



Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager 5.1 (SCCP)

Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE

Corporate 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: 408 526-4100

Text Part Number: OL-11528-01



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

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

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

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

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

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

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

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

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

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

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

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0609R)



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

Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager 5.1 (SCCP), Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE

Copyright © 2006 Cisco Systems, Inc. All rights reserved.



Preface xiii

Overview xiii

Audience xiii

Organization xiv

Related Documentation xv

Obtaining Documentation xvi

 Cisco.com xvi

 Product Documentation DVD xvii

 Ordering Documentation xvii

Documentation Feedback xviii

Cisco Product Security Overview xviii

 Reporting Security Problems in Cisco Products xix

Obtaining Technical Assistance xx

 Cisco Technical Support & Documentation Website xx

 Submitting a Service Request xxi

 Definitions of Service Request Severity xxi

Obtaining Additional Publications and Information xxii

Document Conventions xxiii

CHAPTER 1

An Overview of the Cisco Unified IP Phone 1-1

Understanding the Cisco Unified IP Phone 7961G/7961G-GE and
7941G/7941G-GE 1-2

What Networking Protocols are Used? 1-5

What Features are Supported on the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE? 1-7

Feature Overview 1-8

Configuring Telephony Features 1-9

Configuring Network Parameters Using the Cisco Unified IP Phone 1-9

Providing Users with Feature Information 1-10

Understanding Security Features for Cisco Unified IP Phones 1-10

Overview of Supported Security Features 1-12

Understanding Security Profiles 1-16

Identifying Encrypted and Authenticated Phone Calls 1-16

Security Restrictions 1-17

Overview of Configuring and Installing Cisco Unified IP Phones 1-17

Configuring Cisco Unified IP Phones in Cisco Unified CallManager 1-18

Checklist for Configuring the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE in Cisco Unified CallManager 1-18

Installing Cisco Unified IP Phones 1-22

Checklist for Installing the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE 1-23

CHAPTER 2

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

Understanding Interactions with Other Cisco Unified IP Telephony Products 2-2

Understanding How the Cisco Unified IP Phone Interacts with Cisco Unified CallManager 2-2

Understanding How the Cisco Unified IP Phone Interacts with the VLAN 2-3

Providing Power to the Cisco Unified IP Phone 2-5

Power Guidelines 2-6

Power Outage 2-7

Obtaining Additional Information about Power 2-8

Understanding Phone Configuration Files 2-8

Understanding the Phone Startup Process 2-9

Adding Phones to the Cisco Unified CallManager Database	2-12
Adding Phones with Auto-Registration	2-13
Adding Phones with Auto-Registration and TAPS	2-14
Adding Phones with Cisco Unified CallManager Administration	2-15
Adding Phones with BAT	2-16
Using Cisco Unified IP Phones with Different Protocols	2-17
Converting a New Phone from SCCP to SIP	2-17
Converting an In-Use Phone from SCCP to SIP	2-18
Converting an In-Use Phone from SIP to SCCP	2-18
Deploying a Phone in an SCCP and SIP Environment	2-18
Determining the MAC Address for a Cisco Unified IP Phone	2-19

CHAPTER 3**Setting Up the Cisco Unified IP Phone 3-1**

Before You Begin	3-2
Network Requirements	3-2
Cisco Unified CallManager Configuration	3-2
Safety	3-3
Understanding the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE Components	3-5
Network and Access Ports	3-5
Handset	3-6
Speakerphone	3-6
Headset	3-6
Audio Quality Subjective to the User	3-7
Connecting a Headset	3-7
Disabling a Headset	3-8
Using External Devices with Your Cisco Unified IP Phone	3-8
Installing the Cisco Unified IP Phone	3-9
Attaching the Cisco Unified IP Phone Expansion Module 7914	3-12

Adjusting the Placement of the Cisco Unified IP Phone	3-14
Adjusting Cisco Unified IP Phone Placement on the Desktop	3-14
Securing the Phone with a Cable Lock	3-14
Mounting the Phone to the Wall	3-15
Verifying the Phone Startup Process	3-17
Configuring Startup Network Settings	3-19
Configuring Security on the Cisco Unified IP Phone	3-19

CHAPTER 4

Configuring Settings on the Cisco Unified IP Phone 4-1

Configuration Menus on the Cisco Unified IP Phone	4-1
Displaying a Configuration Menu	4-2
Unlocking and Locking Options	4-3
Editing Values	4-4
Overview of Options Configurable from a Phone	4-5
Network Configuration Menu	4-7
Device Configuration Menu	4-15
CallManager Configuration Menu	4-15
HTTP Configuration Menu	4-17
Locale Configuration Menu	4-18
UI Configuration Menu	4-19
Media Configuration Menu	4-20
Ethernet Configuration Menu	4-21
Security Configuration Menu	4-21
QoS Configuration Menu	4-23
Network Configuration	4-23

CHAPTER 5

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

Telephony Features Available for the Cisco Unified IP Phone	5-2
Configuring Corporate and Personal Directories	5-15

Configuring Corporate Directories	5-16
Configuring Personal Directory	5-16
Modifying Phone Button Templates	5-17
Configuring Softkey Templates	5-18
Setting Up Services	5-18
Adding Users to Cisco Unified CallManager	5-19
Managing the User Options Web Pages	5-20
Giving Users Access to the User Options Web Pages	5-20
Specifying Options that Appear on the User Options Web Pages	5-20

CHAPTER 6
Customizing the Cisco Unified IP Phone 6-1

Customizing and Modifying Configuration Files	6-1
Creating Custom Phone Rings	6-2
Ringlist.xml File Format Requirements	6-2
PCM File Requirements for Custom Ring Types	6-3
Configuring a Custom Phone Ring	6-4
Creating Custom Background Images	6-5
List.xml File Format Requirements	6-5
PNG File Requirements for Custom Background Images	6-6
Configuring a Background Image	6-7

CHAPTER 7
Viewing Security Information, Model Information, Status, and Statistics on the Cisco Unified IP Phone 7-1

Security Configuration Menu	7-2
CTL File Menu	7-3
Trust List Menu	7-4
Model Information Screen	7-5
Status Menu	7-6
Status Messages Screen	7-6

Network Statistics Screen	7-15
Firmware Versions Screen	7-17
Expansion Module Status Screen	7-18
Call Statistics Screen	7-19

CHAPTER 8

Monitoring the Cisco Unified IP Phone Remotely 8-1

Accessing the Web Page for a Phone	8-2
Disabling and Enabling Web Page Access	8-3
Device Information	8-4
Network Configuration	8-5
Network Statistics	8-10
Device Logs	8-12
Streaming Statistics	8-13

CHAPTER 9

Troubleshooting and Maintenance 9-1

Resolving Startup Problems	9-2
Symptom: The Cisco Unified IP Phone Does Not Go Through its Normal Startup Process	9-2
Symptom: The Cisco Unified IP Phone Does Not Register with Cisco Unified CallManager	9-3
Identifying Error Messages	9-4
Checking Network Connectivity	9-4
Verifying TFTP Server Settings	9-4
Verifying IP Addressing and Routing	9-5
Verifying DNS Settings	9-5
Verifying Cisco Unified CallManager Settings	9-5
Cisco Unified CallManager and TFTP Services Are Not Running	9-6
Creating a New Configuration File	9-7
Registering the Phone with Cisco Unified CallManager	9-8

Symptom: Cisco Unified IP Phone Unable to Obtain IP Address	9-8
Cisco Unified IP Phone Resets Unexpectedly	9-8
Verifying the Physical Connection	9-9
Identifying Intermittent Network Outages	9-9
Verifying DHCP Settings	9-9
Checking Static IP Address Settings	9-10
Verifying the Voice VLAN Configuration	9-10
Verifying that the Phones Have Not Been Intentionally Reset	9-10
Eliminating DNS or Other Connectivity Errors	9-11
Troubleshooting Cisco Unified IP Phone Security	9-12
General Troubleshooting Tips	9-13
General Troubleshooting Tips for the Cisco Unified IP Phone Expansion Module 7914	9-16
Resetting or Restoring the Cisco Unified IP Phone	9-16
Performing a Basic Reset	9-16
Performing a Factory Reset	9-17
Using the Quality Report Tool	9-20
Monitoring the Voice Quality of Calls	9-20
Where to Go for More Troubleshooting Information	9-23
Cleaning the Cisco Unified IP Phone	9-23

APPENDIX A

Providing Information to Users Via a Website A-1

How Users Obtain Support for the Cisco Unified IP Phone	A-2
How Users Access the Online Help System on the Cisco Unified IP Phone	A-2
How Users Get Copies of Cisco Unified IP Phone Manuals	A-3
How Users Subscribe to Services and Configure Phone Features	A-3
How Users Access a Voice Messaging System	A-4
How Users Configure Personal Directory Entries	A-5

Installing and Configuring the Cisco Unified IP Phone Address Book Synchronizer **A-5**

APPENDIX B

Supporting International Users B-1

Adding Language Overlays to Phone Buttons **B-1**

Installing the Cisco Unified CallManager Locale Installer **B-2**

APPENDIX C

Technical Specifications C-1

Physical and Operating Environment Specifications **C-1**

Cable Specifications **C-2**

Network and Access Port Pinouts **C-2**

INDEX



Preface

Overview

The *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager 5.1 (SCCP), Cisco Unified IP Phone 7961G, 7961G-GE and 7941G, 7941G-GE* 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 CallManager or other network devices. See the [“Related Documentation”](#) section on page xv.

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 CallManager, many of the tasks in this manual require familiarity with Cisco Unified CallManager.

