.	For more information, go to the “ Client Matter Codes and Forced Authorization Codes ” chapter in the <i>Cisco Unified Communications Manager Features and Services Guide</i> .
Group Call Pickup (Cisco Unified IP Phone 6911 only)	Allows a user to answer a call that is ringing on a directory number in another group.	For more information, go to the “ Call Pickup ” chapter in the <i>Cisco Unified Communications Manager Features and Services Guide</i> .
Hold Status	<p>Enables phones with a shared line to distinguish between the local and remote lines that placed a call on hold.</p> <p>The Line LED illuminates green light for Local Hold and red light for Remote Hold.</p>	No configuration is required.
Hold/Resume	<p>Allows the user to move a connected call from an active state to a held state by using the Hold button. The user resumes a held call by pressing the line button, speaker button, or going off-hook.</p> <p>Note The LED on the line button flashes green when a local call is on hold and the LED flashes red when a remote call is on hold.</p>	Requires no configuration, unless you want to use music on hold. See “Music-on-Hold” in this table for information.

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

Feature	Description	Configuration Reference
Meet Me Conference (Cisco Unified IP Phone 6911 only)	Allows a user to host a Meet Me conference in which other participants call a predetermined number at a scheduled time. The user joins a meet me conference by pressing the feature button and the meet me conference number.	For more information go to the “ Meet Me Number/Pattern Configuration ” chapter in the <i>Cisco Unified Communications Manager Administration Guide</i> .
Message Waiting	Defines directory numbers for message-waiting on and message-waiting off indicator. A directly connected voice-messaging system uses the specified directory number to set or to clear a message-waiting indication for a particular Cisco Unified IP Phone.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Administration Guide</i>, “Message Waiting Configuration” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter.
Message Waiting Indicator	A light on the handset that indicates that a user has one or more new voice messages.	For more information refer to: <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Administration Guide</i>, “Message Waiting Configuration” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter.
Music on Hold	Plays music while callers are on hold.	For more information go to the “ Music On Hold ” chapter in the <i>Cisco Unified Communications Manager Features and Services Guide</i> .
Mute (Cisco Unified IP Phone 6911 only)	Mutes the microphone from the handset or speakerphone.	Requires no configuration.
On-hook Call Transfer	Allows a user to press the Transfer button and then go on-hook to complete a call transfer.	For more information refer to <i>Cisco Unified Communications Manager System Guide</i> , “Cisco Unified IP Phones” chapter.
Plus Dialing	Allows the user to dial E.164 numbers prefixed with a “+” sign. To dial the + sign, the user needs to press and hold the “*” key for at least 1 second. This applies to dialing the first digit for both on-hook or off-hook calls.	Requires no configuration.
Private Line Automated Ringdown (PLAR)	The Cisco Unified Communications Manager administrator can configure a phone number that the Cisco Unified IP Phone dials as soon as the handset goes off-hook. This can be useful for phones that are designated for calling emergency or “hotline” numbers.	For more information, go to the “ Directory Number Configuration ” chapter in the <i>Cisco Unified Communications Manager Administration Guide</i> .

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

Feature	Description	Configuration Reference
Redial	Allows users to call the most recently dialed phone number by pressing the Redial button.	Requires no configuration.
Remote Port Configuration	<p>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.</p> <p>Note If the ports are configured for Remote Port Configuration in Cisco Unified CM, the data cannot be changed on the phone.</p>	<p>To configure the parameter in the Cisco Unified CM Administration application, choose Device > Phone, select the appropriate IP phone, and scroll to the Product Specific Configuration Layout pane (Switch Port Remote Configuration or PC Port Remote Configuration).</p> <p>To configure the setting on multiple phones simultaneously, configure the remote configuration in either Enterprise Phone Configuration (System > Enterprise Phone Configuration) or Common Phone Profile Configuration (Device > Device Settings > Common Phone Profile). (Switch Port Remote Configuration or PC Port Remote Configuration)</p>
Shared Line	Allows a user to have multiple phones that share the same phone number or allows a user to share a phone number with a coworker.	For more information, go to the “ Understanding Directory Numbers ” chapter in the <i>Cisco Unified Communications Manager System Guide</i> .
Monitoring and Recording (Cisco Unified IP Phone 6911 only)	<p>Allows a supervisor to monitor an active call silently. The supervisor cannot be heard by either party on the call. The user may receive an audible alert during a call when it is being monitored.</p> <p>When a call is secure, a lock icon is displayed. Callers may also receive an audible alert to indicate that the call is being monitored. The connected parties may also receive an audible alert that indicates the call is secure and is being monitored.</p> <p>When an active call is being monitored or recorded, you can receive or place intercom calls; however, if you place an intercom call, the active call is put on hold. This causes the recording session to terminate and the monitoring session to suspend. To resume the monitoring session, the person being monitored must resume the call.</p>	For more information, refer to the <i>Cisco Unified Communications Manager Features and Services Guide</i> , “ Monitoring and Recording ” chapter.
Speed Dialing (Cisco Unified IP Phone 6911 only)	<p>Dials a specified number that has been previously stored.</p> <p>You have to configure this feature on the Cisco Unified Communications Manager; the users use the Feature key and the Feature Code to access speed dial.</p>	<p>For more information refer to:</p> <ul style="list-style-type: none"> • <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone” chapter.

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

Feature	Description	Configuration Reference
Time-of-Day Routing	Restricts access to specified telephony features by time period.	For more information refer to: <ul style="list-style-type: none"> <i>Cisco Unified Communications Manager Administration Guide</i>, “Time Period Configuration” chapter. <i>Cisco Unified Communications Manager System Guide</i>, “Time-of-Day Routing” chapter.
Time Zone Update	Updates the Cisco Unified IP Phone with time zone changes.	For more information, refer to the <i>Cisco Unified Communications Manager Administration Guide</i> , “ Date/Time Group Configuration ” chapter.
Transfer	Allows users to redirect connected calls from their phones to another number.	Some JTAPI/TAPI applications are not compatible with the Direct Transfer feature implementation on the Cisco Unified IP Phone 6901 and 6911.
Voice messaging system	Enables callers to leave messages if calls are unanswered. Messages are accessed using the Message button on the Cisco Unified IP Phone 6911. Messages are accessed using the access code on the Cisco Unified IP Phone 6901.	For more information refer to: <ul style="list-style-type: none"> <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Voice-Mail Port Configuration” chapter. <i>Cisco Unified Communications Manager System Guide</i>, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter.

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:

- Create a personal directory.
- Set up speed dial and call forwarding numbers.

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

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

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

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

For more information, go to the “[Bulk Administration](#)” chapter in *Cisco Unified Communications Manager Administration Guide*.

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



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

For more information on LDAP, go to the “[Understanding the Directory](#)” chapter in the *Cisco Unified Communications Manager System Guide*.

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

Managing the User Options Web Pages

From the User Options web page, users can customize and control several phone features and settings. For detailed information about the User Options web pages, refer to *Cisco Unified IP Phone 6901 and 6911 User Guide for Cisco Unified Communications Manager*.

Giving Users Access to the User Options Web Pages

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

To add the user to the standard Cisco Unified Communications Manager end user group, you must 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 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 to find the end users that you want to add and click **Find**.
- Step 6** A list of end users that matches your search criteria displays.
- Step 7** In the list of records that display, click the check box next to the users that you want to add to this user group. If the list comprises multiple pages, use the links at the bottom to see more results.



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

- Step 8** Click **Add Selected**.
-

To associate 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.
- Step 8** From Related Links drop-down list in the upper, right corner of the window, select **Back to User**, and click **Go**.
The End User Configuration window displays and the associated devices that you chose display in the Controlled Devices pane.
- Step 9** Click **Save Selected/Changes**.
-

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 name of the Cisco Unified Communications Manager.
- A user ID and default password are needed to access the application.
These settings correspond to the values you entered when you added the user to Cisco Unified Communications Manager (see the [“Adding Users to Cisco Unified Communications Manager” section on page 5-8](#)).

For additional information, refer to:

- *Cisco Unified Communications Manager Administration Guide*, “[User Group Configuration](#)” chapter.
- *Cisco Unified Communications Manager Administration Guide*, “[End User Configuration](#)” chapter.

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 Call Forwarding
- Show Message Waiting Lamp
- Show Audible Message Waiting Indicator

**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 for the parameter:

- **True**—Option displays on the User Options web pages (default except for Show Ring Settings, 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.
-



CHAPTER 6

Monitoring the Cisco Unified IP Phone Remotely

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

- Device information
- Network setup information
- Network statistics
- Device logs
- Streaming statistics

This chapter describes the information that you can obtain from the phone's web page. You can use this information to remotely monitor the operation of a phone and to assist with troubleshooting.

For more information about troubleshooting the Cisco Unified IP Phone, [Chapter 7, “Troubleshooting and Maintenance.”](#)

This chapter includes these topics:

- [Accessing the Web Page for a Phone, page 6-2](#)
- [Disabling and Enabling Web Page Access, page 6-3](#)
- [Device Information, page 6-3](#)
- [Network Setup, page 6-4](#)
- [Network Statistics, page 6-7](#)
- [Device Logs, page 6-9](#)
- [Streaming Statistics, page 6-13](#)

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 the [“Disabling and Enabling Web Page Access” section on page 6-3](#) for more information.

Procedure

-
- Step 1** Obtain the IP address of the Cisco Unified IP Phone using one of these methods:
- Search for the phone in Cisco Unified Communications Manager 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 *, #, and 0 buttons simultaneously, enter the password, and then follow the voice prompts to review the network setting.
- 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`
-

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

- **Device Information**—Displays device settings and related information for the phone. For more information, see the [“Device Information” section on page 6-3](#).
- **Network Setup**—Displays network configuration information and information about other phone settings. For more information, see the [“Network Setup” section on page 6-4](#).
- **Network Statistics**—Includes the following hyperlinks, which provide information about network traffic:
 - **Ethernet Information**—Displays information about Ethernet traffic. For more information, see the [“Network Statistics” section on page 6-7](#).
 - **Network (Port)**—Displays information about network traffic to and from the network port on the phone. For more information, see the [“Network Statistics” section on page 6-7](#).
- **Device Logs**—Includes the following hyperlinks, which provide information that you can use for troubleshooting:
 - **Console Logs**—Includes hyperlinks to individual log files. For more information, see the [“Device Logs” section on page 6-9](#).
 - **Core Dumps**—Includes hyperlinks to individual dump files. For more information, see the [“Device Logs” section on page 6-9](#).
 - **Status Messages**—Displays up to 30 of the most recent status messages that the phone has generated since it was last powered up. For more information, see the [“Device Logs” section on page 6-9](#).
- **Streaming Statistics**—Includes the following hyperlink:
 - **Stream**—Displays a variety of streaming statistics. For more information, see the [“Streaming Statistics” section on page 6-13](#).

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 CM User Options web pages.

To 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, choose **Disabled**.
 - Step 5** Click **Save**.
 - Step 6** Click **Apply Config**.
-

To enable web page access when it is disabled, see the preceding steps about disabling access. Follow the same steps, but choose **Enabled** in [Step 4](#) to enable the web page.

Device Information

The Device Information area on a phone's web page displays device settings and related information for the phone. [Table 6-1](#) 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”](#) section on [page 6-2](#), and then click the **Device Information** hyperlink.

Table 6-1 Device Information Area Items

Item	Description
MAC Address	Media Access Control (MAC) address of the phone
Host Name	Unique, fixed name that is automatically assigned to the phone based on its MAC address
Phone DN	Directory number assigned to the phone
App Load ID	Identifier of the firmware running on the phone
Boot Load ID	Identifier of the factory-installed load running on the phone
Hardware Revision	Revision value of the phone hardware
Serial Number	Unique serial number of the phone
Model Number	Model number of the phone
Message Waiting	Indicates if there is a voice message waiting on the primary line for this phone

Table 6-1 Device Information Area Items (continued)

Item	Description
UDI	Displays the following Cisco Unique Device Identifier (UDI) information about the phone: <ul style="list-style-type: none"> • Device Type—Indicates hardware type. For example, phone displays for all phone models • Device Description—Displays the name of the phone associated with the indicated model type • Product Identifier—Specifies the phone model • Version Identifier—Represents the hardware version of the phone • Serial Number—Displays the unique serial number of the phone
Time	Time obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs
Time Zone	Time zone obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs
Date	Date obtained from the Date/Time Group in Cisco Unified Communications Manager to which the phone belongs

Network Setup

The Network Setup on a phone's web page displays network setup information and information about other phone settings. [Table 6-2](#) describes these items.

You can view and set many of these items from the Network Setup Menu and the Phone Information Menu on the Cisco Unified IP Phone. For more information, see [Chapter 4, “Configuring Settings on the Cisco Unified IP Phone.”](#)

To display the Network Setup area, access the web page for the phone as described in the [“Accessing the Web Page for a Phone”](#) section on [page 6-2](#), and then click the **Network Configuration** hyperlink.

Table 6-2 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.
MAC Address	Media Access Control (MAC) address of the phone.
Host Name	Host name that the DHCP server assigned to the phone.
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.
IP Address	Internet Protocol (IP) address of the phone.
Subnet Mask	Subnet mask used by the phone.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone.
TFTP Server 2	Backup Trivial File Transfer Protocol (TFTP) server used by the phone.
Default Router 1	Default router used by the phone.
DNS Server 1 through 5	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS server (DNS Server 2 - 5) used by the phone.

Table 6-2 Network Configuration Area Items (continued)

Item	Description
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.
CallManager 1–5	<p>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.</p> <p>For an available server, an item will show the Cisco Unified Communications Manager server IP address and one of the following states:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
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.
Forwarding Delay	Indicates whether the internal switch begins forwarding packets between the PC port and switched port on your phone when your 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 SW port. You should set forwarding delay to enabled when you connect both ports to switches for redundant uplinks or when you daisy-chain phones together.
Automatic Port Synchronization (Cisco Unified IP Phone 6911 only)	Indicates if the automatic port synchronization is enabled or disabled. 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.
SW Port Remote Configuration	Indicates if software port configuration of the speed and duplex mode for the SW port is enabled or disabled.
PC Port Remote Configuration (Cisco Unified IP Phone 6911 only)	Indicates if remote port configuration of the speed and duplex mode for the PC port is enabled or disabled.

Table 6-2 Network Configuration Area Items (continued)

Item	Description
SW Port Setup	Speed and duplex of the switch port, where: <ul style="list-style-type: none"> • 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 Setup (Cisco Unified IP Phone 6911 only)	Speed and duplex of the switch port, where: <ul style="list-style-type: none"> • 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
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.
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 (Cisco Unified IP Phone 6911 only)	Indicates whether the PC port on the phone is enabled or disabled.
Speaker Enabled (Cisco Unified IP Phone 6911 only)	Indicates whether the speakerphone is enabled on the phone.
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.
Video Capability Enabled (Cisco Unified IP Phone 6911 only)	Indicates whether the phone can participate in video calls when connected to an appropriately equipped PC.
Voice VLAN Enabled	Indicates whether the phone allows a device attached to the PC port to access the Voice VLAN.
DSCP for Call Control	DSCP IP classification for call control signaling.
DSCP for Configuration	DSCP IP classification for any phone configuration transfer.
DSCP for Services	DSCP IP classification for phone-based services.
Security Mode	Displays the security mode that is set for the phone.