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 softkey templates, setting up services, and adding users to Cisco Unified CallManager
Chapter 7, “Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone”	Explains how to view model information, status messages, network statistics, and firmware information from the Cisco Unified IP Phone
Chapter 8, “Monitoring the Cisco Unified IP Phone Remotely”	Describes the information that you can obtain from the phone’s web page, and how to use this information to remotely monitor the operation of a phone and to assist with troubleshooting
Chapter 9, “Troubleshooting and Maintenance”	Provides tips for troubleshooting the Cisco Unified IP Phone and the Cisco Unified IP Phone Expansion Module 7914
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

Related Documentation

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

Cisco Unified IP Phone 7961G, 7961G-GE and 7941G, 7941G-GE

These publications are available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm

- *Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE Phone Guide*
- *Cisco Unified IP Phone 7941G and 7941G-GE Installation Guide*
- *Cisco Unified IP Phone 7961G and 7961G-GE Installation Guide*
- *Cisco Unified IP Phone Features A–Z*
- *Cisco Unified IP Phone Expansion Module 7914 Phone Guide*
- *Installing the Wall Mount Kit for the Cisco Unified IP Phone*
- *Regulatory Compliance and Safety Information for the Cisco Unified IP Phone 7900 Series*

Cisco Unified CallManager

These publications are available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm

- *Cisco Unified CallManager Administration Guide*
- *Cisco Unified CallManager System Guide*
- *Cisco Unified CallManager Security Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Features and Services Guide*

- *Cisco Unified CallManager Bulk Administration Guide*
- *Cisco Unified CallManager Troubleshooting Guide*
- *Installing and Configuring the Cisco Customer Directory Configuration Plugin*
- *Cisco IP Telephony Platform Administration Guide*
- *Cisco Unified CallManager Compatibility Matrix*

Troubleshooting

This document is available to registered Cisco.com users at the following URL:
http://www.cisco.com/warp/customer/788/AVVID/telecaster_trouble.html

- *Using the 79xx Status Information For Troubleshooting* tech note

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL:

<http://tools.cisco.com/RPF/register/register.do>) Registered users can access the tool at this URL:

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

**Tip**

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

<http://www.cisco.com/offer/subscribe>

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:
<http://www.cisco.com/univercd/cc/td/doc/abtnucd/136957.htm>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

Document Conventions

This document uses the following conventions:



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 conventions:

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

Waarschuwing

BELANGRIJKE VEILIGHEIDSINSTRUCTIES

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus TÄRKEITÄ TURVALLISUUSOHJEITA

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET**Attention IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS**Warnung WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza IMPORTANTI ISTRUZIONI SULLA SICUREZZA

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI**Advarsel VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE**Aviso INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! INSTRUCCIONES IMPORTANTES DE SEGURIDAD

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES**Varning! VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR**Figyelem FONTOS BIZTONSÁGI ELOÍRÁSOK**

Ez a figyelmeztető jel veszélyre utal. Sérülésveszélyt rejtő helyzetben van. Mielőtt bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplő figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján kereshető meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение

ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告

重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告

安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

주의 중요 안전 지침

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

Aviso INSTRUÇÕES IMPORTANTES DE SEGURANÇA

Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.

GUARDE ESTAS INSTRUÇÕES

Advarsel VIGTIGE SIKKERHEDSANVISNINGER

Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.

GEM DISSE ANVISNINGER

تحذير

إرشادات الأمان الهامة

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في آخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز. قم بحفظ هذه الإرشادات

Upozorenje VAŽNE SIGURNOSNE NAPOMENE

Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.

SACUVAJTE OVE UPUTE**Upozornění DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY**

Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.

USCHOVEJTE TYTO POKYNY**Προειδοποίηση ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ**

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כדי לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

Симболот за предупредување значи опасност. Се наоѓате во ситуација што може да предизвика телесни повреди. Пред да работите со опремата, бидете свесни за ризикот што постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во преведените безбедносни предупредувања што се испорачани со уредот.

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ**Upozornenie DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY**

Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.

USCHOVAJTE SI TENTO NÁVOD



An Overview of the Cisco Unified IP Phone

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

A Cisco Unified IP Phone, like other network devices, must be configured and managed. These phones support G.711, G.729, G.729a, G.729b, G.729ab, and wideband (16bits, 16kHz) audio compression. The phone also encodes and decodes the G.722 wideband codec.

This chapter includes the following topics:

- [Understanding the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE, page 1-2](#)
- [What Networking Protocols are Used?, page 1-5](#)
- [What Features are Supported on the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE?, page 1-8](#)

- [Understanding Security Features for Cisco Unified IP Phones, page 1-11](#)
- [Overview of Configuring and Installing Cisco Unified IP Phones, page 1-21](#)

**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 7961G/7961G-GE and 7941G/7941G-GE

[Figure 1-1](#) shows the main components of the Cisco Unified IP Phone 7961G and 7961G-GE, and [Figure 1-2](#) shows the main components of the Cisco Unified IP Phone 7941G and 7941G-GE.

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



Figure 1-2 Cisco Unified IP Phone 7941G and 7941G-GE

1 Programmable buttons 	Depending on configuration, programmable buttons provide access to: • Phone lines (line buttons) • Speed-dial numbers (speed-dial buttons, including the BLF speed-dial feature) • Web-based services (for example, a Personal Address Book (PAB) button) • Phone features (for example, a Privacy button) The buttons illuminate to indicate status:  Green, steady—Active call  Green, flashing—Held call  Amber, steady—Privacy in use  Amber, flashing—Incoming call  Red steady—Remote line in use (shared line or BLF status)
--	---

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

What Networking Protocols are Used?

Cisco Unified IP Phones support several industry-standard and Cisco networking protocols required for voice communication. [Table 1-1](#) provides an overview of the networking protocols that the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE support.

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

Networking Protocol	Purpose	Usage Notes
Bootstrap Protocol (BootP)	BootP enables a network device such as the Cisco Unified IP Phone to discover certain startup information, such as its IP address.	If you are using BootP to assign IP addresses to the Cisco Unified IP Phone, the BOOTP Server option shows “Yes” in the network configuration settings on the phone.
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 you 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, refer to <i>Cisco Unified CallManager System Guide</i> .

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

Networking Protocol	Purpose	Usage Notes
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Cisco Unified IP Phones use HTTP for the XML services and for troubleshooting purposes.
IEEE 802.1X	The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.	The Cisco Unified IP Phone implements the IEEE 802.1X standard by providing support for the EAP-MD5 option for 802.1X authentication. When 802.1X authentication is enabled on the phone, you should disable the PC port and voice VLAN. Refer to the “Supporting 802.1X Authentication on Cisco Unified IP Phones” section on page 1-18 for additional information.
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communicate using IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnets, and gateways identifications are automatically assigned if you are using the Cisco Unified IP Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally.
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.

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

Networking Protocol	Purpose	Usage Notes
Real-Time Control Protocol (RTCP)	RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round trip delay) on RTP streams.	RTCP is disabled by default, but you can enable it on a per phone basis using Cisco Unified CallManager. For more information, see the “Network Configuration Menu” section on page 4-27 .
Skinny Client Control Protocol (SCCP)	SCCP includes a messaging set that allows communications between call control servers and endpoint clients such as IP Phones. SCCP is proprietary to Cisco Systems.	Cisco Unified IP Phones use SCCP for call control. You can configure the Cisco Unified IP Phone to use either SCCP or Session Initiation Protocol (SIP).
Session Initiation Protocol (SIP)	SIP is an emerging standard for setting up telephone calls, multimedia conferencing, and other types of communications on the Internet.	Cisco Unified IP Phones use SCCP for call control. You can configure the Cisco Unified IP Phone to use either SCCP or SIP.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Cisco Unified IP Phones use TCP to connect to Cisco Unified CallManager and to access XML services.
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	When security is implemented, Cisco Unified IP Phones use the TLS protocol when securely registering with Cisco Unified CallManager.
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 using the Network Configuration menu on the phone.

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

Networking Protocol	Purpose	Usage Notes
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 2-2](#)

[Understanding the Phone Startup Process, page 2-9](#)

[Network Configuration Menu, page 4-7](#)

What Features are Supported on the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE?

The Cisco Unified IP Phone functions much like a digital business phone, allowing you to place and receive telephone 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 1-10](#)
- [Configuring Network Parameters Using the Cisco Unified IP Phone, page 1-10](#)
- [Providing Users with Feature Information, page 1-11](#)

Feature Overview

Cisco Unified IP Phones provide traditional telephony functionality, such as call forwarding and transferring, redialing, speed dialing, conference calling, and voice messaging system access. Cisco Unified IP phones also provide a variety of other features. For an overview of the telephony features that the Cisco Unified IP Phone supports and for tips on configuring them, see the [“Telephony Features Available for the Cisco Unified IP Phone”](#) section on page 5-2.

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

The Cisco Unified IP Phone can interact with other services and devices on your IP network to provide enhanced functionality. For example, you can integrate the Cisco Unified IP Phones with the corporate Lightweight Directory Access Protocol 3 (LDAP3) standard directory to enable users to search for co-worker contact information directly from their IP phones. You can also use XML to enable users to access information such as weather, stocks, quote of the day, and other web-based information. For information about configuring such services, see the [“Configuring Corporate Directories”](#) section on page 5-16 and the [“Setting Up Services”](#) section on page 5-18.

Finally, because the Cisco Unified IP Phone is a network device, you can obtain detailed status information from it directly. This information can assist you with troubleshooting any problems users might encounter when using their IP phones. See [Chapter 7, “Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone,”](#) for more information.

Related Topics

- [Configuring Settings on the Cisco Unified IP Phone, page 4-1](#)
- [Configuring Features, Templates, Services, and Users, page 5-1](#)
- [Troubleshooting and Maintenance, page 9-1](#)

Configuring Telephony Features

You can modify additional settings for the Cisco Unified IP Phone from the Cisco Unified CallManager Administration application. Use this web-based application to set up phone registration criteria and calling search spaces, to configure corporate directories and services, and to modify phone button templates, among other tasks. See the “[Telephony Features Available for the Cisco Unified IP Phone](#)” section on page 5-2 and the Cisco Unified CallManager documentation for additional information.