Table 6-2 Network Configuration Area Items (continued)

Item	Description
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.
Span to PC Port (Cisco Unified IP Phone 6911 only)	Indicates whether the phone will forward packets transmitted and received on the network port to the access port.
CDP: PC Port (Cisco Unified IP Phone 6911 only)	Indicates whether CDP is supported on the PC port (default is enabled). Enable CDP on the PC port when Cisco VT Advantage/Unified Video Advantage (CVTA) is connected to the PC port. CVTA does not work without CDP interaction with the phone. When CDP is disabled in Cisco Unified Communications Manager, a warning is displayed, indicating that disabling CDP on the PC port prevents CVTA from working. The current PC and switch port CDP values are shown on the Settings menu.
CDP: SW Port	Indicates whether CDP is supported on the switch port (default is enabled). Enable CDP on the switch port for VLAN assignment for the phone, power negotiation, QoS management, and 802.1x security. Enable CDP on the switch port when the phone is connected to a Cisco switch. When CDP is disabled in Cisco Unified Communications Manager, a warning is presented, indicating that CDP should be disabled on the switch port only if the phone is connected to a non-Cisco switch. The current PC and switch port CDP values are shown on the Settings menu.

Network Statistics

The following network statistics hyperlinks on a phone's web page provide information about network traffic on the phone. To display a network statistics area, access the web page for the phone as described in the [“Accessing the Web Page for a Phone”](#) section on page 6-2.

- Ethernet Information—Displays information about Ethernet traffic. [Table 6-3](#) describes the items in this area.
- Network Information (Cisco Unified IP Phone 6901)—Displays information about network traffic to and from the network port (10/100 SW) on the phone. [Table 6-5](#) describes the items in this area.
- Network and Access Information (Cisco Unified IP Phone 6911)—Displays information about network traffic to and from the network port (10/100 SW) on the phone. [Table 6-5](#) describes the items in this area.

Table 6-3 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

Table 6-3 Ethernet Information Items (continued)

Item	Description
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 6-4 Network Items on the Cisco Unified IP Phone 6901

Item	Description
Tx Frames	Total number of packets transmitted by the phone
Tx broadcast	Total number of broadcast packets transmitted by the phone
Tx unicast	Total number of unicast packets transmitted by the phone
Rx Frames	Total number of packets received by the phone
Rx broadcast	Total number of broadcast packets received by the phone
Rx unicast	Total number of unicast packets received by the phone
Neighbor Device ID	Identifier of a device connected to this port discovered by CDP protocol or LLDP
Neighbor IP Address	IP address of the neighbor device discovered by CDP protocol
Neighbor Port	Neighbor device port to which the phone is connected discovered by CDP protocol
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
Restart Cause	Reason for the last restart
Port	Speed and duplex information
IPv4	IPv4 Address

Table 6-5 Network and Access Items on the Cisco Unified IP Phone 6911

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

Table 6-5 Network and Access Items on the Cisco Unified IP Phone 6911 (continued)

Item	Description
Rx unicast	Total number of unicast packets received by the phone
Rx shortErr	Total number of FCS error packets or Align error packets received that are less than 64 bytes in size
Rx shortGood	Total number of good packets received that are less than 64 bytes size
Rx longGood	Total number of good packets received that are greater than 1522 bytes in size
Rx longErr	Total number of FCS error packets or Align error packets received that are greater than 1522 bytes in size
Rx size64	Total number of packets received, including bad packets, that are between 0 and 64 bytes in size
Rx 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
Neighbor Device ID	Identifier of a device connected to this port discovered by CDP protocol or LLDP
Neighbor IP Address	IP address of the neighbor device discovered by CDP protocol
Neighbor Port	Neighbor device port to which the phone is connected discovered by CDP protocol
Port Information	Speed and duplex information

Device Logs

The following device logs hyperlinks on a phone's web page provide information you can use to help monitor and troubleshoot the phone. To access a device log area, access the web page for the phone as described in the [“Accessing the Web Page for a Phone”](#) section on page 6-2.

- 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 30 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 Web page of the phone. [Table 6-6](#) describes the status messages that may be displayed.
- **Debug Display**—Displays debug messages that might be useful to the Cisco Technical Assistance Center (TAC) if you require assistance with troubleshooting.

Status Messages

The Status Messages web page displays up to 30 of the most recent status messages that the phone has generated since it was last powered up. You can access the Status Messages web page even if the phone is not running. [Table 6-6](#) describes the status messages. This table also includes possible explanations and actions to troubleshoot errors.

Table 6-6 Status Messages on the Cisco Unified IP Phone 6900 Series Phones

Message	Description	Possible Explanation and Action
CFG file not found	The name-based and default configuration file was not found on the TFTP Server.	<p>The configuration file for a phone is created when the phone is added to the Cisco Unified Communications Manager database. If the phone has not been added to the Cisco Unified Communications Manager database, the TFTP server generates a CFG File Not Found response.</p> <ul style="list-style-type: none"> • Phone is not registered with Cisco Unified Communications Manager. <p>You must manually add the phone to Cisco Unified Communications Manager if you are not allowing phones to auto-register. See the “Adding Phones to the Cisco Unified Communications Manager Database” section on page 2-7 for details.</p> <ul style="list-style-type: none"> • 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 the TFTP server configuration.
CFG TFTP Size Error	The configuration file is too large for the file system on the phone.	Power cycle the phone.
Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firmware and place it in the TFTPPath directory. You should only copy files into this directory when the TFTP server software is shut down, otherwise the files may be corrupted.

Table 6-6 Status Messages on the Cisco Unified IP Phone 6900 Series Phones (continued)

Message	Description	Possible Explanation and Action
DHCP timeout	DHCP server did not respond.	<ul style="list-style-type: none"> 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 the DHCP server configuration. Errors persist—Consider assigning a static IP address.
DNS timeout	DNS server did not respond.	<ul style="list-style-type: none"> 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 the DNS server configuration.
DNS unknown host	DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	<ul style="list-style-type: none"> Verify that the host names of the TFTP server or Cisco Unified Communications Manager are configured properly in DNS. Consider using IP addresses rather than host names.
Duplicate IP	Another device is using the IP address assigned to the phone.	<ul style="list-style-type: none"> If the phone has a static IP address, verify that you have not assigned a duplicate IP address. If you are using DHCP, check the DHCP server configuration.
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.	<p>From Cisco Unified Operating System Administration, check that the following files are located within subdirectories in the TFTP File Management:</p> <ul style="list-style-type: none"> Located in subdirectory with the same name as network locale: <ul style="list-style-type: none"> tones.xml Located in subdirectory with the same name as user locale: <ul style="list-style-type: none"> glyphs.xml dictionary.xml kate.xml
File not found	The phone cannot locate, on the TFTP server, the phone load file that is specified in the phone configuration file.	From Cisco Unified Operating System Administration, make sure that the phone load file is on the TFTP server, and that the entry in the configuration file is correct.
IP address released	The phone has been configured to release its IP address.	The phone remains idle until it is power cycled or you reset the DHCP address.

Table 6-6 Status Messages on the Cisco Unified IP Phone 6900 Series Phones (continued)

Message	Description	Possible Explanation and Action
Load ID incorrect	Load ID of the software file is of the wrong type.	Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose Device > Phone). Verify that the load ID is entered correctly.
Load rejected HC	The application that was downloaded is not compatible with the phone's hardware.	Occurs if you were attempting to install a version of software on this phone that did not support hardware changes on this newer phone. Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose Device > Phone). Re-enter the load displayed on the phone.
No default router	DHCP or static configuration did not specify a default router.	<ul style="list-style-type: none"> If the phone has a static IP address, verify that the default router has been configured. If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.
No DNS server IP	A name was specified but DHCP or static IP configuration did not specify a DNS server address.	<ul style="list-style-type: none"> If the phone has a static IP address, verify that the DNS server has been configured. If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.
TFTP access error	TFTP server is pointing to a directory that does not exist.	<ul style="list-style-type: none"> 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 the TFTP server configuration.
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.

Table 6-6 Status Messages on the Cisco Unified IP Phone 6900 Series Phones (continued)

Message	Description	Possible Explanation and Action
TFTP server not authorized	The specified TFTP server could not be found in the phone's CTL.	<ul style="list-style-type: none"> The DHCP server has the wrong configuration file for the TFTP server. In this case, update the TFTP server configuration to specify the correct TFTP server. The CTL file was made and then the TFTP server address changed. In this case, regenerate the CTL file. If the phone is using a static IP address, the phone may be configured with the wrong TFTP server address. In this case, enter the correct TFTP server address in the Network Configuration menu on the phone. If the TFTP server address is correct, there may be a problem with the CTL file. In this case, run the CTL client and update the CTL file, making sure that the proper TFTP servers are included in this file.
TFTP timeout	TFTP server did not respond.	<ul style="list-style-type: none"> 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 the TFTP server configuration.
Timed Out	Supplicant attempted 802.1X transaction but timed out due the absence of an authenticator.	Authentication typically times out if 802.1X is not configured on the switch.
Version error	The name of the phone load file is incorrect.	Make sure that the phone load file has the correct name.
XmlDefault.cnf.xml, or .cnf.xml corresponding to the phone device name	Name of the configuration file.	None. This is an informational message indicating the name of the configuration file for the phone.

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. Cisco Unified IP Phone 6900 Series phones use only Stream 1.

To display a Streaming Statistics area, access the web page for the phone as described in the [“Accessing the Web Page for a Phone”](#) section on page 6-2, and then click the **Stream 1** hyperlink.

[Table 6-7](#) describes the items in the Streaming Statistics areas.

Table 6-7 Streaming Statistics Area Items

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

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

Related Topics

[“Configuring Settings on the Cisco Unified IP Phone”](#) chapter



CHAPTER 7

Troubleshooting and Maintenance

This chapter provides information that can assist you in troubleshooting problems with your Cisco Unified IP Phone or with your IP telephony network. It also explains how to clean and maintain your phone.

If you need additional assistance to resolve an issue, see the [“Obtaining Documentation, Obtaining Support, and Security Guidelines”](#) section on page ix.

This chapter includes these topics:

- [Resolving Startup Problems](#), page 7-1
- [Cisco Unified IP Phone Resets Unexpectedly](#), page 7-6
- [General Troubleshooting Tips](#), page 7-8
- [Resetting or Restoring the Cisco Unified IP Phone](#), page 7-10
- [Monitoring the Voice Quality of Calls](#), page 7-11
- [Using Voice Quality Metrics](#), page 7-11
- [Where to Go for More Troubleshooting Information](#), page 7-13
- [Cleaning the Cisco Unified IP Phone](#), page 7-13

Resolving Startup Problems

After installing a Cisco Unified IP Phone into your network and adding it to Cisco Unified Communications Manager, the phone should start up as described in the [“Verifying the Phone Startup Process”](#) section on page 3-9. If the phone does not start up properly, see the following sections for troubleshooting information:

- [Symptom: The Cisco Unified IP Phone Does Not Go Through its Normal Startup Process](#), page 7-2
- [Symptom: The Cisco Unified IP Phone Does Not Register with Cisco Unified Communications Manager](#), page 7-2
- [Symptom: Cisco Unified IP Phone Unable to Obtain IP Address](#), page 7-5

Symptom: The Cisco Unified IP Phone Does Not Go Through its Normal Startup Process

When you connect a Cisco Unified IP Phone into the network port, the phone should go through its normal startup process as described in [“Verifying the Phone Startup Process” section on page 3-9](#). 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, perform a factory reset of the phone. For instructions, see the [“Performing a Factory Reset” section on page 7-10](#).

If after attempting these solutions, the phone still does not function, 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 (all LED buttons on) but 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 7-3](#)
- [Checking Network Connectivity, page 7-3](#)
- [Verifying TFTP Server Settings, page 7-3](#)
- [Verifying IP Addressing and Routing, page 7-3](#)
- [Cisco CallManager and TFTP Services Are Not Running, page 7-4](#)
- [Creating a New Configuration File, page 7-4](#)
- [Checking Network Connectivity, page 7-3](#)

In addition, problems with security may prevent the phone from starting up properly. See the “[General Troubleshooting Tips](#)” section on page 7-8 for more information.

Identifying Error Messages

As the phone cycles through the startup process, you can access status messages that might provide you with information about the cause of a problem. See the “[Device Logs](#)” section on page 6-9 for instructions about accessing status messages.

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 *, #, and 0 buttons simultaneously, entering the password, and then following the voice prompts to review the network setting.

If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option. See the “[Configuring Settings on the Cisco Unified IP Phone](#)” section on page 4-1.

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 or Option 66.

You can also enable the phone to use an alternate TFTP server. Such a setting is particularly useful if the phone was recently moved from one location to another. See the “[Configuring Settings on the Cisco Unified IP Phone](#)” section on page 4-1 for instructions.

Verifying IP Addressing and Routing

You should verify the IP addressing and routing settings on the phone. If you are using DHCP, the DHCP server should provide these values. If you have assigned a static IP address to the phone, you must enter these values manually.

On the Cisco Unified IP Phone, press the *, #, and 0 buttons simultaneously, enter the password, and then follow the voice prompts to review the following options:

- IP Address, Subnet Mask, Default Router—If you have assigned a static IP address to the phone, you must manually enter settings for these options. See the “[Configuring Settings on the Cisco Unified IP Phone](#)” section on page 4-1 for instructions.

If you are using DHCP, check the IP addresses distributed by your DHCP server. Refer to the *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* document, available at this URL:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

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



Note

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

Creating a New Configuration File

If you continue to have problems with a particular phone that other suggestions in this chapter do not resolve, the configuration file may be corrupted.

To create a new configuration file, follow these steps:

Procedure

-
- Step 1** From Cisco Unified Communications Manager, choose **Device > Phone > Find** to locate the phone experiencing problems.
 - Step 2** Choose **Delete** to remove the phone from the Cisco Unified Communications Manager database.
 - Step 3** Add the phone back to the Cisco Unified Communications Manager database. See the [“Adding Phones to the Cisco Unified Communications Manager Database”](#) section on page 2-7 for details.
 - Step 4** Power cycle the phone.
-

**Note**

- When you remove a phone from the Cisco Unified Communications Manager database, its configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone's directory number or numbers remain in the Cisco Unified Communications Manager database. They are called "unassigned DNS" and can be used for other devices. If unassigned DNS are not used by other devices, delete them from the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers. Refer to *Cisco Unified Communications Manager Administration Guide* for more information.
- Changing the buttons on a phone button template, or assigning a different phone button template to a phone, may result in directory numbers that are no longer accessible from the phone. The directory numbers are still assigned to the phone in the Cisco Unified Communications Manager database, but there is no button on the phone with which calls can be answered. These directory numbers should be removed from the phone and deleted if necessary.

Registering the Phone with Cisco Unified Communications Manager

A Cisco Unified IP Phone can register with a Cisco Unified Communications Manager server only if the phone has been added to the server or if auto-registration is enabled and if there is a sufficient number of unit licenses. Review the information and procedures in the ["Adding Phones to the Cisco Unified Communications Manager Database"](#) section on page 2-7 to ensure that the phone has been added to the Cisco Unified Communications Manager database.

To verify that the phone is in the Cisco Unified Communications Manager database, choose **Device > Phone > Find** from Cisco Unified Communications Manager Administration to search for the phone based on its MAC Address. For information about determining a MAC address, see the ["Using Cisco Unified IP Phones with Different Protocols"](#) section on page 2-11.

If the phone is already in the Cisco Unified Communications Manager database, its configuration file may be damaged. See the ["Creating a New Configuration File"](#) section on page 7-4 for assistance.

For more information on licensing go to the [Licenses for Phones](#) section in the *Cisco Unified Communications Manager System Guide*

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 not be on the same network or VLAN as the DHCP server, or the switch port to which the phone is connected may be disabled. Make sure that the network or VLAN to which the phone is connected has access to the DHCP server, and make sure that the switch port is enabled.

Cisco Unified IP Phone Resets Unexpectedly

If users report that their phones are resetting during calls or while idle on their desk, you should investigate the cause. If the network connection and Cisco Unified Communications Manager connection are stable, a Cisco Unified IP Phone should not reset on its own.