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

You can access the complete Cisco Unified CallManager documentation suite at this location:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm

Related Topic

- [Telephony Features Available for the Cisco Unified IP Phone, page 5-2](#)

Configuring Network Parameters Using the Cisco Unified IP Phone

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

For more information about configuring features and viewing statistics from the phone, see [Chapter 4, “Configuring Settings on the Cisco Unified IP Phone”](#) and see [Chapter 7, “Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone.”](#)

Providing Users with Feature Information

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

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm.

From this site, you can view various user guides.

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

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

Understanding Security Features for Cisco Unified IP Phones

Implementing security in the Cisco Unified CallManager system prevents identity theft of the phone and Cisco Unified CallManager 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.

[Table 1-2](#) shows where you can find additional information about security in this and other documents.

Table 1-2 *Cisco Unified IP Phone and Cisco Unified CallManager Security Topics*

Topic	Reference
Detailed explanation of security, including set up, configuration, and troubleshooting information for Cisco Unified CallManager and Cisco Unified IP Phones	Refer to <i>Cisco Unified CallManager Security Guide</i>
Security features supported on the Cisco Unified IP Phone	See the “Overview of Supported Security Features” section on page 1-13
Restrictions regarding security features	See the “Security Restrictions” section on page 1-18
Viewing a security profile name	See the “Understanding Security Profiles” section on page 1-17
Identifying phone calls for which security is implemented	See the “Identifying Encrypted and Authenticated Phone Calls” section on page 1-17
TLS connection	- See the “What Networking Protocols are Used?” section on page 1-5 - See the “Adding Phones to the Cisco Unified CallManager Database” section on page 2-12
Security and the phone startup process	See the “Understanding the Phone Startup Process” section on page 2-9
Security and phone configuration files	See the “Adding Phones to the Cisco Unified CallManager Database” section on page 2-12
Changing the TFTP Server 1 or TFTP Server 2 option on the phone when security is implemented	See Table 4-2 , in the “Network Configuration Menu” section on page 4-7
Understanding security icons in the CallManager 1 through CallManager 5 options in the Device Configuration Menu on the phone	See the “CallManager Configuration Menu” section on page 4-15
Items on the Security Configuration menu that you access from the Device Configuration menu on the phone	See the “Security Configuration Menu” section on page 4-25
Items on the Security Configuration menu that you access from the Settings menu on the phone	See the “Security Configuration Menu” section on page 4-29

Table 1-2 Cisco Unified IP Phone and Cisco Unified CallManager Security Topics (continued)

Topic	Reference
Unlocking the CTL file	See the “CTL File Screen” section on page 4-31
Disabling access to a phone’s web pages	See the “Disabling and Enabling Web Page Access” section on page 8-3
Troubleshooting	• See the “Troubleshooting Cisco Unified IP Phone Security” section on page 9-12 • Refer to the <i>Cisco Unified CallManager Security Guide</i>
Deleting the CTL file from the phone	See the “Resetting or Restoring the Cisco Unified IP Phone” section on page 9-17
Resetting or restoring the phone	See the “Resetting or Restoring the Cisco Unified IP Phone” section on page 9-17
802.1X Authentication for Cisco Unified IP Phones	See these sections: • “Supporting 802.1X Authentication on Cisco Unified IP Phones” section on page 1-18 • “Security Configuration Menu” section on page 4-25 • “Status Menu” section on page 7-3 • “Troubleshooting Cisco Unified IP Phone Security” section on page 9-12

Overview of Supported Security Features

[Table 1-3](#) provides an overview of the security features that the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE support. For more information about these features and about Cisco Unified CallManager and Cisco Unified IP Phone security, refer to *Cisco Unified CallManager Security Guide*.

For information about current security settings on a phone, choose **Settings > Security Configuration** and choose **Settings > Device Configuration > Security Configuration**. For more information, see the [“Security Configuration Menu”](#) section on page 4-25.



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 CallManager Security Guide*.

Table 1-3 Overview of Security Features

Feature	Description
Image authentication	Signed binary files (with the extension .sbn) prevent tampering with the firmware image before it is loaded on a phone. Tampering with the image causes a phone to fail the authentication process and reject the new image.
Customer-site certificate installation	Each Cisco Unified IP Phone requires a unique certificate for device authentication. Phones include a manufacturing installed certificate (MIC), but for additional security, you can specify in Cisco Unified CallManager Administration that a certificate be installed by using the CAPF ¹ . Alternatively, you can install an LSC from the Security Configuration menu on the phone. See the “Configuring Security on the Cisco Unified IP Phone” section on page 3-19 for more information.
Device authentication	Occurs between the Cisco Unified CallManager 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 CallManager should occur, and, if necessary, creates a secure signaling path between the entities using TLS protocol. Cisco Unified CallManager will not register phones unless they can be authenticated by the Cisco Unified CallManager.
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.

Table 1-3 Overview of Security Features (continued)

Feature	Description
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 CallManager to authenticate the phone.
Secure SRST reference	After you configure a SRST reference for security and then reset the dependent devices in Cisco Unified CallManager Administration, the TFTP server adds the SRST certificate to the phone cnf.xml file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router.
Media encryption	Uses SRTP to ensure that the media streams between supported devices proves secure and that only the intended device receives and reads the data. Includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport.
Signaling encryption	Ensures that all SCCP signaling messages that are sent between the device and the Cisco Unified CallManager server are encrypted.
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure that are too processing-intensive for the phone, and it 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, or encrypted. See the “Understanding Security Profiles” section on page 1-17 for more information.
Encrypted configuration files	Lets you ensure the privacy of phone configuration files.
Optional disabling of the web server functionality for a phone	You can prevent access to a phone’s web page, which displays a variety of operational statistics for the phone.

Table 1-3 Overview of Security Features (continued)

Feature	Description
Phone hardening	Additional security options, which you control from Cisco Unified CallManager Administration: - Disabling PC port - Disabling Gratuitous ARP (GARP) - Disabling PC Voice VLAN access - Disabling access to the Setting menus, or providing restricted access that allows access to the User Preferences menu and saving volume changes only - Disabling access to web pages for a phone. Note You can view current settings for the PC Port Disabled, GARP Enabled, and Voice VLAN enabled options by looking at the phone’s Security Configuration menu. For more information, see the “Device Configuration Menu” section on page 4-15.
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 1-18 for more information.

1. CAPF = Certificate Authority Proxy Function

Related Topics

- [Understanding Security Profiles, page 1-17](#)
- [Identifying Encrypted and Authenticated Phone Calls, page 1-17](#)
- [Security Restrictions, page 1-18](#)
- [Device Configuration Menu, page 4-15](#)

Understanding Security Profiles

All Cisco Unified IP Phones that support Cisco Unified CallManager 5.1 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 CallManager Security Guide, Release 5.1(1)*.

To view the security mode that is set for the phone, look at the Security Mode setting in the Security Configuration menu. For more information, see the [“Security Configuration Menu” section on page 4-25](#).

Related Topics

- [Identifying Encrypted and Authenticated Phone Calls, page 1-17](#)
- [Security Restrictions, page 1-18](#)
- [Device Configuration Menu, page 4-15](#)

Identifying Encrypted and Authenticated Phone Calls

When security is implemented for a phone, you can identify authenticated or encrypted phone calls by icons on the screen on the phone.

In an authenticated call, all devices participating in the establishment of the call are authenticated by the Cisco Unified CallManager. When a call in progress is authenticated, the call progress icon to the right of the call duration timer in the phone LCD screen changes to this icon .

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



Note

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

Related Topic

- [Understanding Security Profiles, page 1-17](#)
- [Understanding Security Features for Cisco Unified IP Phones, page 1-11](#)
- [Security Restrictions, page 1-18](#)

Security Restrictions

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

If the initiator phone is configured for encryption, the barge initiator can barge into an authenticated or nonsecure call from the encrypted phone. After the barge occurs, Cisco Unified CallManager classifies the call as nonsecure.

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

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

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 1-19](#)
- [Required Network Components, page 1-19](#)
- [Best Practices—Requirements and Recommendations, page 1-20](#)

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 initial release of the IP phone 802.1X supplicant implements the EAP-MD5 option for 802.1X authentication.

Required Network Components

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

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

Best Practices—Requirements and Recommendations

- **Enable 802.1X Authentication**—If you want to use the 802.1X standard to authenticate Cisco Unified IP Phones, be sure that you have properly configured the other components before enabling it on the phone. See the [“802.1X Authentication and Status” section on page 4-40](#) for more information.
- **Configure PC Port**—The 802.1X standard does not take into account the use of VLANs and thus recommends that only a single device should be authenticated to a specific switch port. However, some switches (including Cisco Catalyst switches) support multi-domain authentication. The switch configuration determines whether you can connect a PC to the phone’s PC port.
 - **Enabled**—If you are using a switch that supports multi-domain authentication, you can enable the PC port and connect a PC to it. In this case, Cisco Unified IP Phones support proxy EAPOL-Logoff to monitor the authentication exchanges between the switch and the attached PC. For more information about IEEE 802.1X support on the Cisco Catalyst switches, refer to the Cisco Catalyst switch configuration guides at:
 - **Disabled**—If the switch does not support multiple 802.1X-compliant devices on the same port, you should disable the PC Port when 802.1X authentication is enabled. See the [“Security Configuration Menu” section on page 4-25](#) for more information. If you do not disable this port and subsequently attempt to attach a PC to it, the switch will deny network access to both the phone and the PC.
- **Configure Voice VLAN**—Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.
 - **Enabled**—If you are using a switch that supports multi-domain authentication, you can continue to use the voice VLAN.
 - **Disabled**—If the switch does not support multi-domain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN. See the [“Security Configuration Menu” section on page 4-25](#) for more information.
- **Enter MD5 Shared Secret**—If you disable 802.1X authentication or perform a factory reset on the phone, the previously configured MD5 shared secret is deleted. See the [“802.1X Authentication and Status” section on page 4-40](#) for more information.