Typically, a phone resets if it has problems connecting to the Ethernet network or to Cisco Unified Communications Manager. These sections can help you identify the cause of a phone resetting in your network:

- [Verifying the Physical Connection, page 7-6](#)
- [Identifying Intermittent Network Outages, page 7-6](#)
- [Verifying DHCP Settings, page 7-6](#)
- [Checking Static IP Address Settings, page 7-7](#)
- [Verifying the Voice VLAN Configuration, page 7-7](#)
- [Verifying that the Phones Have Not Been Intentionally Reset, page 7-7](#)
- [Eliminating DNS or Other Connectivity Errors, page 7-7](#)

Verifying the Physical Connection

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

Identifying Intermittent Network Outages

Intermittent network outages affect data and voice traffic differently. Your network might have been experiencing intermittent outages without detection. If so, data traffic can resend lost packets and verify that packets are received and transmitted. However, voice traffic cannot recapture lost packets. Rather than retransmitting a lost network connection, the phone resets and attempts to reconnect its network connection.

If you are experiencing problems with the voice network, you should investigate whether an existing problem is simply being exposed.

Verifying DHCP Settings

The following suggestions can help you determine if the phone has been properly configured to use DHCP:

1. Verify that you have properly configured the phone to use DHCP. See the [“Configuring Settings on the Cisco Unified IP Phone” section on page 4-1](#) for more information.
2. Verify that the DHCP server has been set up properly.
3. Verify the DHCP lease duration. Cisco recommends that you set it to 8 days.

Checking Static IP Address Settings

If the phone has been assigned a static IP address, verify that you have entered the correct settings. See the [“Configuring Settings on the Cisco Unified IP Phone” section on page 4-1](#) for more information.

Verifying the Voice VLAN Configuration

If the Cisco Unified IP Phone appears to reset during heavy network usage (for example, following extensive web surfing on a computer connected to the same switch as the phone), it is likely that you do not have a voice VLAN configured.

Isolating the phones on a separate auxiliary VLAN increases the quality of the voice traffic. See the [“Understanding How the Cisco Unified IP Phone 6911 Interacts with the VLAN” section on page 2-2](#) for details.

Verifying that the Phones Have Not Been Intentionally Reset

If you are not the only administrator with access to Cisco Unified Communications Manager, you should verify that no one else has intentionally reset the phones.

You can check whether a Cisco Unified IP Phone received a command from Cisco Unified Communications Manager to reset by pressing the **Applications** button on the phone and choosing **Administrator Settings > Status > Network Statistics**. If the phone was recently reset, one of these messages appears:

- Reset-Reset—Phone closed due to receiving a Reset/Reset from Cisco Unified Communications Manager Administration.
- Reset-Restart—Phone closed due to receiving a Reset/Restart from Cisco Unified Communications Manager Administration.

Eliminating DNS or Other Connectivity Errors

If the phone continues to reset, follow these steps to eliminate DNS or other connectivity errors:

Procedure

-
- Step 1** Use the Reset Settings menu to reset phone settings to their default values. See the [“Resetting or Restoring the Cisco Unified IP Phone” section on page 7-10](#) for details.
- Step 2** Modify DHCP and IP settings:
- a. Disable DHCP. See the [“Configuring Settings on the Cisco Unified IP Phone” section on page 4-1](#) for instructions.
 - b. Assign static IP values to the phone. See the [“Configuring Settings on the Cisco Unified IP Phone” section on page 4-1](#) for instructions. Use the same default router setting used for other functioning Cisco Unified IP Phones.
 - c. Assign a TFTP server. See the [“Configuring Settings on the Cisco Unified IP Phone” section on page 4-1](#) for instructions. Use the same TFTP server used for other functioning Cisco Unified IP Phones.

- Step 3** On the Cisco Unified Communications Manager server, verify that the local host files have the correct Cisco Unified Communications Manager server name mapped to the correct IP address.
- Step 4** From Cisco Unified Communications Manager, choose **System > Server** and verify that the server is referred to by its IP address and not by its DNS name.
- Step 5** From Cisco Unified Communications Manager, choose **Device > Phone > Find** and verify that you have assigned the correct MAC address to this Cisco Unified IP Phone. For information about determining a MAC address, see the [“Using Cisco Unified IP Phones with Different Protocols”](#) section on page 2-11.
- Step 6** Power cycle the phone.

Checking Power Connection

In most cases, a phone will restart if it powers up by using external power but loses that connection and switches to PoE. Similarly, a phone may restart if it powers up by using PoE and then gets connected to an external power supply.

General Troubleshooting Tips

[Table 7-1](#) provides general troubleshooting information for the Cisco Unified IP Phone.

Table 7-1 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.	<p>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.</p> <p> Caution The computer’s network card cannot receive power through the network connection; if power comes through the connection, the network card can be destroyed. To protect a network card, wait 10 seconds or longer after unplugging the cable from the phone before plugging it into a computer. This delay gives the switch enough time to recognize that there is no longer a phone on the line and to stop providing power to the cable.</p>

Table 7-1 Cisco Unified IP Phone Troubleshooting (continued)

Summary	Explanation
Changing the telephone configuration.	By default, the network configuration options are locked to prevent users from making changes that could impact their network connectivity. You must unlock the network configuration options before you can configure them. See the “ Accessing the Phone Configuration Settings ” section on page 4-2 for details.
Phone resetting.	The phone resets when it loses contact with the Cisco Unified Communications Manager software. This lost connection can be due to any network connectivity disruption, including cable breaks, switch outages, and switch reboots.
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.
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.
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.
Loopback condition.	<p>A loopback condition can occur when the following conditions are met:</p> <ul style="list-style-type: none"> • The SW Port Configuration option in the Network Configuration menu on the phone is set to 10 Half (10-BaseT / half duplex) • The phone receives power from an external power supply • The phone is powered down (the power supply is disconnected) <p>In this case, the switch port on the phone can become disabled and the following message will appear in the switch console log:</p> <pre>HALF_DUX_COLLISION_EXCEED_THRESHOLD</pre> <p>To resolve this problem, re-enable the port from the switch.</p>
One-way audio.	When at least one person in a call does not receive audio, IP connectivity between phones is not established. Check the configurations in routers and switches to ensure that IP connectivity is properly configured.
Phone call cannot be established.	<p>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.</p> <p>Verify the following:</p> <ol style="list-style-type: none"> 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.

Resetting or Restoring the Cisco Unified IP Phone

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

- [Performing a Basic Reset, page 7-10](#)
- [Performing a Factory Reset, page 7-10](#)

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 7-2](#) 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 7-2 Basic Reset Methods

Operation	Performing	Explanation
Restart phone	Unplug the power cable and plug it back in.	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.
Reset Settings	Reset the phone to its factory settings.	Resets user and network configuration settings to their default values, 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:

- 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 (phone recovers by using the image in the inactive partition of flash to boot up).

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.

To perform a factory reset of a phone, you can use the IVR to reset the network settings to factory default or you can perform the following steps:

Procedure

-
- Step 1** Unplug the power cable from the phone and then plug it back in.
The phone begins its power-up cycle.

Step 2 While the phone is powering up, press and hold # button until the Line LED turns green.

Step 3 Release the # button and press **123456789*0#**.

The line button LED turns red. The phone reboots when it is finished.

Monitoring the Voice Quality of Calls

To measure the voice quality of calls that are sent and received within the network, Cisco Unified IP Phones use these statistical metrics that are based on concealment events. The DSP plays concealment frames to mask frame loss in the voice packet stream.

- Concealment Ratio metrics—Show the ratio of concealment frames over total speech frames. An interval conceal ratio is calculated every 3 seconds.
- Concealed Second metrics—Show the number of seconds in which the DSP plays concealment frames due to lost frames. A severely “concealed second” is a second in which the DSP plays more than five percent concealment frames.
- Mean Opinion Score (MOS) for Listening Quality (LQK) Voice Metrics—Uses a numeric score to estimate the relative voice-listening quality. The Cisco Unified IP Phones calculate the MOS LQK based audible-concealment events due to a frame loss in the preceding 8 seconds and includes weighting factors such as codec type and frame size.

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



Note

Concealment ratio and concealment seconds are primary measurements based on frame loss. A Conceal Ratio of zero indicates that the IP network is delivering frames and packets on time with no loss.

You can access voice quality metrics remotely by using Streaming Statistics (see the [Monitoring the Cisco Unified IP Phone Remotely](#) chapter).

Using Voice Quality Metrics

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

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

The MOS LQK scores can vary based on the codec that the Cisco Unified IP Phone uses. The following codecs provide these corresponding maximum MOS LQK scores under normal conditions with zero frame loss for Cisco Unified Phones 6921, 6941, and 6961:

- G.711: 4.5 MOS LQK
- G.722: 4.5 MOS LQK

- G.728/iLBC: 3.9 MOS LQK
- G.729A/AB: 3.7 MOS LQK

**Note**

- Cisco Voice Transmission Quality (CVTQ) does not support wideband (7 kHz) speech codecs, because ITU has not defined the extension of the technique to wideband. Therefore, MOS LQK scores that correspond to G.711 performance are reported for G.722 calls to allow basic quality monitoring, rather than not reporting an MOS score.
- Reporting G.711-scale MOS scores for wideband calls through the use of CVTQ allows basic-quality classifications to be indicated as good/normal or bad/abnormal. Calls with high scores (approximately 4.5) indicate high quality or a low packet loss, and lower scores (approximately 3.5) indicate low quality or a high packet loss.
- Unlike MOS, the conceal ratio and concealed seconds metrics remain valid and useful for both wideband and narrowband calls.

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

Troubleshooting Tips

When you observe significant and persistent changes to metrics, use [Table 7-3](#) for general troubleshooting information.

Table 7-3 Changes to Voice Quality Metrics

Metric Change	Condition
Conceal Ratio and Conceal Seconds increase significantly	Network impairment from packet loss or high jitter.
Conceal Ratio is near or at zero, but the voice quality is poor.	<ul style="list-style-type: none"> • Noise or distortion in the audio channel such as echo or audio levels. • Tandem calls that undergo multiple encode/decode such as calls to a cellular network or calling card network. • Acoustic problems coming from a speakerphone, handsfree cellular phone or wireless headset. Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.
MOS LQK scores decrease significantly	Network impairment from packet loss or high jitter levels: <ul style="list-style-type: none"> • Average MOS LQK decreases may indicate widespread and uniform impairment. • Individual MOS LQK decreases may indicate bursty impairment. Cross-check the conceal ratio and conceal seconds for evidence of packet loss and jitter.

Table 7-3 *Changes to Voice Quality Metrics (continued)*

Metric Change	Condition
MOS LQK scores increase significantly	<ul style="list-style-type: none"> • Check to see if the phone is using a different codec than expected (RxType and TxType). • Check to see if the MOS LQK version changed after a firmware upgrade.

**Note**

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

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_troubleshoot_and_alerts.html

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

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

Cleaning the Cisco Unified IP Phone

To clean your Cisco Unified IP phone, use only a dry soft cloth to gently wipe the phone. 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 Phone, page A-1](#)
- [How Users Configure Phone Features, page A-2](#)
- [How Users Access a Voice Messaging System, page A-2](#)
- [For information using a voice messaging system, refer to Cisco Unified IP Phone 6901 and 6911 User Guide for Cisco Unified Communications Manager., page A-2](#)

How Users Obtain Support for the Cisco Unified IP Phone

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

Giving Users Access to the User Options Web Pages

Before a user can access the User Options web pages, you must use Cisco Unified Communications Manager Administration to add the user to a standard Cisco Unified Communications Manager end user group: choose **User Management > User Groups**. For additional information, refer to:

- [“User Group Configuration”](#) chapter in the *Cisco Unified Communications Manager Administration Guide*
- [“Role Configuration”](#) chapter in the *Cisco Unified Communications Manager Administration Guide*

How Users 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 setting up speed dial on the Cisco Unified IP Phone 6911, setting up call forwarding numbers on the Cisco Unified IP Phone 6901 and 6911, and creating a personal address book. Keep in mind that configuring settings on a phone by using a website might be new for your end users. You need to provide as much information as possible to ensure that they can successfully access and use the User Options web pages.

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

- The URL required to access the application. This URL is:
http://<server_name:portnumber>/ccmuser/, where *server_name* is the host on which the web server is installed.
- A user ID and default password are needed to access the application.
These settings correspond to the values you entered when you added the user to Cisco Unified Communications Manager (see the [“Adding Users to Cisco Unified Communications Manager” section on page 5-8](#)).
- 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.

For information using the User Options web pages, refer to *Cisco Unified IP Phone 6901 and 6911 User Guide for Cisco Unified Communications Manager*.

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 PIN for accessing the voice messaging system.
Make sure that you have configured a default voice messaging system PIN 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.

For information using a voice messaging system, refer to *Cisco Unified IP Phone 6901 and 6911 User Guide for Cisco Unified Communications Manager*.



APPENDIX **B**

Supporting International Users

Localized versions of the Cisco Unified IP Phones are available. If you are supporting Cisco Unified IP Phones in a non-English environment, refer to the following sections to ensure that the phones are set up properly for your users:

[Installing the Cisco Unified Communications Manager Locale Installer, page B-1](#)

For information on changing the language that is displayed on the User Options web page, refer to *Cisco Unified IP Phone 6901 and 6911 User Guide for Cisco Unified Communications Manager*.

Installing the Cisco Unified Communications Manager Locale Installer

If you are using Cisco Unified IP Phones in a locale other than English (United States), you must install the locale-specific version of the Cisco Unified Communications Manager Locale Installer on every Cisco Unified Communications Manager server in the cluster. Installing the locale installer ensures that you have the latest translated text, user and network locales, and country-specific phone tones available for the Cisco Unified IP Phones.

You can find locale-specific versions of the Cisco Unified Communications Manager Locale Installer at <http://www.cisco.com/kobayashi/sw-center/telephony/callmgr/locale-installer.shtml>.

For more information, refer to the “Locale Installation” section in the “Software Upgrades” chapter of the *Cisco Unified Communications Operating System Administration Guide*.



Note

All languages may not be immediately available, so continue to check the website for updates.



Technical Specifications

The following sections describe the technical specifications for the Cisco Unified IP Phone 6901 and 6911.

- [Physical and Operating Environment Specifications, page C-1](#)
- [Cable Specifications, page C-2](#)
- [Network and Access Port Pinouts, page C-3](#)

Physical and Operating Environment Specifications

[Table C-1](#) shows the physical and operating environment specifications for the Cisco Unified IP Phone 6901.

Table C-1 Physical and Operating Environment Specifications for the Cisco Unified IP Phone 6901

Specification	Value or Range
Operating temperature	23° to 113°F (-5° to 45°C)
Operating relative humidity	10% to 90% (non-condensing)
Storage temperature	-13° to 158°F (-25° to 70°C)
Height	8.1 in. (20.5 cm)
Width	3.7 in. (9.4 cm)
Depth	<ul style="list-style-type: none">• 2.12 in. (5.4 cm)—With footstand closed• 3.42 in. (8.7 cm)—With footstand open
Weight	<ul style="list-style-type: none">• 1.37 lb (621.2 g)—Black handset phone (Europe)• 1.37 lb (662 g)—White handset phone (Europe)• 1.44 lb (655.2 g)—Black handset phone (North America)• 1.53 lb (695 g)—White handset phone (North America)
Power	<ul style="list-style-type: none">• 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

Table C-1 Physical and Operating Environment Specifications for the Cisco Unified IP Phone 6901 (continued)

Specification	Value or Range
Cables	Category 3/5/5e for 10-Mbps cables with four pairs Category 5/5e for 100-Mbps cables with four pairs Note Cables have four pairs of wires for a total of eight 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).

Table C-2 shows the physical and operating environment specifications for the Cisco Unified IP Phone 6911.

Table C-2 Physical and Operating Environment Specifications for the Cisco Unified IP Phone 6911

Specification	Value or Range
Operating temperature	23° to 113°F (-5° to 45°C)
Operating relative humidity	10% to 90% (non-condensing)
Storage temperature	-13° to 158°F (-25° to 70°C)
Height	8.07 in. (20.5 cm)
Width	7.4 in. (18.8 cm)
Depth	5.76 in. (14.64 cm)—Excluding the handset
Weight	<ul style="list-style-type: none"> 1.53 lb (697 g)—Black handset phone 1.65 lb (750.3 g)—White handset phone
Power	<ul style="list-style-type: none"> 100-240 VAC, 50-60 Hz, 0.5 A—When using the AC adapter 48 VDC, 0.2 A—When using the in-line power over the network cable
Cables	Category 3/5/5e for 10-Mbps cables with 4 pairs Category 5/5e for 100-Mbps cables with 4 pairs Note Cables have 4 pairs of wires for a total of 8 conductors.
Distance Requirements	As supported by the Ethernet Specification, it is assumed that the maximum cable length between each Cisco Unified IP Phone and the switch is 100 meters (330 feet).

Cable Specifications

- RJ-9 jack (4-conductor) for handset connection.
- RJ-45 jack for the LAN 10/100BaseT connection (labeled 10/100 SW on the Cisco Unified IP Phone 6901 and 6911).
- RJ-45 jack for a second 10/100BaseT compliant connection (labeled 10/100 PC on the Cisco Unified IP Phone 6911).
- 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 `network` on the Cisco Unified IP Phone.
- The access port is labeled `computer` on the Cisco Unified IP Phone (Cisco Unified IP Phone 6911 only).

Network Port Connector

Table C-3 describes the network port connector pinouts.

Table C-3 Network Port Connector Pinouts

Pin Number	Function
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-

Note “BI” stands for bi-directional, while DA, DB, DC and DD stand for “Data A”, “Data B”, “Data C” and “Data D”, respectively.

Access Port Connector

Table C-4 describes the access port connector pinouts.

Table C-4 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 **D**

Basic Phone Administration Steps

This appendix provides minimum, basic configuration steps for you to do the following:

- Add a new user to Cisco Unified Communications Manager Administration
- Configure a new phone for that user
- Associate that user to that phone
- Complete other basic end-user configuration tasks

The procedures provide one method for performing these tasks and are not the only way to perform these tasks. They are a streamlined approach to get a new user and corresponding phone running on the system.

These procedures are designed to be used on a mature Cisco Unified Communications Manager system where calling search spaces, partitions, and other complicated configuration have already been done and are in place for existing users.

This section contains these topics:

- [Example User Information for These Procedures, page D-1](#)
- [Adding a User to Cisco Unified Communications Manager, page D-2](#)
- [Configuring the Phone, page D-3](#)
- [Performing Final End User Configuration Steps, page D-6](#)

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: 6901
- 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 D-2](#)
- [Adding a User Directly to Cisco Unified Communications Manager, page D-2](#)

Adding a User From an External LDAP Directory

If you added a user to an LDAP Directory (a non-Cisco Unified Communications Server directory), you can immediately synchronize that directory to the Cisco Unified Communications Manager on which you are adding this same user and the user's phone by following these steps:

Procedure

-
- Step 1** Login to 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 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” section on page D-3](#).
-

Adding a User Directly to Cisco Unified Communications Manager

If you are not using an LDAP directory, you can add a user directly to Cisco Unified Communications Manager Administration by following these steps:

Procedure

-
- Step 1** Choose **User Management > End User**.
 - Step 2** Click **Add New**.
The End User Configuration window appears.
 - Step 3** 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 4 Click **Save**.

Proceed to the section [Configuring the Phone, page D-3](#).

Configuring the Phone

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

Procedure

- Step 1** From Cisco Unified Communications Manager administration, choose **Device > Phone**.
- Step 2** Click **Add New**.
- Step 3** Select the user's phone model from the Phone Type drop-down list, then click **Next**.
The Phone Configuration window appears.

On the Phone Configuration window, you can use the default values for most of the fields.

To configure the required fields and some key additional fields, follow these steps:

Procedure

- Step 1** For the required fields, possible values can be configured as follows:



Note The configuration is based on the example of user *johndoe*.

- 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 backside of 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 where you can enter a useful description. This will help you, if you need to search for information about this user.
- Device Pool—Choose the device pool for which you want to assign this phone. The device pool defines sets of common characteristics for devices, such as region, date/time group, 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 features on a phone and identifies the predetermined number to be dialed after pressing the feature button. To configure the Predetermined Number for a feature, navigate to the Phone Button Template of Cisco Unified IP Phone 6911. In the template, 1 is always assigned to the line, so the button number minus 1 is the predetermined number that is provided by your system administrator.



Note Phone button templates are defined on the Phone Button Template Configuration window of Cisco Unified Communications Manager Administration (**Device > Device Settings > Phone Button Template**). You can use the search field(s) in conjunction with the **Find** button to find all configured phone button templates and their current settings.

- Common Phone Profile—From the drop-down list, choose a common phone profile from the list of available common phone profiles.



Note Common Phone Profiles are defined on the Common Phone Profile Configuration window of Cisco Unified Communications Manager Administration (**Device > Device Settings > Common Phone Profile**). You can use the search field(s) in conjunction with the **Find** button to find all configured common phone profiles and their current settings.

- Calling Search Space—From the drop-down list, choose the appropriate calling search space (CSS). A calling search space comprises a collection of partitions (analogous to a collection of available phone books) that are searched to determine how a dialed number should be routed. The calling search space for the device and the calling search space for the directory number get used together. The directory number CSS takes precedence over the device CSS.



Note Calling Search Spaces are defined on the Calling Search Space Configuration window of Cisco Unified Communications Manager Administration (**Calling routing > Class of Control > Calling Search Space**). You can use the search field(s) in conjunction with the **Find** button to find all configured Calling Search Spaces and their current settings.

- Location—Choose the appropriate location for this Cisco Unified IP Phone.
- Owner User ID—From the drop-down list, choose the user ID of the assigned phone user.

- b. In the Protocol Specific Information pane of this window, choose a Device Security Profile from the drop-down list. To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. If the phone does not support security, choose a non-secure profile.

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



Note The security profile chosen should be based on the overall security strategy of the company.

- c. In the Extension Information pane of this window, check the Enable Extension Mobility box if this phone supports Cisco Extension Mobility.
- d. Click **Save**.

Step 2 Configure line settings:

- a. On the Phone Configuration window, click Line 1 on the left pane of the window. The Directory Number Configuration window appears.
- b. In the Directory Number field, enter a valid number that can be dialed.



Note This field should contain the same number that appears in the Telephone Number field on the User Configuration window.

Example: 26640 is the directory number of user John Doe in the example above.

- c. From the Route Partition drop-down list, choose the partition to which the directory number belongs. If you do not want to restrict access to the directory number, choose <None> for the partition.
- d. From the Calling Search Space drop-down list (Directory Number Settings pane of the Directory Number Configuration window), choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. The value that you choose applies to all devices that are using this directory number.
- e. In the Call Pickup and Call Forward Settings pane of the Directory Number Configuration window, choose the items (i.e. Forward All, Forward Busy Internal) and corresponding destinations to which calls should be sent.

Example: If you want incoming internal and external calls that receive a busy signal to be forwarded to the voice mail for this line, check the Voice Mail box next to the “Forward Busy Internal” and “Forward Busy External” items in the left column of the Call Pickup and Call Forward Settings pane.

- f. In the “Line 1 on Device...” pane of the Directory Number Configuration window, configure the following:
 - Display (Internal Caller ID field)—You can enter the first name and last name of the user of this device so that this name will be displayed for all internal calls. You can also leave this field blank to have the system display the phone extension.
 - External Phone Number Mask—Indicate phone number (or mask) that is used to send Caller ID information when a call is placed from this line.

You can enter a maximum of 24 number and "X" characters. The Xs represent the directory number and must appear at the end of the pattern.

Example: Using the John Doe extension in the example above, if you specify a mask of 408902XXXX, an external call from extension 6640 displays a caller ID number of 4089026640.



Note This setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the **Propagate Selected** button. (The check box at right displays only if other devices share this directory number.)

- g. Click **Save**.
- h. Click **Associate End Users** at the bottom of the window to associate a user to the line being configured. Use the **Find** button in conjunction with the Search fields to locate the user, then check the box next to the user's name, then click **Add Selected**. The user's name and user ID should now appear in the "Users Associated With Line" pane of the Directory Number Configuration window.
- i. Click **Save**. The user is now associated with Line 1 on the phone.
- j. If your phone has a second line, configure Line 2.
- k. Associate the user with the device:
 - Choose **User Management > End User**.
 - Use the search boxes and the Find button to locate the user you have added (i.e. *doe* for the last name).
 - Click on the user ID (that is, *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 D-6](#).

Performing Final End User Configuration Steps

If you are not already on the End User Configuration page, choose **User Management > End User** to perform some final configuration tasks. Use the Search fields and the Find button to locate the user (i.e. John Doe), then click on the user ID to get to the End User Configuration window for the user.

In the End User configuration window, do the following:

Procedure

- Step 1** In the Directory Number Associations pane of the screen, set the primary extension from the drop-down list.
- Step 2** In the Mobility Information pane, check the Enable Mobility box.
- Step 3** In the Permissions Information pane, use the User Group buttons to add this user to any user groups. For example, you may want to add the user to a group that has been defined as a "Standard CCM End User Group."

To view all configured user groups, choose **User Management > User Group**.

Step 4 Click **Save**.



APPENDIX **E**

Installing the Wall Mount for the Cisco Unified IP Phone 6901 and 6911

This appendix contains information on installing the wall mount for use with the Cisco Unified IP Phone 6901 and 6911 phones.

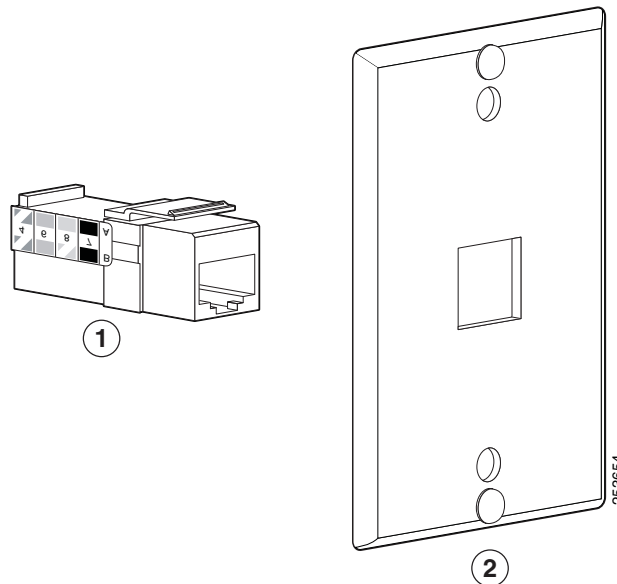
Installing a Wall Mount for the Cisco Unified IP Phone 6901

The following section describes how to install the Wall Mount plate for use with the Cisco Unified IP Phone 6901.

Cisco recommends that you use the Leviton Wall Mount plate (Leviton type number: 4108W-0SP) for mounting the Cisco Unified IP Phone 6901. The wall mount plate must be ordered separately from the phone.

[Figure E-1](#) shows a list of items required to mount the Cisco Unified IP Phone 6901 on the wall using the Leviton Wall Mount plate.

Figure E-1 **Leviton Wall Mount Plate**

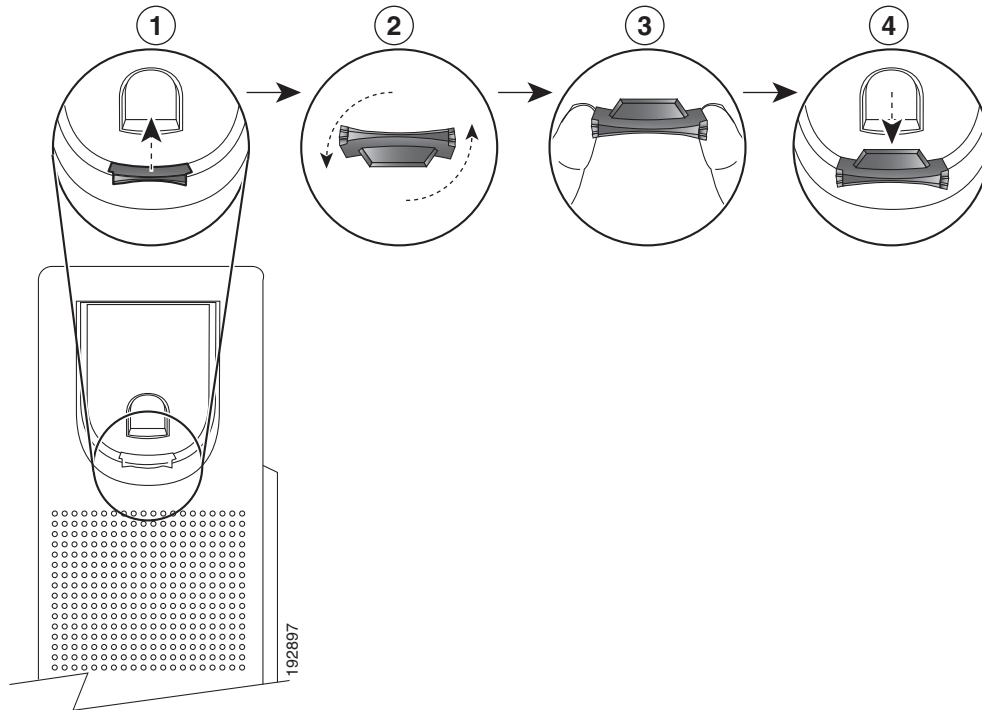


1	RJ45 Connector	2	Leviton Wall Mount Plate
----------	----------------	----------	--------------------------

Before You Begin

Before you mount the phone on the wall, ensure that the handset rest is such that the receiver will not slip out of the cradle (Figure E-2).

Figure E-2 Preparing the Handset Hookswitch



1	Remove the handset from the cradle and pull the plastic tab from the handset rest.
2	Rotate the tab 180 degrees.
3	Hold the tab between two fingers, with the corner notches facing you. Make sure the tab lines up evenly with the slot in the handset cradle. (Figure E-2).
4	Press the tab evenly into the slot. An extension protrudes from the top of the rotated tab. Return the handset to the handset rest.

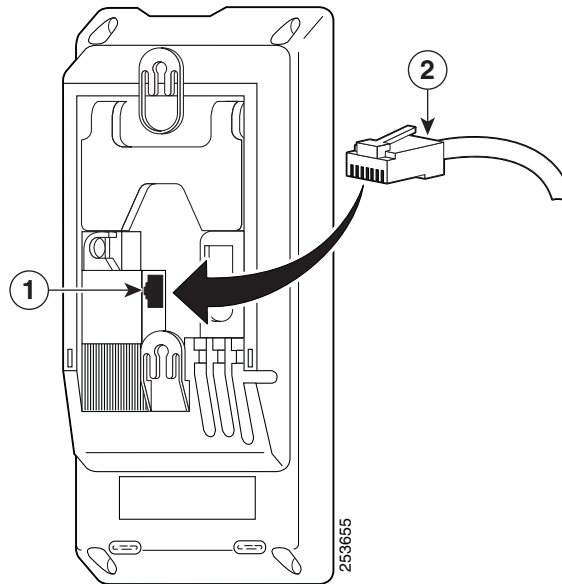
Installing the Phone on Wall Mount Plate

To install the phone on the wall mount plate, follow these steps:

Procedure

- Step 1** Plug the telephone line cord (RJ45 connector) into the phone jack at the base of the phone (Figure E-3).