Overview of Configuring and Installing Cisco Unified IP Phones

When deploying a new IP telephony system, system administrators and network administrators must complete several initial configuration tasks to prepare the network for IP telephony service. For information and a checklist for setting up and configuring a complete Cisco IP telephony network, refer to the “System Configuration Overview” chapter in *Cisco Unified CallManager System Guide*.

After you have set up the IP telephony system and configured system-wide features in Cisco Unified CallManager, 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 CallManager, page 1-21](#)
- [Installing Cisco Unified IP Phones, page 1-26](#)

Configuring Cisco Unified IP Phones in Cisco Unified CallManager

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

- Auto-registration
- Cisco Unified CallManager 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 CallManager Database](#)” section on page 2-12.

For general information about configuring phones in Cisco Unified CallManager, refer to the “Cisco Unified IP Phone” chapter in *Cisco Unified CallManager System Guide*.

Checklist for Configuring the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE in Cisco Unified CallManager

Table 1-4 provides an overview and checklist of configuration tasks for the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE in Cisco Unified CallManager 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 1-4 Checklist for Configuring the Cisco Unified IP Phone 7961G/7961G-GE/7941G/7941G-GE in Cisco Unified CallManager

Task	Purpose	For More Information
1. Gather the following information about the phone: • Phone Model • MAC address • Physical location of the phone • Name or user ID of phone user • Device pool • Partition, calling search space, and location information • Number of lines and associated directory numbers (DNs) to assign to the phone • Cisco Unified CallManager user to associate with the phone • Phone usage information that affects phone button template, softkey template, phone features, IP Phone services, or phone applications	Provides list of configuration requirements for setting up phones. Identifies preliminary configuration that you need to perform before configuring individual phones, such as phone button templates or softkey templates.	Refer to <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phone” chapter. See the “Telephony Features Available for the Cisco Unified IP Phone” section on page 5-2.

Table 1-4 Checklist for Configuring the Cisco Unified IP Phone 7961G/7961G-GE/7941G/7941G-GE in Cisco Unified CallManager (continued)

Task	Purpose	For More Information
2. Customize phone button templates (if required).	Changes the number of line buttons, speed-dial buttons, Service URL buttons or adds a Privacy button to meet user needs.	Refer to <i>Cisco Unified CallManager Administration Guide</i> , “Phone Button Template Configuration” chapter. See the “Modifying Phone Button Templates” section on page 5-17.
3. Add and configure the phone by completing these required fields in the Phone Configuration window: • Phone type • Description (user name or ID) • MAC address • Device pool • Partition • Calling Search Space • Button template • Product Specific Configuration • Softkey template (if customized)	Adds the device with its default settings to the Cisco Unified CallManager database.	Refer to <i>Cisco Unified CallManager Administration Guide</i> , “Cisco Unified IP Phone Configuration” chapter. For information about Product Specific Configuration fields, refer to “?” Button Help in the Phone Configuration window.

Table 1-4 Checklist for Configuring the Cisco Unified IP Phone 7961G/7961G-GE/7941G/7941G-GE in Cisco Unified CallManager (continued)

Task	Purpose	For More Information
4. Add and configure directory numbers (lines) on the phone by completing these required fields in the Directory Number Configuration window. • Directory number(s) • Partition • Multiple Calls and Call Waiting • Call Forwarding and Pickup (if used) • Voice Messaging (if used)	Adds primary and secondary directory numbers and features associated with directory numbers to the phone.	Refer to <i>Cisco Unified CallManager Administration Guide</i> , “Cisco Unified IP Phone Configuration” chapter: “Adding a Directory Number” section “Creating a Cisco Unity Voice Mailbox” section. See the “Telephony Features Available for the Cisco Unified IP Phone” section on page 5-2.
5. Customize softkey templates.	Adds, deletes, or changes order of softkey features that display on the user’s phone to meet feature usage needs.	Refer to <i>Cisco Unified CallManager Administration Guide</i> , “Softkey Template Configuration” chapter. See the “Configuring Softkey Templates” section on page 5-18.
6. Configure speed-dial buttons and assign speed-dial numbers (optional).	Adds speed-dial buttons and numbers, Note Users can change speed-dial settings on their phones by using Cisco Unified IP Phone User Options.	Refer to <i>Cisco Unified CallManager Administration Guide</i> , “Cisco Unified IP Phone Configuration” chapter, “Configuring Speed-Dial Buttons” section.

Table 1-4 Checklist for Configuring the Cisco Unified IP Phone 7961G/7961G-GE/7941G/7941G-GE in Cisco Unified CallManager (continued)

Task	Purpose	For More Information
7. Configure Cisco Unified IP Phone services and assign services (optional).	Provides IP Phone services. Note Users can add or change services on their phones by using the Cisco Unified IP Phone User Options.	Refer to <i>Cisco Unified CallManager Administration Guide</i> , “Cisco Unified IP Phone Services Configuration” chapter. See the “Setting Up Services” section on page 5-18 .
8. Assign services to phone buttons (optional).	Provides single button access to an IP phone service or URL.	Refer to <i>Cisco Unified CallManager Administration Guide</i> , “Cisco Unified IP Phone Configuration” chapter, “Adding a Cisco Unified IP Phone Service to a Phone Button” section.
9. Add user information by configuring required fields: - Name (last) - User ID - Password (for User Options web pages) - PIN (for use with Extension Mobility and Personal Directory)	Adds user information to the global directory for Cisco Unified CallManager.	Refer to <i>Cisco Unified CallManager Administration Guide</i> , “Adding a New User” chapter. See the “Adding Users to Cisco Unified CallManager” section on page 5-19 .

Table 1-4 Checklist for Configuring the Cisco Unified IP Phone 7961G/7961G-GE/7941G/7941G-GE in Cisco Unified CallManager (continued)

Task	Purpose	For More Information
10. Associate a user with a phone (optional).	Provides users with control over their phone such as forwarding calls or adding speed-dial numbers or services. Note Some phones, such as those in conference rooms, do not have an associated user.	Refer to <i>Cisco Unified CallManager Administration Guide</i> , “Adding a New User” chapter, “Associating Devices to a User” section.

Installing Cisco Unified IP Phones

After you have added the phones to the Cisco Unified CallManager database, you can complete the phone installation. You (or the phone users) can install the phone at the users’s location. The Cisco Unified IP Phone Installation Guide that ships in the box with each phone provides directions for connecting the phone handset, cables, and other accessories.



Note

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

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

After the phone is connected to the network, the phone startup process begins and the phone registers with Cisco Unified CallManager. 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 7961G/7961G-GE and 7941G/7941G-GE

Table 1-5 provides an overview and checklist of installation tasks for the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE. 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 1-5 Checklist for Installing the Cisco Unified IP Phone 7961G/7961G-GE/7941G/7941G-GE

Task	Purpose	For More Information
1. Choose the power source for the phone: - Power over Ethernet (PoE) - External power supply	Determines how the phone receives power.	See the “Providing Power to the Cisco Unified IP Phone” section on page 2-4.
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 3-9. See the “Adjusting the Placement of the Cisco Unified IP Phone” section on page 3-14.
3. Add a Cisco Unified IP Phone Expansion Module 7914 to the Cisco Unified IP Phone 7961G/7961G-GE (optional).	Extends functionality of a Cisco Unified IP Phone 7961G/7961G-GE by adding 14 line appearances or speed dial numbers.	See the “Attaching the Cisco Unified IP Phone Expansion Module 7914” section on page 3-12.
4. Monitor the phone startup process.	Verifies that phone is configured properly.	See the “Verifying the Phone Startup Process” section on page 3-17.

Table 1-5 Checklist for Installing the Cisco Unified IP Phone 7961G/7961G-GE/7941G/7941G-GE

Task	Purpose	For More Information
5. Configure these network settings on the phone by choosing Settings > Network Configuration. To enable DHCP: - Set DHCP Enabled to Yes - To use an alternate TFTP server, set Alternate TFTP Server to Yes Enter IP address for TFTP Server 1 To disable DHCP: - Set DHCP Enabled to No - Enter static IP address for phone - Enter subnet mask - Enter default router IP addresses - Enter domain name where phone resides - Set Alternate TFTP Server to Yes Enter IP address for TFTP Server 1	Using DHCP—The IP address is automatically assigned and the Cisco Unified IP Phone is directed to a TFTP Server. Note Consult with the network administrator if you need to assign an alternative TFTP server instead of using the TFTP server assigned by DHCP. Without DHCP—You must configure the IP address, TFTP server, subnet mask, domain name, and default router locally on the phone.	See the “Configuring Startup Network Settings” section on page 3-19. See the “Network Configuration Menu” section on page 4-7.
6. Set up security on the phone.	Provides protection against data tampering threats and identity theft of phones.	See the “Configuring Security on the Cisco Unified IP Phone” section on page 3-19 .
7. Make calls with the Cisco Unified IP Phone.	Verifies that the phone and features work correctly.	Refer to <i>Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE Phone Guide</i> .
8. Provide information to end users about how to use their phones and how to configure their phone options.	Ensures that users have adequate information to successfully use their Cisco Unified IP Phones.	See Appendix A, “Providing Information to Users Via a Website.”



Preparing to Install the Cisco Unified IP Phone on Your Network

Cisco Unified IP Phones enable you to communicate 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 CallManager.

This chapter focuses on the interactions between the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE and Cisco Unified CallManager, 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/partner/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 2-2](#)
- [Providing Power to the Cisco Unified IP Phone, page 2-4](#)
- [Understanding Phone Configuration Files, page 2-8](#)
- [Understanding the Phone Startup Process, page 2-9](#)

- [Adding Phones to the Cisco Unified CallManager Database, page 2-12](#)
- [Using Cisco Unified IP Phones with Different Protocols, page 2-17](#)
- [Determining the MAC Address for a Cisco Unified IP Phone, page 2-19](#)

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 CallManager system before sending and receiving calls.