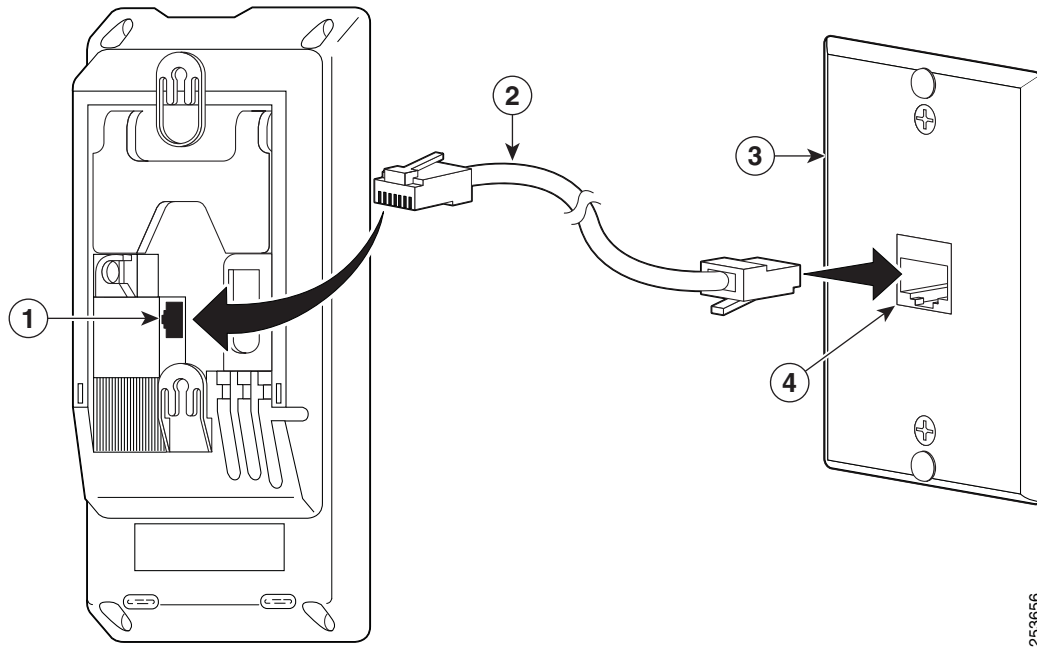
Figure E-3 RJ45 Connector in the Phone Jack



1	Network Port on the Phone
2	RJ45 Connector

Step 2 Plug the RJ45 connector into the wall mount phone jack (Figure E-4).

Figure E-4 RJ45 Connector in the Wall Mount Jack

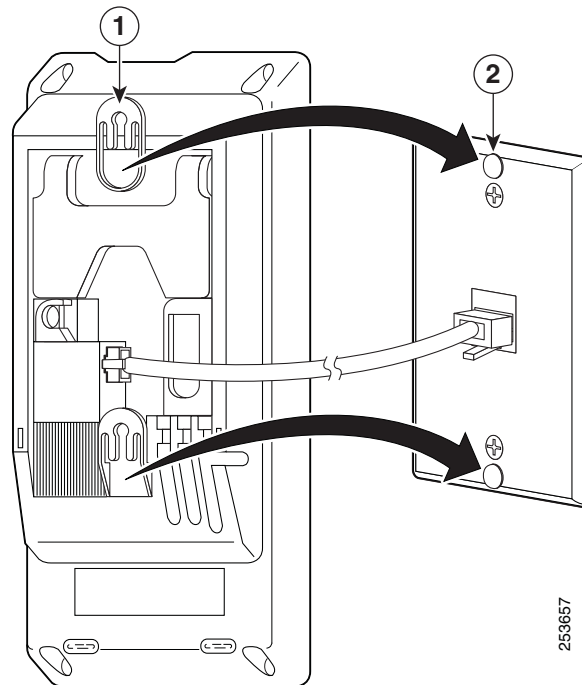


253656

1	Network Port on the Phone	3	Wall Mount Plate
2	RJ45 Connector	4	Network Port on the Wall Mount Plate

Step 3 Slip the mounting holes on the base of the wall mount plate and over the wall mount pins (Figure E-5).

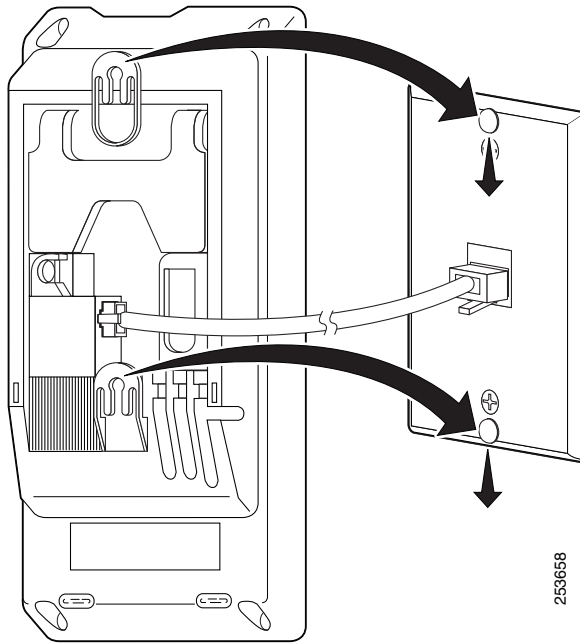
Figure E-5 Mounting Holes



1	Mounting Hole on the Phone
2	Wall Mount Pin on the Wall Mount Plate

Step 4 Firmly slide the IP phone down into place (Figure E-6).

Figure E-6 Sliding the IP Phone

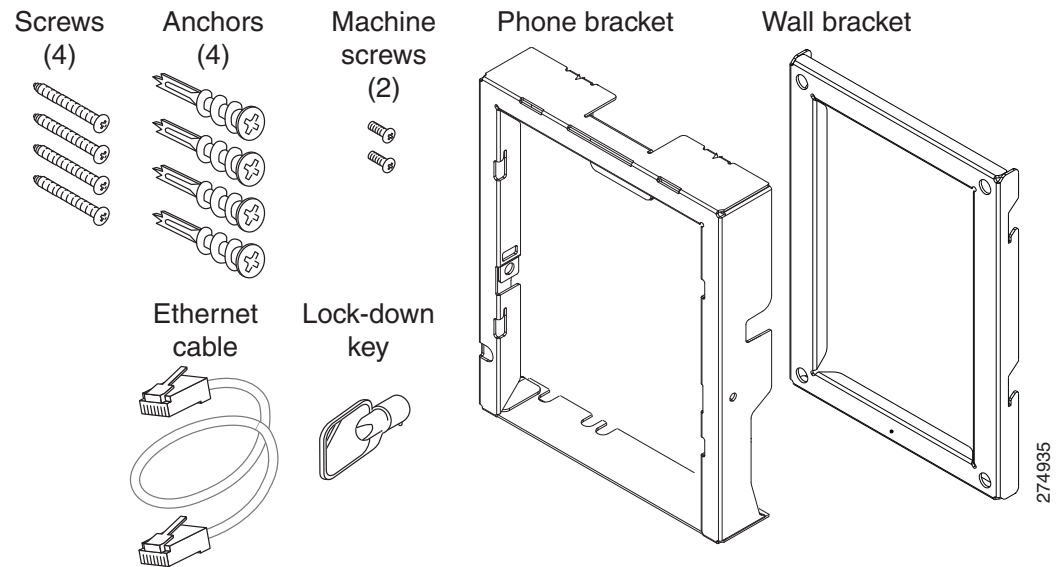


Installing a Wall Mount for the Cisco Unified IP Phone 6911

The following section describes how to install the wall mount for use with the Cisco Unified IP Phone 6911.

Figure E-7 shows a list of items included in the Wall Mount Kit for the Cisco Unified IP Phone 6911.

Figure E-7 Wall Mount Kit for Cisco Unified IP Phone 6911



The package includes the following items:

- One phone bracket
- One wall bracket
- Four 10-12x1 inch Phillips-head screws with 4 anchors
- Two 4-40x1/4 inch machine screws
- One six-inch Ethernet cable
- One key if the bracket includes the optional lock

Before You Begin

You will need these tools to install the bracket:

- #1 and #2 Phillips-head screwdrivers
- Level

You must also install an Ethernet jack for the telephone in the desired location if an Ethernet jack does not currently exist. This jack must be wired appropriately for an Ethernet connection. You cannot use a regular telephone jack. For more information on phone installation requirements and warnings, see the [Setting Up the Cisco Unified IP Phone](#) chapter.

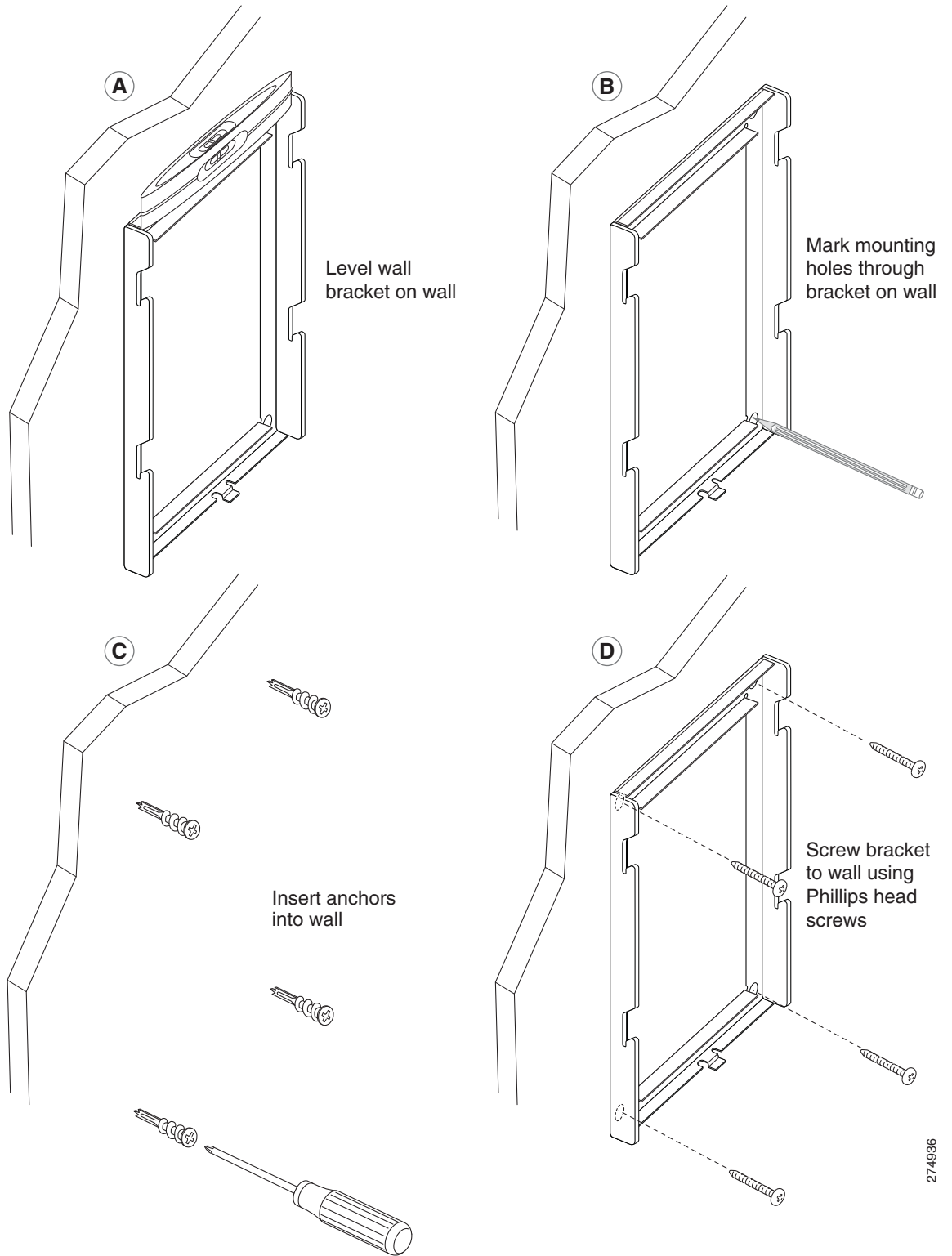
Installing the Bracket

To install the phone on the wall, follow these steps:

Procedure

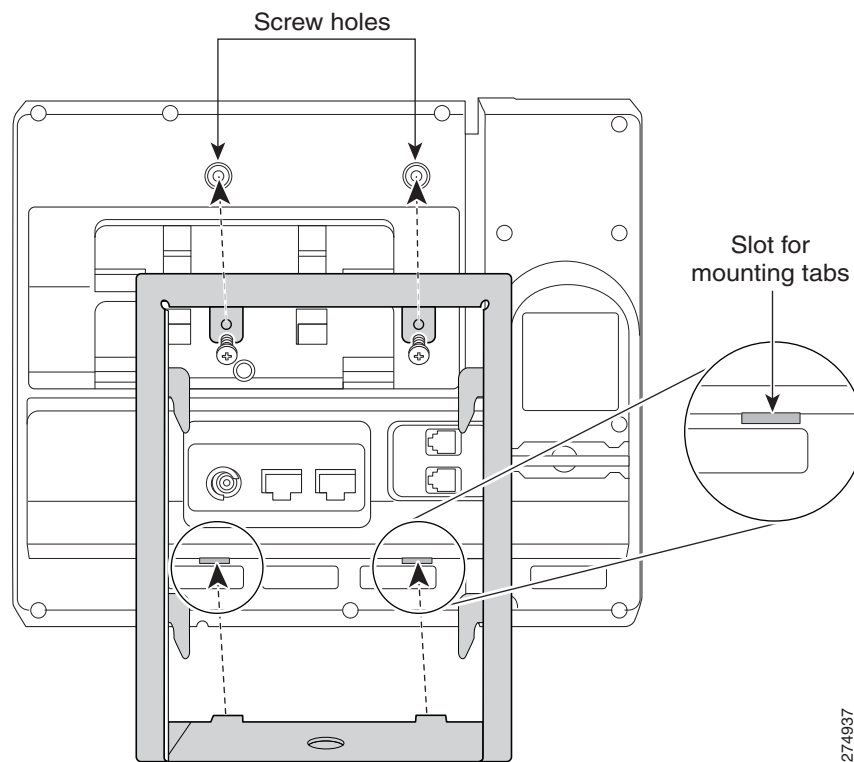
-
- Step 1** Mount the wall bracket in the desired location ([Figure E-8](#)). You can install the wall bracket over an Ethernet jack, or you can run the Ethernet network cable to a jack nearby.
- a. Use the Level to ensure the wall bracket is level, then use a pencil to mark the screw holes.
 - b. Using a #2 Phillips-head screwdriver, carefully center the anchor over the pencil mark and press the anchor into the wall to make markings on the wall.
 - c. Screw the anchor clockwise into the wall until it is seated flush.
 - d. Use the included screws and a #2 Phillips-head screwdriver to attach the wall bracket to the wall.

Figure E-8 Mounting the Wall Bracket



- Step 2** Attach the phone bracket to the IP phone ([Figure E-9](#)).
- a. Detach the handset cord (and headset cord, if there is a headset), power cord, and any other attached cords from the base of the phone.
 - b. Remove the label covers that are concealing the screw holes.
 - c. Attach the phone bracket by inserting the tabs into the mounting tabs on the phone. The phone's ports should be accessible through the holes in the bracket.
 - d. Secure the phone bracket to the IP Phone with the Phillips-head screws.
 - e. Thread the handset cord (and headset cord, if using one). Reattach the cords and seat them in the clips incorporated into the phone body.