This section includes the following topics:

- [Understanding How the Cisco Unified IP Phone Interacts with Cisco Unified CallManager, page 2-2](#)
- [Understanding How the Cisco Unified IP Phone Interacts with the VLAN, page 2-3](#)

Understanding How the Cisco Unified IP Phone Interacts with Cisco Unified CallManager

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

- Firmware for phones
- Authentication and encryption (if configured for the telephony system)
- Configuration file and CTL file, via TFTP service
- Phone registration

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

For information about configuring Cisco Unified CallManager to work with the IP devices described in this chapter, refer to *Cisco Unified CallManager Administration Guide*, *Cisco Unified CallManager System Guide*, and to *Cisco Unified CallManager Security 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 1-11.

**Note**

If the Cisco Unified IP Phone model that you want to configure does not appear in the Phone Type drop-down list in Cisco Unified CallManager Administration, go to the following URL and install the latest support patch for your version of Cisco Unified CallManager:

<http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>

Related Topic

- [Telephony Features Available for the Cisco Unified IP Phone, page 5-2](#)

Understanding How the Cisco Unified IP Phone Interacts with the VLAN

The Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE have an internal Ethernet switch, enabling forwarding of packets to the phone, and to the access port and the network port on the back of the phone.

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

- The current VLANs might be configured on an IP subnet basis. However, additional IP addresses might not be available to assign the phone to the same subnet as other devices connected to the same port.
- Data traffic present on the VLAN supporting phones might reduce the quality of Voice-over-IP traffic.

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

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

- Voice traffic to and from the IP phone (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 related documentation at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/index.htm>

Related Topics

- [Understanding the Phone Startup Process, page 2-9](#)
- [Network Configuration Menu, page 4-7](#)

Providing Power to the Cisco Unified IP Phone

The Cisco Unified IP Phone 7961G, 7961G-GE and 7941G, 7941G-GE 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 2-5](#)
- [Power Outage, page 2-7](#)
- [Obtaining Additional Information about Power, page 2-8](#)

Power Guidelines

[Table 2-1](#) provides guidelines for powering the Cisco Unified IP Phone 7961G and 7941G.

[Table 2-2](#) provides guidelines for powering the Cisco Unified IP Phone 7961G-GE and 7941G-GE.

Table 2-1 Guidelines for Powering the Cisco Unified IP Phone 7961G and 7941G

Power Type	Guidelines
External power— Provided through the CP-PWR-CUBE-3 external power supply.	• The Cisco Unified IP Phone 7961G and 7941G 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.

Table 2-1 *Guidelines for Powering the Cisco Unified IP Phone 7961G and 7941G (continued)*

Power Type	Guidelines
PoE power—Provided by a switch through the Ethernet cable attached to the phone.	• The Cisco Unified IP Phone 7961G and 7941G support Cisco inline PoE. • The Cisco Unified IP Phone 7961G and 7941G support IEEE 802.3af 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 Phones 7961G and 7941G.

Table 2-2 *Guidelines for Powering the Cisco Unified IP Phone 7961G-GE and 7941G-GE*

Power Type	Guidelines
External power—Provided through the CP-PWR-CUBE-3 external power supply.	• The Cisco Unified IP Phone 7961G-GE and 7941G-GE use the CP-PWR-CUBE-3 external power supply only.
External power—Provided through the Cisco Unified IP Phone Power Injector.	The Cisco Unified IP Phone Power Injector may be used with any Cisco Unified IP Phone. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco Unified IP Phone Power Injector is connected between a switch port and the IP Phone, and supports a maximum cable length of 100m between the unpowered switch and the IP Phone.

Table 2-2 ***Guidelines for Powering the Cisco Unified IP Phone 7961G-GE and 7941G-GE***

Power Type	Guidelines
PoE power—Provided by a switch through the Ethernet cable attached to the phone.	• The gigabit Ethernet Cisco Unified IP Phone 79161G-GE and 7941G-GE do not support Cisco inline PoE. • The Cisco Unified IP Phone 7961G-GE and 7941G-GE support IEEE 802.3af power on signal pairs and spare pairs. The Cisco Unified IP Phone 79161G-GE and 7941G-GE are not compatible with Cisco switches that are not IEEE-compliant. • To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply. • Make sure that the CatOS or IOS version running on your switch supports your intended phone deployment. Refer to the documentation for your switch for operating system version information.
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 Phones 7961G-GE and 7941G-GE.

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 2-3](#). These documents provide information about the following topics:

- Cisco switches that work with the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE
- The Cisco IOS releases that support bidirectional power negotiation
- Other requirements and restrictions regarding power

Table 2-3 **Related Documentation for Power**

Document Topics	URL
Cisco Unified IP Phone Power Injector	http://www.cisco.com/en/US/products/hw/phones/p_s379/prod_installation_guides_list.html
PoE Solutions	http://www.cisco.com/en/US/netsol/ns340/ns394/ns147/ns412/networking_solutions_package.html
Cisco Catalyst Switches	http://www.cisco.com/univercd/cc/td/doc/product/lan/index.htm
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 CallManager. In general, any time you make a change in Cisco Unified CallManager that requires the phone to be reset, a change is made to the phone's configuration file automatically.

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

In addition, if the device security mode in the configuration file is set to Authenticated and the CTL file on the phone has a valid certificate for Cisco Unified CallManager, the phone establishes a TLS connection to Cisco Unified CallManager. 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 will continuously try to obtain a CTL file so that it can register securely.

If you configure security-related settings in Cisco Unified CallManager 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 CallManager Security Guide*. A phone requests a configuration file whenever it resets and registers with Cisco Unified CallManager.

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 CallManager
- The phone has not been added to the Cisco Unified CallManager 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 CallManager Database, the phone registration request will be rejected. In this case, the phone will reset and attempt to register repeatedly.

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

Understanding the Phone Startup Process

When connecting to the VoIP network, the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE go through a standard startup process that is described in [Table 2-4](#). Depending on your specific network configuration, not all of these steps may occur on your Cisco Unified IP Phone.

Table 2-4 *Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE Startup Process*

Step	Description	Related Topics
1. Obtaining Power from the Switch	If a phone is not using external power, the switch provides in-line power through the Ethernet cable attached to the phone.	• Adding Phones to the Cisco Unified CallManager Database, page 2-12. • Resolving Startup Problems, page 9-2.
2. Loading the Stored Phone Image	The Cisco Unified IP Phone has non-volatile Flash memory in which it stores firmware images and user-defined preferences. At startup, the phone runs a bootstrap loader that loads a phone image stored in Flash memory. Using this image, the phone initializes its software and hardware.	Resolving Startup Problems, page 9-2.
3. Configuring VLAN	If the Cisco Unified IP Phone is connected to a Cisco Catalyst switch, the switch next informs the phone of the voice VLAN defined on the switch. The phone needs to know its VLAN membership before it can proceed with the Dynamic Host Configuration Protocol (DHCP) request for an IP address.	• Network Configuration Menu, page 4-7. • Resolving Startup Problems, page 9-2.
4. Obtaining an IP Address	If the Cisco Unified IP Phone is using DHCP to obtain an IP address, the phone queries the DHCP server to obtain one. If you are not using DHCP in your network, you must assign static IP addresses to each phone locally.	• Network Configuration Menu, page 4-7. • Resolving Startup Problems, page 9-2.

Table 2-4 Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE Startup Process

Step	Description	Related Topics
5. Accessing a TFTP Server	In addition to assigning an IP address, the DHCP server directs the Cisco Unified IP Phone to a TFTP Server. If the phone has a statically-defined IP address, you must configure the TFTP server locally on the phone; the phone then contacts the TFTP server directly. Note You can also assign an alternative TFTP server to use instead of the one assigned by DHCP.	• Network Configuration Menu, page 4-7. • Resolving Startup Problems, page 9-2.
6. Requesting the CTL file	The TFTP server stores the certificate trust list (CTL) file. This file contains a list of Cisco Unified CallManagers and TFTP servers that the phone is authorized to connect to. It also contains the certificates necessary for establishing a secure connection between the phone and Cisco Unified CallManager.	For more information, refer to <i>Cisco Unified CallManager Security Guide</i>
7. Requesting the Configuration File	The TFTP server has configuration files, which define parameters for connecting to Cisco Unified CallManager and other information for the phone.	• Adding Phones to the Cisco Unified CallManager Database, page 2-12 • Resolving Startup Problems, page 9-2.

Table 2-4 *Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE Startup Process*

Step	Description	Related Topics
1. Contacting Cisco Unified CallManager	The configuration file defines how the Cisco Unified IP Phone communicates with Cisco Unified CallManager 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 CallManager on the list. If security is implemented, the phone makes a TLS connection. Otherwise, it makes a non-secure TCP connection. If the phone was manually added to the database, Cisco Unified CallManager identifies the phone. If the phone was not manually added to the database and auto-registration is enabled in Cisco Unified CallManager, the phone attempts to auto-register itself in the Cisco Unified CallManager database. Note Auto-registration is disabled when security is enabled on Cisco Unified CallManager. In this case, the phone must be manually added to the Cisco Unified CallManager database.	Resolving Startup Problems, page 9-2.

Adding Phones to the Cisco Unified CallManager Database

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

- [Adding Phones with Auto-Registration, page 2-13](#)
- [Adding Phones with Auto-Registration and TAPS, page 2-14](#)
- [Adding Phones with Cisco Unified CallManager Administration, page 2-15](#)
- [Adding Phones with BAT, page 2-16](#)

Table 2-5 provides an overview of these methods for adding phones to the Cisco Unified CallManager database.

Table 2-5 **Methods for Adding Phones to the Cisco Unified CallManager Database**

Method	Requires MAC Address?	Notes
Auto-registration	No	Results in automatic assignment of directory numbers
Auto-registration with TAPS	No	Requires auto-registration and the Bulk Administration Tool (BAT); updates information in the Cisco Unified IP Phone and in Cisco Unified CallManager Administration
Using the Cisco Unified CallManager 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:

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

**Note**

You should 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 with BAT” section on page 2-16](#).