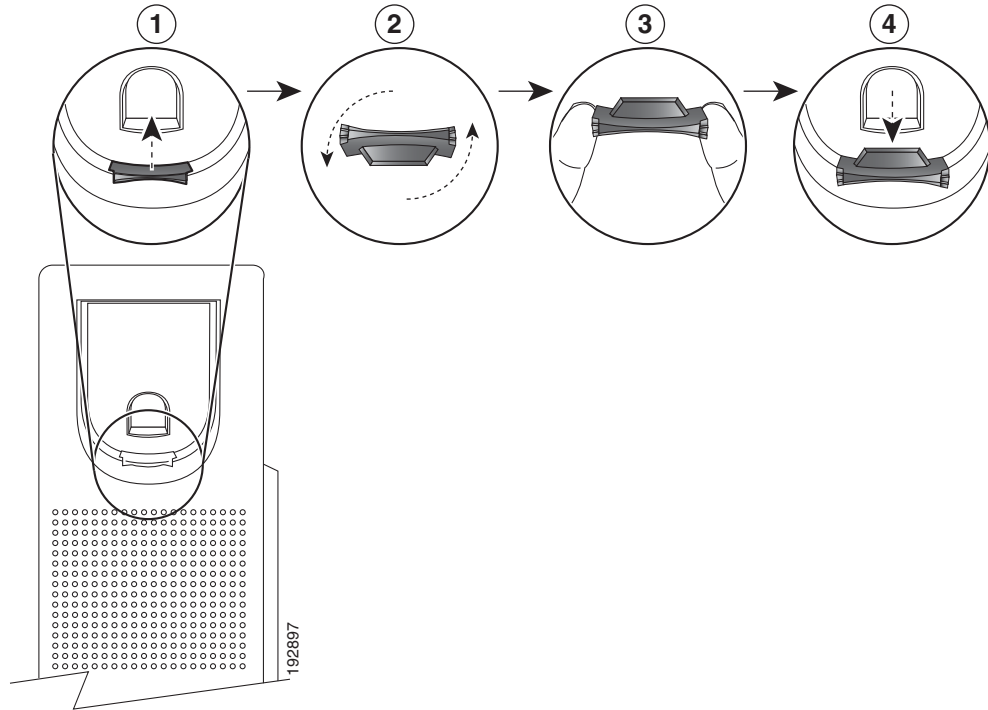
Figure E-9 Attaching the Phone Bracket



274937

- Step 3** Remove the handset wall hookswitch in the handset rest, rotate the hookswitch by 180 degrees, and reinsert the hookswitch. The hookswitch should have a lip on which the handset catches when the phone is vertical (Figure E-10).

Figure E-10 Preparing the Handset Hookswitch

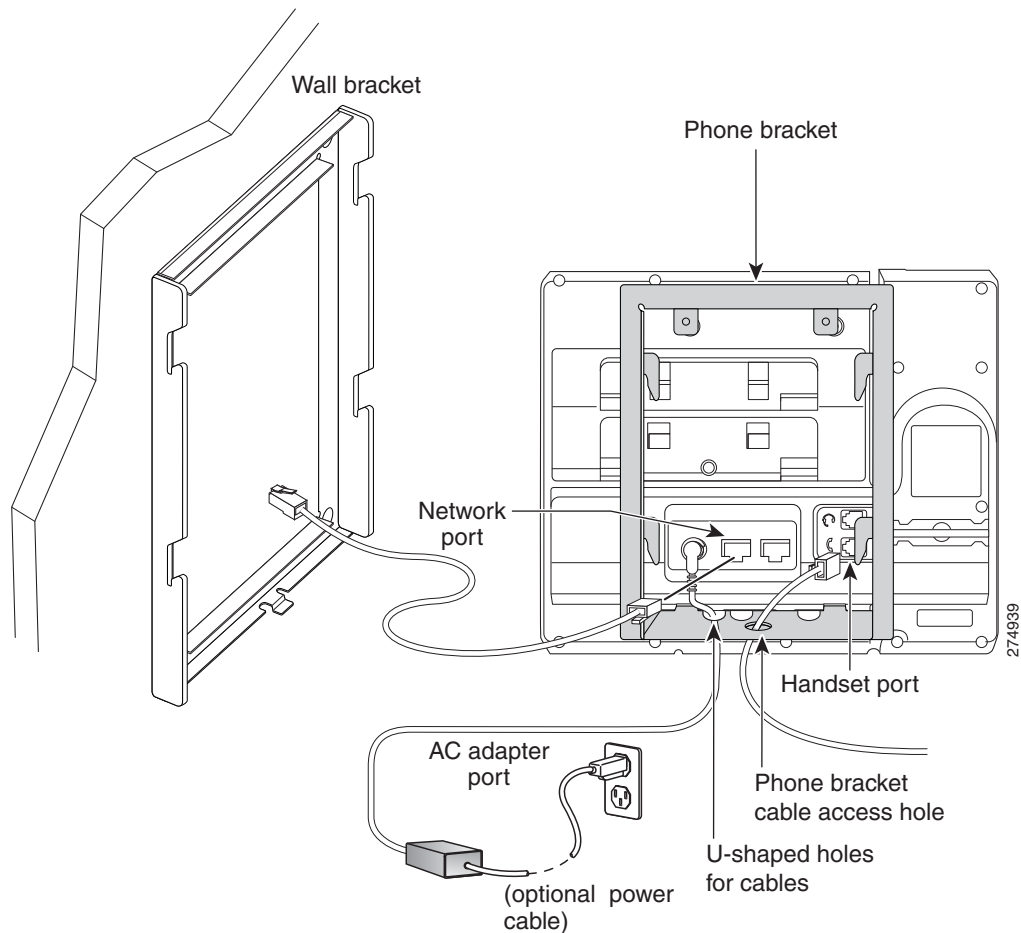


Step 4 Attach the Ethernet cable to the 10/100 SW network port and wall jack.

If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100 PC access port.

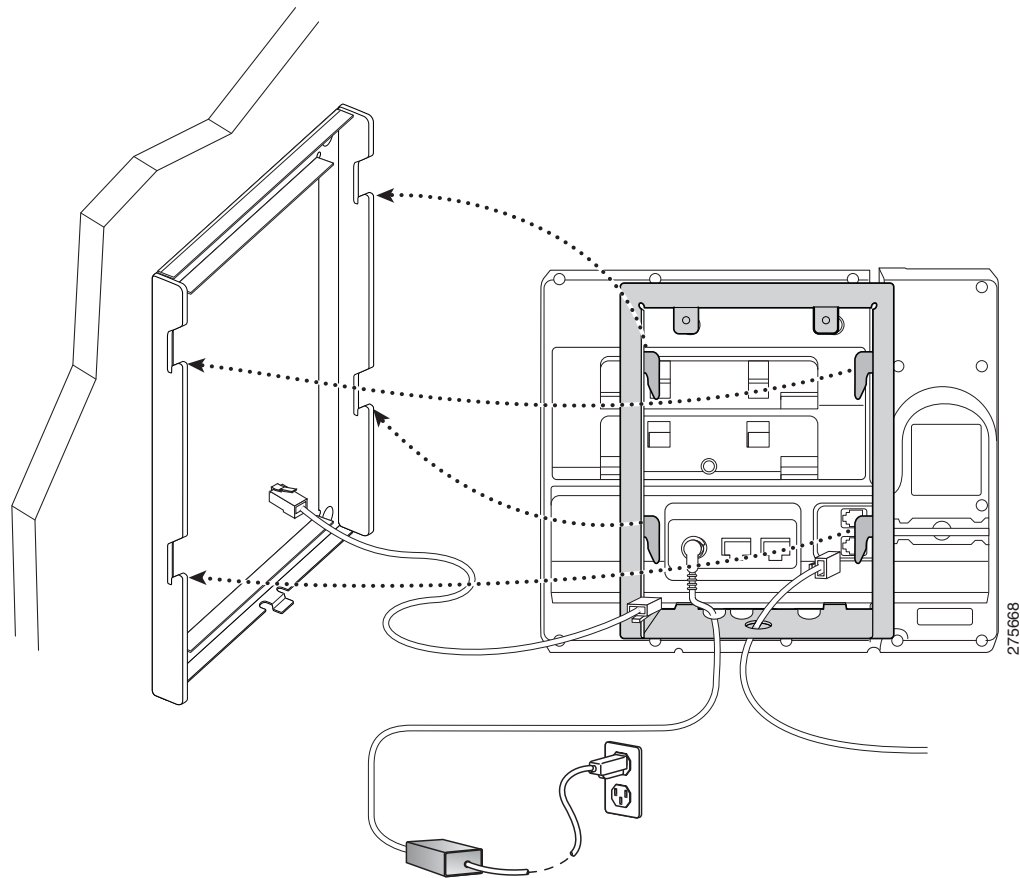
If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips incorporated into the phone body next to the 10/100 PC port (Figure E-11).

Figure E-11 Attaching the Cables



- Step 5** Attach the phone to the wall bracket by inserting the tabs on the top of the phone bracket into the slots on the wall bracket. Ensure that the power cord and any other cable that does not terminate in the wall behind the bracket are positioned in one of the cable-access openings in the bottom of the bracket. The phone and wall brackets' openings together form circular openings with room for one cable per opening (Figure E-12).
- Step 6** Use the locking key to lock the phone to the wall bracket.

Figure E-12 Attaching the Phone to the Wall Bracket





APPENDIX **F**

Cisco Unified IP Phone Non-Lockable Wall Mount

This appendix contains information on installing the following product:

- ADA Non-Lockable Wall Mount Kit for 6900 Series: Installed on the Cisco Unified IP Phone 6911, 6921, 6941, 6945, and 6961.

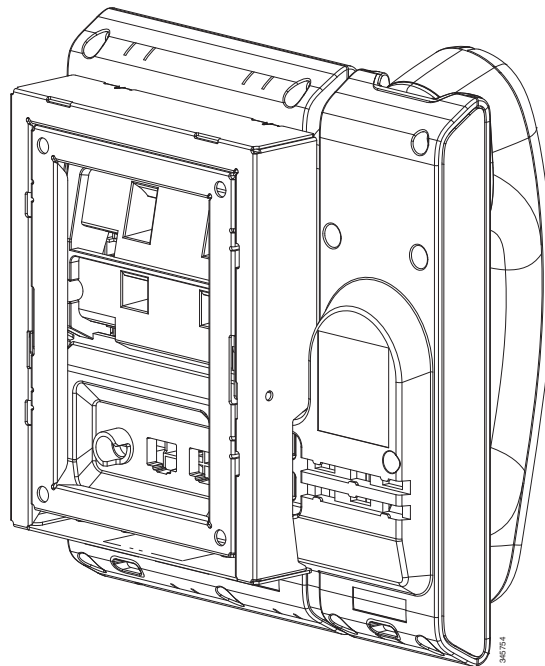
This nonlocking wall mount kit meets ADA 4.4.1 requirements.

ADA Non-Lockable Wall Mount Kit for 6900 Series

This section describes how to install the ADA Non-Lockable Wall Mount Kit for 6900 Series on a Cisco Unified IP Phone 6911, 6921, 6941, 6945, and 6961.

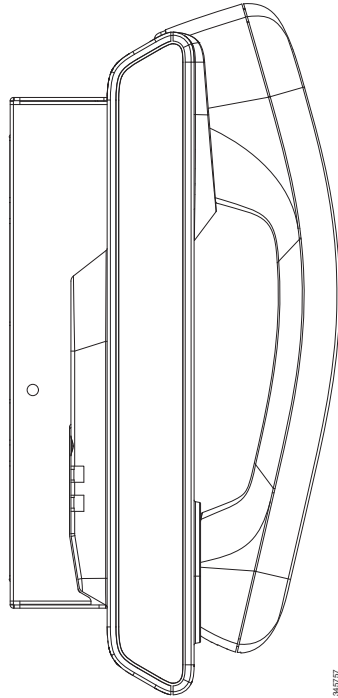
The following figure shows the wall mount kit installed on the phone.

Figure F-1 Back View of ADA Non-Lockable Wall Mount Kit Installed on Phone



The following figure shows the phone with the wall mount kit from the side.

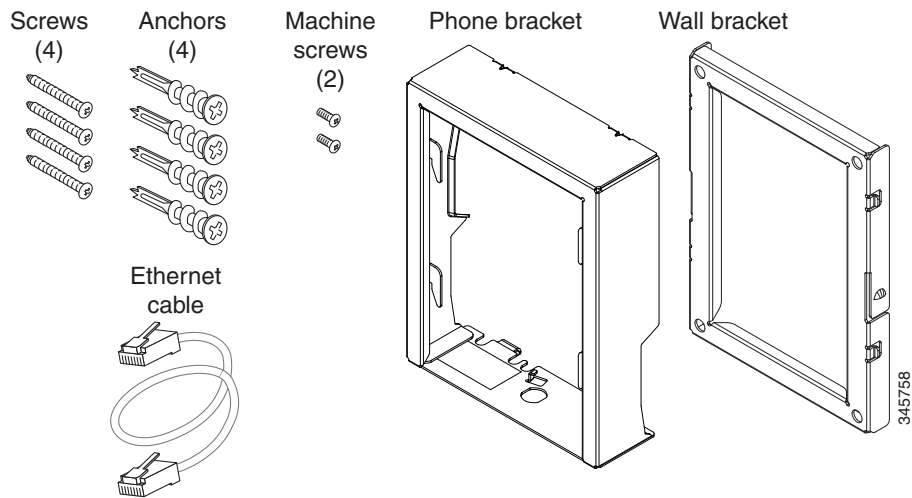
Figure F-2 Side View of ADA Non-Lockable Wall Mount Kit Installed on Phone



Components

The following figure shows the contents of the Wall Mount kit.

Figure F-3 Components



The package includes these items:

- One phone bracket
- One wall bracket
- Four #8-18 x 1.25-inch Phillips-head screws with four anchors
- Two M2.5 x 6 mm machine screws
- One 6-inch Ethernet cable

Before You Begin

You need these tools to install the bracket:

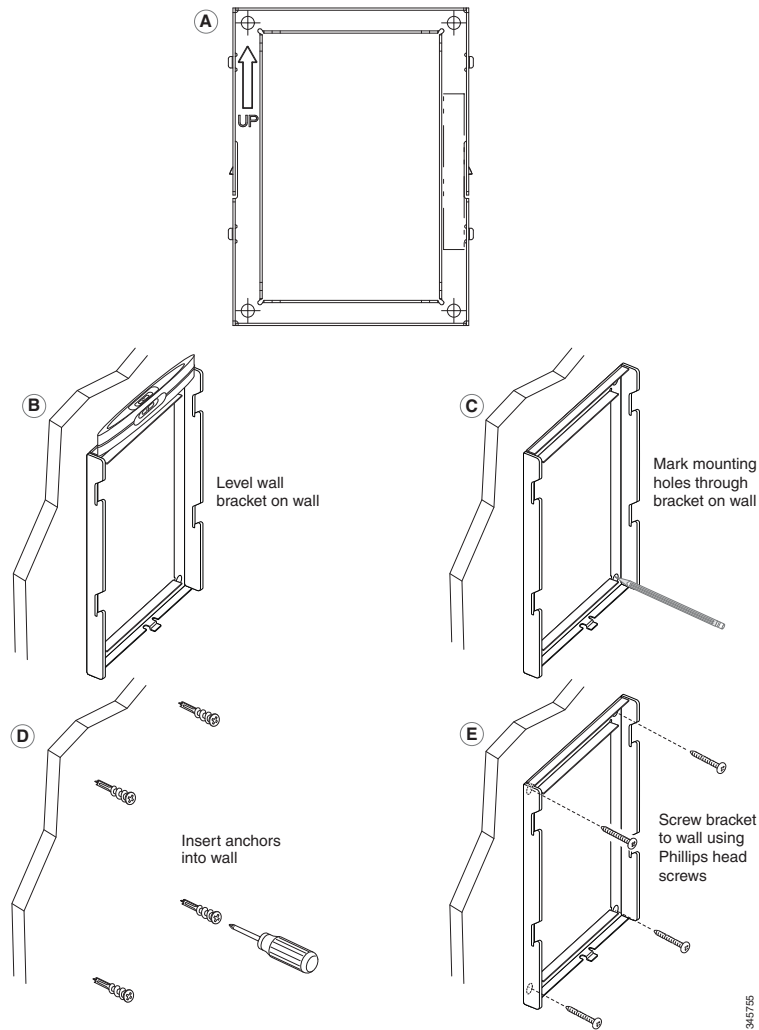
- #1 and #2 Phillips-head screwdrivers
- Level
- Pencil

You must also install an Ethernet jack for the telephone in the desired location if an Ethernet jack does not currently exist. This jack must be wired appropriately for an Ethernet connection. You cannot use a regular telephone jack. For more information about phone installation requirements and warnings, see [Setting Up the Cisco Unified IP Phone, page 3-1](#).