In some cases, you might not want to use auto-registration: for example, if you want to assign a specific directory number to the phone or if you plan to implement authentication or encryption, as described in *Cisco Unified CallManager Security Guide*. For information about enabling auto-registration, refer to “Enabling Auto-Registration” in the *Cisco Unified CallManager Administration Guide*.

**Note**

Cisco Unified CallManager automatically disables auto-registration if you configure the cluster-wide security mode for authentication and encryption through the Cisco CTL client.

Related Topics

- [Adding Phones with Auto-Registration and TAPS, page 2-14](#)
- [Adding Phones with Cisco Unified CallManager Administration, page 2-15](#)
- [Adding Phones with BAT, page 2-16](#)

Adding Phones with Auto-Registration and TAPS

TAPS, the Tool for Auto-Registered Phones Support, works with the Bulk Administration Tool (BAT) to update a batch of phones that were already added to the Cisco Unified CallManager database with dummy MAC addresses. You use TAPS to update MAC addresses and download pre-defined configurations for phones.

You can add phones with auto-registration and TAPS without first gathering MAC addresses from phones.

**Note**

You should 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 with BAT” section on page 2-16](#).

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 CallManager Administration with the correct MAC address.

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

**Note**

Cisco Unified CallManager automatically disables auto-registration if you configure the cluster-wide security mode for authentication and encryption through the Cisco CTL client.

Refer to *Cisco Unified CallManager Bulk Administration Guide* for detailed instructions about BAT and about TAPS.

Related Topics

- [Adding Phones with Auto-Registration, page 2-13](#)
- [Adding Phones with Cisco Unified CallManager Administration, page 2-15](#)
- [Adding Phones with BAT, page 2-16](#)

Adding Phones with Cisco Unified CallManager Administration

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

For information about determining a MAC address, see the [“Determining the MAC Address for a Cisco Unified IP Phone” section on page 2-19](#).

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

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

Related Topics

- [Adding Phones with Auto-Registration, page 2-13](#)
- [Adding Phones with Auto-Registration and TAPS, page 2-14](#)
- [Adding Phones with BAT, page 2-16](#)

Adding Phones with BAT

The Cisco Bulk Administration Tool (BAT) is a plug-in application for Cisco Unified CallManager that enables you to perform batch operations, including registration, on multiple phones.

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

For information about determining a MAC address, see the [“Determining the MAC Address for a Cisco Unified IP Phone”](#) section on page 2-19.

For detailed instructions about using BAT, refer to *Cisco Unified CallManager Administration Guide* and to *Cisco Unified CallManager Bulk Administration Guide*.

Related Topics

- [Adding Phones with Auto-Registration, page 2-13](#)
- [Adding Phones with Auto-Registration and TAPS, page 2-14](#)
- [Adding Phones with Cisco Unified CallManager Administration, page 2-15](#)

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 2-17](#)
- [Converting an In-Use Phone from SCCP to SIP, page 2-18](#)
- [Converting an In-Use Phone from SIP to SCCP, page 2-18](#)
- [Deploying a Phone in an SCCP and SIP Environment, page 2-19](#)

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 CallManager 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 page in Cisco Unified CallManager Administration.

Refer to *Cisco Unified CallManager Administration Guide* for detailed information about Cisco Unified CallManager configuration. Refer to *Cisco Unified CallManager 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 the “Configuring Startup Network Settings” section on page 3-14.
- Step 3** Power cycle the phone.
-

Converting an In-Use Phone from SCCP to SIP

You can use the Bulk Administration Tool (BAT) to convert a phone that is in use in your network from SCCP to SIP. To access BAT from Cisco Unified CallManager Administration, choose **Bulk Administration > Phones > Migrate Phones > SCCP to SIP**. For detailed information, refer to *Cisco Unified CallManager Bulk Administration Guide*.

Converting an In-Use Phone from SIP to SCCP

To convert a phone that is in use in your network from SIP to SCCP, perform these steps. For more information, *Cisco Unified CallManager Administration Guide*.

Procedure

-
- Step 1** In Cisco Unified CallManager Administration, delete the existing SIP phone from the Cisco Unified CallManager database.
- Step 2** In Cisco Unified CallManager Administration, create the phone as an SCCP phone.
- Step 3** Power cycle the 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 CallManager Auto-Registration parameter is SCCP, perform these general steps:

1. Set the Cisco Unified CallManager `auto_registration_protocol` parameter to SCCP.

To do so, from Cisco Unified CallManager Administration, choose **System > Enterprise Parameters**.

2. Install the phones.
3. Change the `auto_registration_protocol` parameter to SIP.
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:

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

For information about accessing the web page, see the [“Accessing the Web Page for a Phone”](#) section on page 8-2.



Setting Up the Cisco Unified IP Phone

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

- [Before You Begin, page 3-2](#)
- [Understanding the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE Components, page 3-5](#)
- [Installing the Cisco Unified IP Phone, page 3-9](#)
- [Attaching the Cisco Unified IP Phone Expansion Module 7914, page 3-12](#)
- [Adjusting the Placement of the Cisco Unified IP Phone, page 3-14](#)
- [Verifying the Phone Startup Process, page 3-17](#)
- [Configuring Startup Network Settings, page 3-19](#)
- [Configuring Security on the Cisco Unified IP Phone, page 3-19](#)



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 3-2](#)
- [Cisco Unified CallManager Configuration, page 3-2](#)
- [Safety, page 3-3](#)

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 CallManager installed in your network and configured to handle call processing
- IP network that supports DHCP or manual assignment of IP address, gateway, and subnet mask

**Note**

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

Cisco Unified CallManager Configuration

The Cisco Unified IP Phone requires Cisco Unified CallManager to handle call processing. Refer to *Cisco Unified CallManager Administration Guide* or to context-sensitive help in the Cisco Unified CallManager application to ensure that Cisco Unified CallManager 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 CallManager before connecting any Cisco Unified IP Phone to the network. For information about enabling and configuring auto-registration, refer to *Cisco Unified CallManager Administration Guide*. Also, see the [“Adding Phones to the Cisco Unified CallManager Database” section on page 2-12](#).

You must use Cisco Unified CallManager 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 5-2](#) for details.

In Cisco Unified CallManager, you can add users to the database and associate them with specific phones. In this way, users gain access to web pages that allow them to configure items such as call forwarding, speed dialing, and voice messaging system options. See the [“Adding Users to Cisco Unified CallManager” section on page 5-19](#) for details.

Safety

Review the following warnings before installing the Cisco Unified IP Phone. To see translations of these warnings, refer to the *Regulatory Compliance and Safety Information for the Cisco Unified IP Phone 7900 Series* document that accompanied this device.



Warning

Read the installation instructions before you connect the system to its power source.



Warning

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.



Warning

Ultimate disposal of this product should be handled according to all national laws and regulations.

**Warning**

Do not work on the system or connect or disconnect cables during periods of lightning activity.

**Warning**

To avoid electric shock, do not connect safety extra low voltage (SELV) circuits to telephone network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.

**Caution**

Inline power circuits provide current over the cable. Use the Cisco provided cable or a minimum 24 AWG communication cable.

The following warnings apply when you use an external power supply.

**Caution**

Only use the proper Cisco approved external power supply. Reference the installation manual provided with the phone.

**Warning**

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15 A U.S. (240 VAC, 10 A international) is used on the phase conductors (all current-carrying conductors).

**Warning**

The device is designed to work with TN power systems.

**Warning**

The plug-socket combination must be accessible at all times because it serves as the main disconnecting device. #331

Understanding the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE Components

The Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE includes these components on the phone or as accessories for the phone:

- [Network and Access Ports, page 3-5](#)
- [Handset, page 3-6](#)
- [Speakerphone, page 3-6](#)
- [Headset, page 3-6](#)

Network and Access Ports

The back of the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE include these ports:

- Network port
 - labeled 10/100 SW on the 7961G and 7941G
 - labeled 10/100/1000 SW on the 7961G-GE and 7941G-GE
- Access port
 - labeled 10/100 PC on the 7961G and 7941G
 - labeled 10/100/1000 PC on the 7961G-GE and 7941G-GE

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

Use the SW network port to connect the phone to the network. You must use a straight-through cable on these ports. The phone can also obtain inline power from a switch over these connections. See the [“Adding Phones to the Cisco Unified CallManager Database”](#) section on page 2-12 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

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

You can disable the speakerphone through the Cisco Unified CallManager Administration application. To do so, choose **Device > Phone** and locate the phone you want to modify. In the Phone Configuration web page for the phone, check the **Disable Speakerphone** check box.

Headset

Although Cisco Systems performs some internal testing of third-party headsets for use with the Cisco Unified IP Phones, Cisco does not certify or support products from headset or handset vendors. Because of the inherent environmental and hardware inconsistencies in the locations where Cisco Unified IP Phones are deployed, there is not a single “best” solution that is optimal for all environments. Cisco recommends that customers test the headsets that work best in their environment before deploying a large number of units in their network.

In some instances, the mechanics or electronics of various headsets can cause remote parties to hear an echo of their own voice when they speak to Cisco Unified IP Phone users.

Cisco Systems recommends the use of good quality external devices, like headsets that are screened against unwanted radio frequency (RF) and audio frequency (AF) signals. Depending on the quality of these devices and their proximity to other devices such as cell phones and two-way radios, some audio noise may still occur. See the [“Using External Devices with Your Cisco Unified IP Phone” section on page 3-8](#) for more information.

The primary reason that support of a headset would be inappropriate for an installation is the potential for an audible hum. This hum can either be heard by the remote party or by both the remote party and the Cisco Unified IP Phone user. Some potential humming or buzzing sounds can be caused by a range of outside sources, for example, electric lights, being near electric motors, large PC monitors. In some cases, a hum experienced by a user may be reduced or eliminated by using a local power cube. See the “[Safety](#)” section on page 3-3 for more information.