Install Non-Lockable Wall Mount Kit for Phone

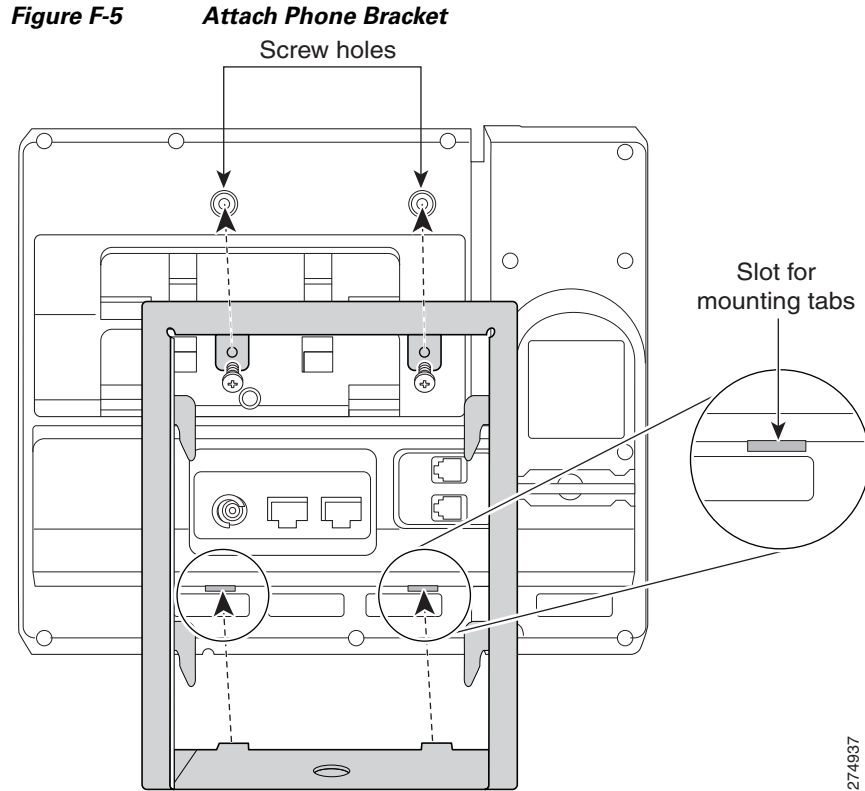
-
- Step 1** Mount the wall bracket in the desired location. You can install the bracket over an Ethernet jack, or you can run the Ethernet network cable to a jack nearby.
- a. Hold the bracket on the wall, placing it so that the arrow on the back of the bracket is pointing up.
 - b. Use the level to ensure the bracket is level and use a pencil to mark the screw holes.
 - c. Use a #2 Phillips-head screwdriver to carefully center the anchor over the pencil mark and press the anchor into the wall.
 - d. Screw the anchor clockwise into the wall until it is seated flush.
 - e. Use the included screws and a #2 Phillips-head screwdriver to attach the bracket to the wall.

The following figure shows the steps to mount the wall bracket.

Figure F-4 *Mount the Wall Bracket***Step 2** Attach the phone bracket to the IP phone.

- a. Detach the handset cord (and headset cord, if there is a headset), power cord, and any other attached cords from the base of the phone.
- b. Remove the label covers that are concealing the screw holes.
- c. Attach the phone bracket by inserting the tabs into the mounting tabs on the phone. The phone ports should be accessible through the holes in the bracket.
- d. Secure the phone bracket to the IP Phone with the machine screws.
- e. Thread the handset cord (and headset cord, if using one). Reattach the cords and seat them in the clips incorporated into the phone body.

The following figure shows how to attach the phone bracket.

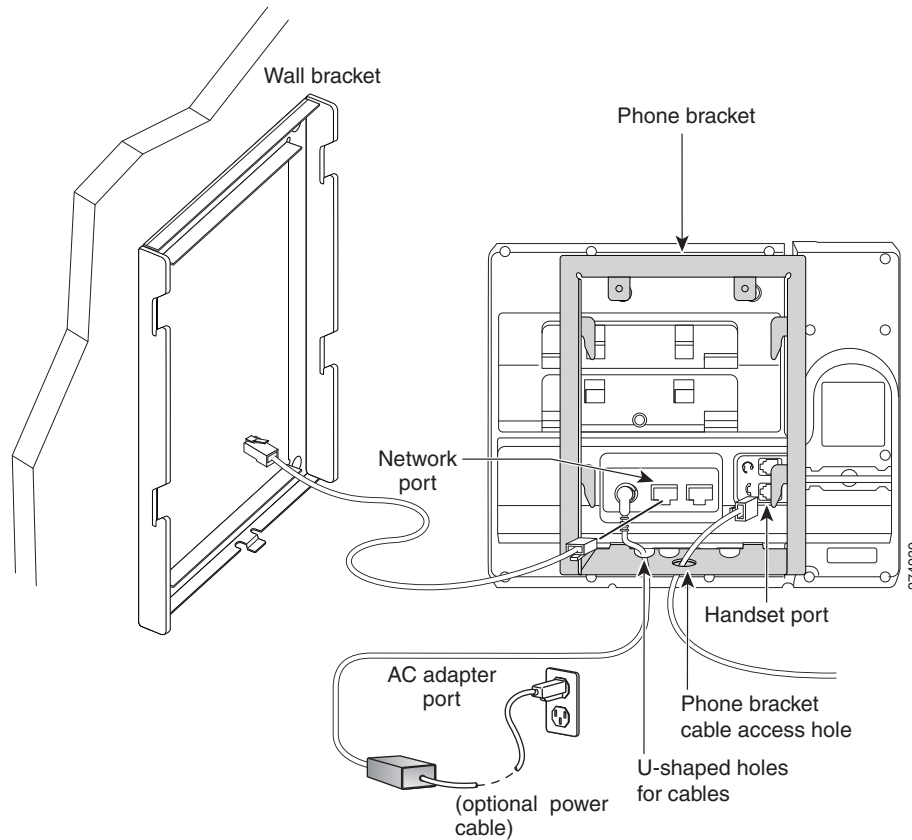


Step 3 Attach the cables.

- a. Attach the Ethernet cable to the 10/100 SW network port and wall jack.
- b. (Optional) If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100 PC access port.
- c. (Optional) If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips incorporated into the phone body next to the 10/100 PC port.

The following figure shows the cable attachment.

Figure F-6 Attach Cables



- Step 4** Attach the phone to the wall bracket by inserting the tabs on the top of the phone bracket into the slots on the wall bracket.

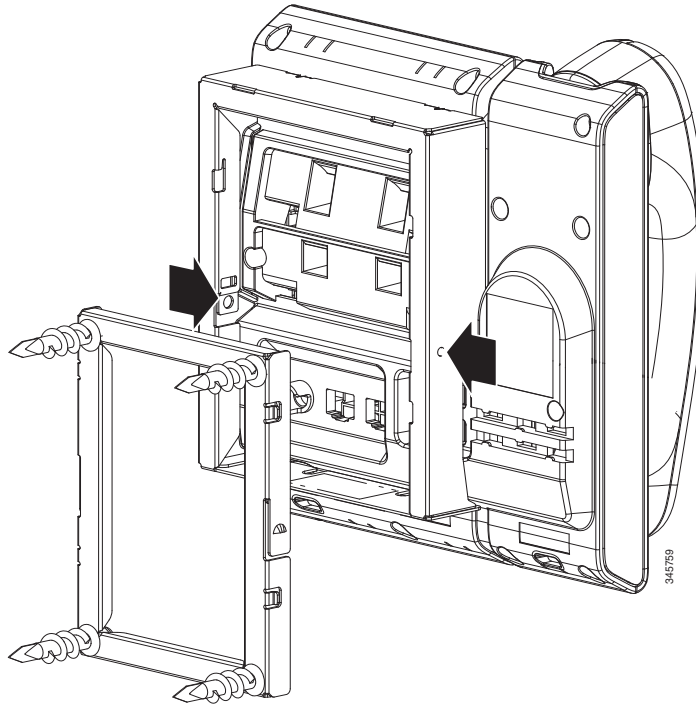
Use the cable-access openings in the bottom of the bracket to position the power cord and any other cable that does not terminate in the wall behind the bracket. The phone and wall bracket openings together form circular openings with room for one cable per opening.

- Step 5** Proceed to [Before You Begin, page E-2](#).

Remove Phone from Non-Lockable Wall Mount

The phone mounting plate contains two tabs to lock the plate into the wall bracket. The following figure shows the location and shape of the tabs.

The following figure shows the tab location.

Figure F-7 **Tab Location**

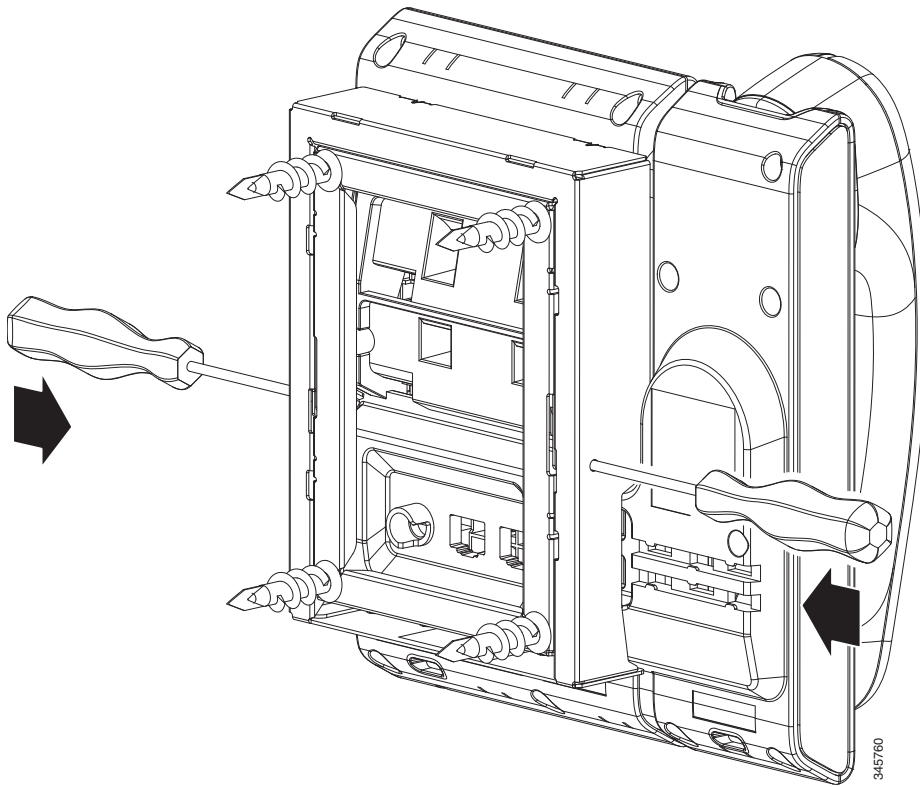
To remove the phone and mounting plate from the wall bracket, you must disengage these tabs.

Before You Begin

You require two screwdrivers or metal sticks.

-
- Step 1** Push the screw drivers into the left and right holes in the phone mounting plate approximately 1 in. (2.5 cm).
- Step 2** Press firmly inwards (towards the phone) to disengage the tabs, lift up on the phone to release the phone from the wall bracket, and then pull the phone towards you.

The following figure shows how to disengage the tabs.

Figure F-8 Disengage tabs



APPENDIX **G**

Feature Support by Protocol for the Cisco Unified IP Phone 6901 and 6911

This appendix provides information about feature support for the Cisco Unified IP Phones 6901 and 6911 using the SCCP or SIP protocol with Cisco Unified Communications Manager Release 8.5(1).

[Table G-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, refer to the Cisco Unified IP Phone user guide.

The guide is available at this URL:

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

The specific sections that describe the features in the phone guide are referenced in [Table G-1](#).

Table G-1 Cisco Unified IP Phones Feature Support by Protocol

Features	Protocol		For More Information
	SCCP	SIP	
Calling Features			
Agent Greeting	Supported	Supported	Basic Call Handling—Answering a Call
Audible Message Waiting Indicator (AMWI)	Supported	Supported	Accessing Voice Messages
Auto Answer (Cisco Unified IP Phone 6911 only)	Supported	Supported	Using a Handset, Headset, and Speakerphone—Using Auto Answer
Automatic Port Synchronization (Cisco Unified IP Phone 6911 only)	Supported	Supported	
cBarge	Supported	Supported	Advanced Call Handling—Using a Shared Line
Block external to external transfer	Supported	Supported	
Call Back	Supported	Supported	Basic Call Handling—Placing a Call: Additional Options

Table G-1 Cisco Unified IP Phones Feature Support by Protocol (continued)

Features	Protocol		For More Information
	SCCP	SIP	
Calling Features			
Call Forward All	Supported	Supported	Basic Call Handling—Forwarding Calls to Another Number
Call Forward All Breakout	Supported	Supported	
Call Forward All Loop Prevention	Supported	Supported	
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 Pickup/Group Call Pickup (Cisco Unified IP Phone 6911 only)	Supported	Supported	Advanced Call Handling—Picking Up a Redirected Call on Your Phone”
Call Waiting	Supported	Supported	Basic Call Handling—Answering a Call
Client Matter Codes (CMC)	Supported	Not supported	Basic Call Handling—Placing a Call: Additional Options
Forced Authorization Codes (FAC)	Supported	Not supported	Basic Call Handling—Placing a Call: Additional Options
Group Call Pickup (Cisco Unified IP Phone 6911 only)	Supported	Supported	
Hold/Resume	Supported	Supported	Basic Call Handling—Using Hold and Resume
Meet-Me Conference (Cisco Unified IP Phone 6911 only)	Supported	Supported	Basic Call Handling—Making Conference Calls
Message Waiting Indicator	Supported	Supported	
Music on Hold	Supported	Supported	
Mute (Cisco Unified IP Phone 6911 only)	Supported	Supported	Basic Call Handling—Using Mute
Ringer Volume Control	Supported	Supported	
Plus Dialing	Supported	Supported	Using Call Logs
Private Line Automated Ringdown (PLAR)	Supported	Supported	

Table G-1 Cisco Unified IP Phones Feature Support by Protocol (continued)

Features	Protocol		For More Information
	SCCP	SIP	
Calling Features			
Redial	Supported	Supported	Basic Call Handling—Placing a Call: Basic Options
Shared Line	Supported	Supported	Advanced Call Handling—Using a Shared Line
Monitoring and Recording (Cisco Unified IP Phone 6911 only)	Supported	Supported	
Speed Dialing (Cisco Unified IP Phone 6911 only)	Supported	Supported	Advanced Call Handling—Speed Dialing
Time-of-Day Routing	Supported	Supported	
Transfer	Supported	Supported	Basic Call Handling—Transferring Calls
Voice Mail	Supported	Supported	Accessing Voice Messages section of the Phone Guide





INDEX

Numerics

802.1X

- authentication server [1-18](#)
- authenticator [1-18](#)
- description [1-7](#)
- network components [1-18](#)
- supplicant [1-18](#)