Audio Quality Subjective to the User

Beyond the physical, mechanical and technical performance, the audio portion of a headset must sound good to the user and the party on the far end. Sound is subjective and Cisco cannot guarantee the performance of any headsets or handsets, but some of the headsets and handsets on the sites listed below have been reported to perform well on Cisco Unified IP Phones.

Nevertheless, it is ultimately still the customer’s responsibility to test this equipment in their own environment to determine suitable performance. For information about headsets, For information about headsets, refer to:

<http://www.vxicorp.com/cisco>

<http://www.plantronics.com>

Connecting a Headset

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

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

Disabling a Headset

You can disable the headset through the Cisco Unified CallManager Administration application. If you do so, you also will disable the speakerphone.

To disable the headset from Cisco Unified CallManager Administration, choose **Device > Phone** and locate the phone that you want to modify. In the Phone Configuration web page for the phone, check the **Disable Speakerphone and Headset** check box.

Using External Devices with Your Cisco Unified IP Phone

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

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

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

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

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



Caution

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

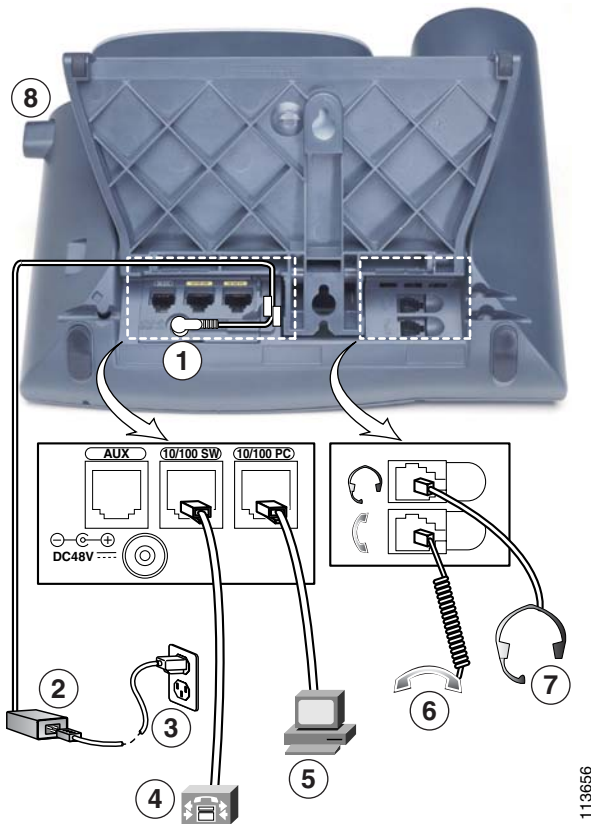
Installing the Cisco Unified IP Phone

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

To install a Cisco Unified IP Phone, perform these steps:

	Procedure	Notes	Reference
Step 1	Connect the handset to the Handset port.	—	—
Step 2	Connect a headset to the Headset port.	Optional. You can add a headset later if you do not connect one now.	See the “ Headset ” section on page 3-6 for supported headsets.
Step 3	Connect the power supply to the Cisco DC Adapter port.	Optional.	See the “ Adding Phones to the Cisco Unified CallManager Database ” section on page 2-12 for guidelines.

	Procedure	Notes	Reference
Step 4	Connect a Category 3 or 5 straight-through Ethernet cable from the switch to the network port labeled 10/100 SW on the Cisco Unified IP Phone 7961G/7941G, or to the network port labeled 10/100/1000 SW on the Cisco Unified IP Phone 7961G-GE/7941G-GE.	Each Cisco Unified IP Phone ships with one Ethernet cable in the box.	See the “ Network and Access Ports ” section on page 3-5 for guidelines.
Step 5	Connect a Category 3 or 5 straight-through Ethernet cable from another network device, such as a desktop computer, to the access port labeled 10/100 PC port on the Cisco Unified IP Phone 7961G/7941G, or to the access port labeled 10/100/1000 PC on the Cisco Unified IP Phone 7961G-GE/7941G-GE.	Optional. You can connect another network device later if you do not connect one now.	See the “ Network and Access Ports ” section on page 3-5 for guidelines.

Figure 3-1 Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE Cable Connections

113656

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

Related Topics

- [Adjusting the Placement of the Cisco Unified IP Phone, page 3-14](#)
- [Verifying the Phone Startup Process, page 3-17](#)
- [Configuring Startup Network Settings, page 3-19](#)
- [Configuring Security on the Cisco Unified IP Phone, page 3-19](#)

Attaching the Cisco Unified IP Phone Expansion Module 7914

The Cisco Unified IP Phone Expansion Module 7914 attaches to a Cisco Unified IP Phone 7961G and 7961G-GE to extend the number or line appearances or programmable buttons on your phone. You can customize the button templates for the Cisco Unified IP Phone Expansion Module 7914 to determine the number of line appearances and speed dial buttons. See the “[Modifying Phone Button Templates](#)” section on page 5-17 for details.

You can attach a Cisco Unified IP Phone Expansion Module 7914 to the Cisco Unified IP Phone 7961G and 7961G-GE:

- When you initially add the phone to Cisco Unified CallManager by selecting **7914 14-Button Line Expansion Module** in the Module 1 or Module 2 fields and selecting the appropriate expansion module firmware. See [Step 6](#) in the following procedure.
- After the phone is configured in Cisco Unified CallManager.

To configure the Cisco Unified IP Phone Expansion Module 7914 on the Cisco Unified IP Phone, follow these steps:

Procedure

Step 1 Log in to the Cisco Unified CallManager Administration application. The Cisco Unified CallManager Administration page appears.

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

The Find and List Phone page appears. You can search for one or more phones that you want to configure for the Cisco Unified IP Phone Expansion Module 7914.

- Step 3** Select and enter your search criteria and click **Find**.
- The Find and List Phone page reappears showing a list of the phones matching your search criteria.
- Step 4** Click the IP Phone that you want to configure for the Cisco Unified IP Phone Expansion Module 7914.
- The Phone Configuration page appears.
- Step 5** Scroll to the Expansion Module Information section of the page.
- Step 6** To add support for one expansion module, in the Module 1 field, select **7914 14-Button Line Expansion Module**.
- To add support for a second expansion module, in the Module 2 field, select **7914 14-Button Line Expansion Module**.
- In the Firmware Load Information section of the page, there are two fields for specifying the firmware load for Modules 1 and 2. You can leave these fields blank to use the default firmware load.
- Step 7** Scroll to the top of the page and click **Update**.
- A message appears asking you to reset the phone for the changes to take effect. Click **OK**.
- Step 8** Click **Reset Phone** for the changes to take effect.
-

**Note**

Refer users to their Cisco Unified CallManager User Options web pages so that they can configure speed dial buttons and program buttons to access phone services on the Cisco Unified IP Phone Expansion Module 7914. See the [“How Users Subscribe to Services and Configure Phone Features”](#) section on page A-4 for more details.

Related Topic

- [Configuring Softkey Templates, page 5-18](#)

Adjusting the Placement of the Cisco Unified IP Phone

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

Adjusting Cisco Unified IP Phone Placement on the Desktop

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

Procedure

-
- | | |
|---------------|--|
| Step 1 | Push in the footstand adjustment button. |
| Step 2 | Adjust the footstand to desired height. |
-

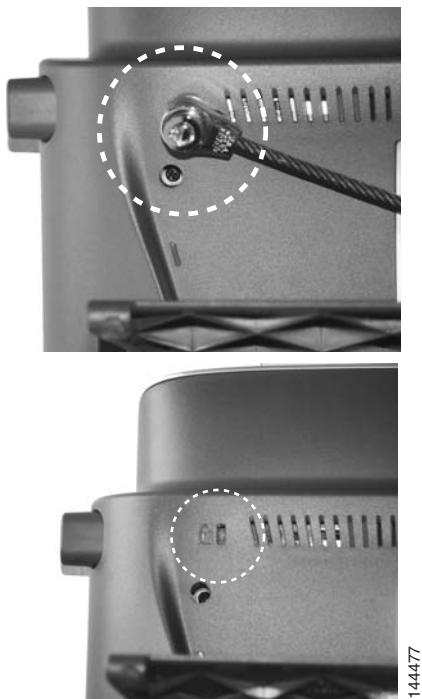
Securing the Phone with a Cable Lock

You can secure the Cisco Unified IP Phone 7961G and 7941G to a desktop using a laptop cable lock. The lock connects to the security slot on the back of the phone and the cable can be secured to a desktop.

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

See [Figure 3-2](#).

Figure 3-2 **Connecting a Cable Lock to the Cisco Unified IP Phone 79761G/7961G-GE and 7941G/7941G-GE**



Mounting the Phone to the Wall

You can mount the Cisco Unified IP Phone on the wall using the footstand as a mounting bracket or you can use special brackets available in a Cisco Unified IP Phone wall mount kit. (Wall mount kits must be ordered separately from the phone.) If you attach the Cisco Unified IP Phone to a wall using the standard footstand and not the wall mount kit, you need to supply the following tools and parts:

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

See [Figure 3-3](#) for a graphical overview of the phone parts.