A

AC adapter, connecting to [3-4](#)

access port

- connecting [3-4](#)
- forwarding packets to [6-7](#)
- purpose [3-3](#)

adding

- Cisco Unified IP Phones manually [2-10](#)
- Cisco Unified IP Phones using auto-registration [2-8](#)
- users to Cisco Unified Communications Manager [5-8](#)

AdvanceAdhocConference service parameter [5-5](#)

agent greeting [5-2, G-1](#)

Audible message waiting indicator [G-1](#)

audible message waiting indicator [5-2](#)

authenticated call [1-15](#)

authentication [1-10, 3-10](#)

authentication server, in 802.1X [1-18](#)

authenticator, in 802.1X [1-18](#)

auto answer [5-2, G-1](#)

automatic port synchronization [5-3](#)

auto-registration

- using [2-8](#)

auxiliary VLAN [2-3](#)

B

barge [G-1](#)

- call security restrictions [1-16](#)

block external to external transfer [5-3, G-1](#)

buttons

- Cisco Unified IP Phone 6911
 - programmable feature [1-5](#)

C

call

- authenticated [1-15](#)
- encrypted [1-15](#)
- security interactions [1-16](#)

call back [G-1](#)

call forward [5-3](#)

- all breakout [G-2](#)

all calls [G-2](#)

all loop prevention [G-2](#)

busy [G-2](#)

call forward all [5-3](#)

call forward busy [5-3](#)

call forward no answer [5-3](#)

call forward no coverage [5-3](#)

configurable display [G-2](#)

destination override [5-4, G-2](#)

loop breakout [5-4](#)

loop prevention [5-4](#)

no answer [G-2](#)

call forward destination override [5-4](#)

call pickup [G-2](#)

call security restrictions using Barge [1-16](#)

- call waiting [5-4, G-2](#)
 - CAPF (Certificate Authority Proxy Function) [1-14](#)
 - cell phone interference [1-1](#)
 - Cisco Discovery Protocol
 - See CDP
 - Cisco Unified Communications Manager
 - adding phone to database of [2-7](#)
 - interactions with [2-2](#)
 - required for Cisco Unified IP Phones [3-2](#)
 - Cisco Unified Communications Manager Administration
 - adding telephony features using [5-1](#)
 - Cisco Unified IP Phone
 - adding manually to Cisco Unified Communications Manager [2-10](#)
 - adding to Cisco Unified Communications Manager [2-7](#)
 - cleaning [7-13](#)
 - configuration checklist [1-21](#)
 - configuration requirements [1-19](#)
 - installation checklist [1-23](#)
 - installation overview [1-19, 1-23](#)
 - installation requirements [1-19](#)
 - mounting to wall [3-9](#)
 - power [2-3](#)
 - registering [2-7](#)
 - registering with Cisco Unified Communications Manager [2-8](#)
 - resetting [7-10](#)
 - technical specifications [C-1](#)
 - web page [6-1](#)
 - Cisco Unified Video Advantage [5-4](#)
 - cleaning the Cisco Unified IP Phone [7-13](#)
 - client matter codes [5-5, G-2](#)
 - computer telephony integration [5-5](#)
 - conference [5-5](#)
 - conference button, description of [1-4](#)
 - conference joining [5-5](#)
 - configuration file
 - creating [7-4](#)
 - encrypted [1-14](#)
 - overview [2-5](#)
 - XmlDefault.cnf.xml [2-5](#)
 - configuring
 - overview [1-19](#)
 - user features [5-8](#)
 - connecting
 - handset [3-4](#)
 - headset [3-4](#)
 - to AC adapter [3-4](#)
 - to a computer [3-4](#)
 - to the network [3-4](#)
 - connecting IP phones to other IP phones (daisy chaining) [7-8](#)
 - CTI application [5-5](#)
 - CUVA [5-4](#)
-
- D**
- data VLAN [2-3](#)
 - Debug Display web page [6-10](#)
 - Default Router 1-5 [4-2](#)
 - device authentication [1-13](#)
 - Device Information web page [6-2, 6-3](#)
 - DHCP [4-1](#)
 - description [1-6](#)
 - troubleshooting [7-6](#)
 - DHCP IP address [7-9](#)
 - directory numbers, assigning manually [2-10](#)
 - DNS server
 - troubleshooting [7-7](#)
 - documentation
 - additional [2-viii](#)
-
- E**
- encrypted call [1-15](#)
 - encrypted configuration files [1-14](#)
 - encryption [1-10](#)
 - media [1-14](#)

enterprise parameters

- call forward options [5-11](#)
- call forward optionsenterprise parameters
 - user options web page defaults [5-11](#)
- user options web page defaults [5-11](#)

error messages, used for troubleshooting [7-3](#)

Ethernet Information web page [6-2, 6-7](#)

external power [2-4](#)

F

feature buttons

- Conference [1-4](#)
- Hold [1-4](#)
- Messages [1-5](#)
- mute [1-5](#)
- Programmable line button [1-5](#)
- Speakerphone [1-5](#)
- Transfer [1-4](#)

features

- configuring on phone, overview [1-10](#)
- configuring with Cisco Unified Communications Manager, overview [1-9](#)
- informing users about, overview [1-10](#)
- support by protocol
 - Audible message waiting indicator [G-1](#)
 - auto answer [G-1](#)
 - barge [G-1](#)
 - block external to external transfer [G-1](#)
 - call back [G-1](#)
 - call forward all breakout [G-2](#)
 - call forward all calls [G-2](#)
 - call forward all loop prevention [G-2](#)
 - call forward busy [G-2](#)
 - call forward configurable display [G-2](#)
 - call forward destination override [G-2](#)
 - call forward no answer [G-2](#)
 - call pickup [G-2](#)
 - call waiting [G-2](#)

- client matter codes [G-2](#)
- forced authorization codes [G-2](#)
- group call pickup [G-2](#)
- hold [G-2](#)
- meet-me conference [G-2](#)
- message waiting [G-2](#)
- monitoring and recording [G-3](#)
- music-on-hold [G-2](#)
- mute [G-2](#)
- Private Line Automated Ringdown (PLAR) [G-2](#)
- redial [G-3](#)
- shared line [G-3](#)
- speed dialing [G-3](#)
- Time-of-Day Routing [G-3](#)
- transfer [G-3](#)
- voice mail [G-3](#)

file authentication [1-13](#)

footstand [3-7](#)

forced authorization codes [5-5, G-2](#)

G

G [1-1](#)

- G.711 μ [1-1](#)
- G.711a [1-1](#)
- G.722 [1-1](#)
- G.729 [1-1](#)
- G.729a [1-1](#)
- G.729ab [1-1](#)
- group call pickup [5-5, G-2](#)

H

handset [1-6](#)

- connecting [3-4](#)
- light strip [1-3, 1-4](#)

headset port [3-4](#)

hold [5-5, G-2](#)

hold button, description of [1-2, 1-4](#)

hookswitch [1-2](#)

HTTP, description [1-6](#)

Hypertext Transfer Protocol

See HTTP

I

icon

shield [1-10](#)

image authentication [1-13](#)

installing

Cisco Unified Communications
Manager configuration [3-2](#)

network requirements [3-1](#)

preparing [2-7](#)

requirements, overview [1-19](#)

interference, cell phone [1-1](#)

Internet Protocol (IP) [1-7](#)

IP Address [4-1](#)

IP address, troubleshooting [7-3](#)

K

keypad, description of [1-3, 1-5](#)

L

light strip [1-3, 1-4](#)

line button, description of [1-3](#)

Locale Installer [B-1](#)

localization

Installing the Cisco Unified Communications Manager
Locale Installer [B-1](#)

M

MAC address [2-12](#)

manufacturing installed certificate (MIC) [1-13](#)

media encryption [1-14](#)

meet me conference [5-6](#)

meet-me conference [G-2](#)

Message Indicators [1-24](#)

messages button, description of [1-5](#)

message waiting [5-6, G-2](#)

Message Waiting Indicator (MWI) [1-24](#)

Message Waiting Lamp [1-24](#)

MIC [1-13](#)

monitoring and recording [5-7, G-3](#)

music-on-hold [5-6, G-2](#)

mute [5-6](#)

feature [G-2](#)

mute button, description of [1-5](#)

N

native VLAN [2-3](#)

Network Configuration menu

options

CDP on PC port [6-7](#)

CDP on switch port [6-7](#)

Default Router 1-5 [4-2](#)

DHCP [4-1](#)

IP Address [4-1](#)

Subnet Mask [4-2](#)

TFTP Server 1 [4-2](#)

Network Configuration web page [6-2, 6-4](#)

network connections, access port [3-3](#)

network connectivity, verifying [7-3](#)

networking protocol

802.1X [1-7](#)

CDP [1-6](#)

DHCP [1-6](#)

HTTP [1-6](#)

IP [1-7](#)

RTCP [1-7](#)

RTP [1-7](#)

SCCP [1-8](#)

SIP [1-8](#)

TCP [1-8](#)

TFTP [1-8](#)

TLS [1-8](#)

UDP [1-8](#)

network outages, identifying [7-6](#)

network port

connecting to [3-4](#)

network requirements, for installing [3-1](#)

network statistics [6-7](#)

Network web page [6-2, 6-7](#)

O

on hook call transfer [5-6](#)

P

phone hardening [1-14](#)

physical connection, verifying [7-6](#)

plus dialing [5-6, G-2](#)

PoE [2-4](#)

ports

access [3-2](#)

network [3-2](#)

power

external [2-3, 2-4](#)

for the phone [2-3](#)

outage [2-4](#)

PoE [2-4](#)

power over Ethernet

See PoE

power source

causing phone to reset [7-8](#)

power injector [2-4](#)

Private Line Automated Ringdown (PLAR) [5-6, G-2](#)

programmable feature buttons [1-5](#)

programmable line button, description of [1-5](#)

protected call

description [1-16](#)

Protected Calls [1-16](#)

R

Real-Time Control Protocol

See RTCP

Real-Time Transport Protocol

See RTP

redial [5-7, G-3](#)

redial button [1-2](#)

remote port configuration [5-7](#)

reset, factory [7-10](#)

reset settings on phone [7-10](#)

resetting

basic [7-10](#)

Cisco Unified IP phone [7-10](#)

continuously [7-6](#)

intentionally [7-7](#)

methods [7-10](#)

ringer, indicator for [1-3, 1-4](#)

ringer volume control [G-2](#)

S

SCCP [1-8](#)

secure conference

restrictions [1-16, 1-17](#)

security restrictions [1-17](#)

secure SRST reference [1-14](#)

security

CAPF (Certificate Authority Proxy Function) [1-14](#)

configuring on phone [3-10](#)

device authentication [1-13](#)

encrypted configuration file [1-14](#)

file authentication [1-13](#)

image authentication [1-13](#)

- Locally Significant Certificate (LSC) [3-10](#)
- media encryption [1-14](#)
- phone hardening [1-14](#)
- secure SRST reference [1-14](#)
- security profiles [1-14, 1-15](#)
- signaling authentication [1-13](#)
- signaling encryption [1-14](#)
- security profiles [1-14, 1-15](#)
- shared line [5-7, G-3](#)
- shield icon [1-10](#)
- signaling authentication [1-13](#)
- signaling encryption [1-14](#)
- SIP [1-8](#)
- Speaker button, disabling [3-3](#)
- speakerphone button, description of [1-5](#)
- speed dialing [5-7, G-3](#)
- SRST [6-5](#)
- standard (ad hoc) conference [5-5](#)
- startup problems [7-1](#)
- startup process
 - accessing TFTP server [2-7](#)
 - configuring VLAN [2-6](#)
 - contacting Cisco Unified Communications Manager [2-7](#)
 - loading stored phone image [2-7](#)
 - obtaining IP address [2-7](#)
 - obtaining power [2-6](#)
 - requesting configuration file [2-7](#)
 - understanding [2-6](#)
- statistics
 - network [6-7](#)
 - streaming [6-13](#)
- Status Messages web page [6-2, 6-10](#)
- Stream 1 web page [6-2, 6-13](#)
- streaming statistics [6-13](#)
- Subnet Mask [4-2](#)
- supplicant, in 802.1X [1-18](#)
- switch
 - Cisco Catalyst [2-2](#)

- internal Ethernet [2-2](#)

T

- TCP [1-8](#)
- technical specifications, for Cisco Unified IP Phone [C-1](#)
- telephone features
 - Cisco Unified Video Advantage [5-4](#)
- telephony features
 - agent greeting [5-2](#)
 - audible message waiting indicator [5-2](#)
 - auto answer [5-2](#)
 - auto barge [5-3](#)
 - automatic port synchronization [5-3](#)
 - block external to external transfer [5-3](#)
 - call forward [5-3](#)
 - call forward destination override [5-4](#)
 - call waiting [5-4](#)
 - cBarge [5-4](#)
 - client matter codes [5-5](#)
 - conference [5-5](#)
 - CTI applications [5-5](#)
 - forced authorization codes [5-5](#)
 - group call pickup [5-5](#)
 - hold [5-5](#)
 - meet me conference [5-6](#)
 - message waiting [5-6](#)
 - monitoring and recording [5-7](#)
 - music-on-hold [5-6](#)
 - mute [5-6](#)
 - on hook call transfer [5-6](#)
 - plus dialing [5-6](#)
 - redial [5-7](#)
 - remote port configuration [5-7](#)
 - shared line [5-7](#)
 - speed dialing [5-7](#)
 - Time-of-Day Routing [5-8](#)
 - time zone [5-8](#)
 - transfer [5-8](#)

- voice messaging system [5-8](#)
- TFTP
 - description [1-8](#)
 - troubleshooting [7-3](#)
- TFTP Server 1 [4-2](#)
- Time-of-Day Routing [5-8, G-3](#)
- time zone update [5-8](#)
- TLS [2-5](#)
- transfer [5-8, G-3](#)
- transfer button, description of [1-4](#)
- Transmission Control Protocol
 - See TCP
- Transport Layer Security
 - See TLS
- Trivial File Transfer Protocol
 - See TFTP
- troubleshooting
 - DHCP [7-6](#)
 - DNS [7-7](#)
 - IP addressing and routing [7-3](#)
 - network connectivity [7-3](#)
 - network outages [7-6](#)
 - phones resetting [7-7](#)
 - physical connection [7-6](#)
 - services on Cisco Unified Communications Manager [7-4](#)
 - TFTP settings [7-3](#)
 - VLAN configuration [7-7](#)

U

- User Datagram Protocol
 - See UDP
- User Options web page
 - description [5-9](#)
 - giving users access to [5-9, A-1](#)
- user options web page
 - call forward settings [5-11](#)
- users

- accessing voice messaging system [A-2](#)
- adding to Cisco Unified Communications Manager [5-8](#)
- providing support to [A-1](#)
- required information [A-1](#)

V

- VLAN
 - auxiliary, for voice traffic [2-3](#)
 - configuring for voice networks [2-2](#)
 - native, for data traffic [2-3](#)
 - verifying [7-7](#)
- VLAN, interaction with [2-2](#)
- voice mail [G-3](#)
- voice messaging system [5-8](#)
- voice messaging system, accessing [A-2](#)
- voice VLAN [2-3](#)
- volume button, description of [1-3, 1-5](#)

W

- wall mounting, Cisco Unified IP Phone [3-9, E-1, F-1](#)
- web page
 - about [6-1](#)
 - accessing [6-2](#)
 - Debug Display [6-10](#)
 - Device Information [6-2, 6-3](#)
 - disabling access to [6-3](#)
 - Ethernet Information [6-2, 6-7](#)
 - Network [6-2, 6-7](#)
 - Network Configuration [6-4](#)
 - Network Configuration web page [6-2](#)
 - preventing access to [6-3](#)
 - Status Messages [6-2, 6-10](#)
 - Stream 1 [6-2, 6-13](#)
- wideband codec [1-1](#)
- WMK [E-1](#)

X

XmlDefault.cnf.xml [2-5](#)