Before You Begin

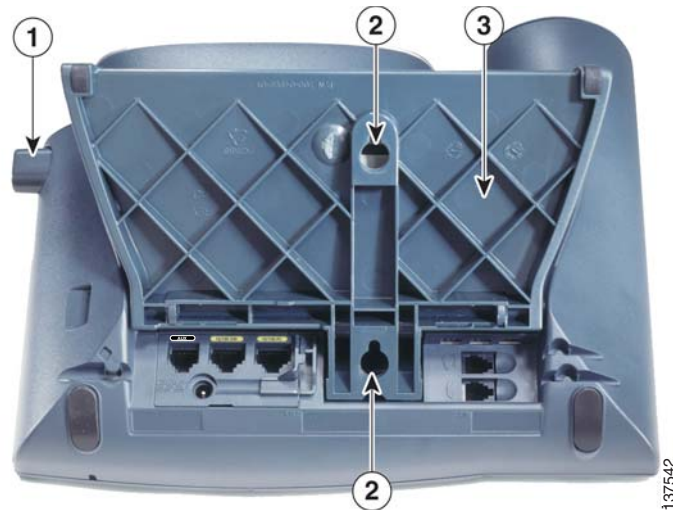
To ensure that the handset attaches securely to a wall-mounted phone, remove the handset wall hook from the handset rest, rotate the hook 180 degrees, and reinsert the hook. Turning the hook exposes a lip on which the handset catches when the phone is vertical. For an illustrated procedure, refer to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

**Caution**

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

Procedure

-
- Step 1** Push in the footstand adjustment button.
 - Step 2** Adjust the footstand so it is flat against the back of the phone.
 - Step 3** Insert two screws into a wall stud, matching them to the two screw holes on the back of the footstand.
The keyholes fit standard phone jack mounts.
 - Step 4** Hang the phone on the wall.
-

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

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

Verifying the Phone Startup Process

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

1. These buttons flash on and off in sequence:
 - Headset (only if the handset is off-hook when the phone powers up. In this case, hang up the handset within 3 seconds or the phone launches its secondary load instead of its primary load.)
 - Mute
 - Speaker

2. Some or all of the line keys flash amber in sequence.

**Caution**

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

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

Normally, this sequence takes just a few seconds. However, if the phone's Flash memory is erased or the phone load is corrupted, the sequence of green flashes will continue while the phone begins a software update procedure. If the phone performs this procedure, the following buttons light to indicate progress:

- Headset—Phone is waiting for the network and completing CDP and DHCP configuration. (A DHCP server must be available in your network.)
 - Mute—Phone is downloading images from the TFTP server.
 - Speaker—Phone is writing images to its Flash memory.
4. The LCD screen displays the Cisco Systems, Inc., logo screen.
 5. These messages appear as the phone starts:
 - Verifying Load (if the phone load does not match the load on the TFTP server). If this message appears, the phone starts up again and repeats step 1 through step 4 above.
 - Configuring IP
 - Updating CTL
 - Updating Locale
 - Configuring CM List
 - Registering
 6. The main LCD screen displays:
 - Current date and time
 - Primary directory number
 - Additional directory numbers and speed dial numbers, if configured
 - Softkeys

If the phone successfully passes through these stages, it has started up properly. If the phone does not start up properly, see the [“Resolving Startup Problems” section on page 9-2](#).

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 mask
- Default gateway IP address
- TFTP server IP address
- You also may configure the domain name and the DNS server settings, if necessary.

Collect this information and see the instructions in [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 CallManager 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 1-11](#). Also, refer to *Cisco Unified CallManager Security Guide*.

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

Alternatively, 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 do so, make sure that the appropriate Cisco Unified CallManager and the Certificate Authority Proxy Function (CAPF) security configurations are complete:

- The CTL file should have a CAPF certificate.
- The CAPF certificate must exist in the /usr/local/cm/.security/certs folder in every server in the cluster.
- The CAPF is running and configured.
- The phone should have the correct load file. To verify the image, choose **Settings > Status > Firmware Versions**. The application load file should begin with P00307.

Refer to *Cisco Unified CallManager Security Guide* for more information.

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

Procedure

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

Step 2 From the phone, choose **Settings > Security Configuration**.



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

Step 3 Press ****#** to unlock settings on the Security Configuration menu.

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

The phone prompts for an authentication string.

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

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

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

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

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

Related Topic

- [Understanding Security Features for Cisco Unified IP Phones, page 1-11](#)



Configuring Settings on the Cisco Unified IP Phone

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

This chapter includes the following topics:

- [Configuration Menus on the Cisco Unified IP Phone, page 4-1](#)
- [Overview of Options Configurable from a Phone, page 4-5](#)
- [Network Configuration Menu, page 4-7](#)
- [Device Configuration Menu, page 4-15](#)
- [Security Configuration Menu, page 4-29](#)

Configuration Menus on the Cisco Unified IP Phone

The Cisco Unified IP Phone includes the following configuration menus:

- **Network Configuration menu**—Provides options for viewing and making a variety of network settings. For more information, see the [“Network Configuration Menu” section on page 4-7](#).
- **Device Configuration menu**—Provides access to sub-menus from which you can view a variety of non network-related settings. For more information, see the [“Device Configuration Menu” section on page 4-15](#).

- Security Configuration menu—Provides options for displaying and modifying security settings. For more information, see the [“Security Configuration Menu” section on page 4-25](#).

Before you can change option settings on the Network Configuration menu, you must unlock options for editing. See the [“Unlocking and Locking Options” section on page 4-4](#) for instructions.

For information about the keys you can use to edit or change option settings, see the [“Editing Values” section on page 4-4](#).

You can control whether a phone user has access to phone settings by using the Settings Access field in the Cisco Unified CallManager Administration Phone Configuration Settings page. See the *Cisco Unified CallManager Administration Guide* for more information.

Related Topics

- [Displaying a Configuration Menu, page 4-2](#)
- [Unlocking and Locking Options, page 4-4](#)
- [Editing Values, page 4-4](#)
- [Overview of Options Configurable from a Phone, page 4-5](#)
- [Network Configuration Menu, page 4-7](#)
- [Device Configuration Menu, page 4-15](#)

Displaying a Configuration Menu

To display a configuration menu, perform the following steps.

Procedure

-
- | | |
|---------------|--|
| Step 1 | Press the Applications Menu button. |
| Step 2 | Choose Settings . |

- Step 3** Perform one of these actions to display the desired menu:
- Use the **Navigation** button to select the desired menu and then press the **Select** softkey.
 - Use the keypad on the phone to enter the number that corresponds to the menu.
- Step 4** To display a submenu repeat [Step 3](#).
- Step 5** To exit a menu, press the **Exit** softkey.
-

**Note**

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

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

If you cannot access an option on the Settings menu, check the Settings Access field. For more information, see the *Cisco Unified CallManager Administration Guide*.

Related Topics

- [Unlocking and Locking Options, page 4-4](#)
- [Editing Values, page 4-4](#)
- [Overview of Options Configurable from a Phone, page 4-5](#)
- [Network Configuration Menu, page 4-7](#)
- [Device Configuration Menu, page 4-15](#)

Unlocking and Locking Options

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

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

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

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



Caution

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

Related Topics

- [Displaying a Configuration Menu, page 4-2](#)
- [Editing Values, page 4-4](#)
- [Overview of Options Configurable from a Phone, page 4-5](#)
- [Network Configuration Menu, page 4-7](#)
- [Device Configuration Menu, page 4-15](#)

Editing Values

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

- Use the keys on the keypad to enter numbers and letters.

- To enter letters using the keypad, use a corresponding number key. Press the key one or more times to display a particular letter. For example, press the 2 key once for “a,” twice quickly for “b,” and three times quickly for “c.” After you pause, the cursor automatically advances to allow you to enter the next letter.
- To enter a period (for example, in an IP address), press the . (period) softkey or press * on the keypad.
- Press the << softkey if you make a mistake. This softkey deletes the character to the left of the cursor.
- Press the **Cancel** softkey before pressing the **Save** softkey to discard any changes that you have made.

**Note**

The Cisco Unified IP Phone provides several methods you can use to reset or restore option settings, if necessary. For more information, see the [“Resetting or Restoring the Cisco Unified IP Phone” section on page 9-17](#).

Related Topics

- [Displaying a Configuration Menu, page 4-2](#)
- [Unlocking and Locking Options, page 4-4](#)
- [Overview of Options Configurable from a Phone, page 4-5](#)
- [Network Configuration Menu, page 4-7](#)
- [Device Configuration Menu, page 4-15](#)

Overview of Options Configurable from a Phone

The settings that you can change on a phone fall into several categories, as shown in [Table 4-1](#). For a detailed explanation of each setting and instructions for changing them, see the [“Network Configuration Menu” section on page 4-7](#).

**Note**

There are several options on the Network Configuration menu and on the Device Configuration Menu that are for display only or that you can configure from Cisco Unified CallManager. These options are also described in the [“Network Configuration Menu”](#) section on page 4-7 or the [“Device Configuration Menu”](#) section on page 4-15.

Table 4-1 *Settings Configurable from a Cisco Unified IP Phone*

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

Related Topics

- [Displaying a Configuration Menu, page 4-2](#)

- [Unlocking and Locking Options, page 4-4](#)
- [Editing Values, page 4-4](#)
- [Network Configuration Menu, page 4-7](#)
- [Device Configuration Menu, page 4-15](#)

Network Configuration Menu

The Network Configuration menu provides options for viewing and making a variety of network settings. [Table 4-2](#) describes these options and, where applicable, explains how to change them.

For information about how to access the Network Configuration menu, see the [“Displaying a Configuration Menu” section on page 4-2](#).

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

For information about the keys you can use to edit options, see the [“Editing Values” section on page 4-4](#).

Table 4-2 **Network Configuration Menu Options**

Option	Description	To Change
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address.	Display only—cannot configure.
BOOTP Server	Indicates whether the phone obtains its configuration from a Bootstrap Protocol (BootP) server instead of from a DHCP server.	Display only—cannot configure.
MAC Address	Unique Media Access Control (MAC) address of the phone.	Display only—cannot configure.
Host Name	Unique host name that the DHCP server assigned to the phone.	Display only—cannot configure.

Table 4-2 **Network Configuration Menu Options (continued)**

Option	Description	To Change
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.	1. Unlock network configuration options. 2. Set the DHCP Enabled option to No. 3. Scroll to the Domain Name option, press the Edit softkey, and then enter a new domain name. 4. Press the Validate softkey and then press the Save softkey.
IP Address	Internet Protocol (IP) address of the phone. If you assign an IP address with this option, you must also assign a subnet mask and default router. See the Subnet Mask and Default Router options in this table.	1. Unlock network configuration options. 2. Set the DHCP Enabled option to No. 3. Scroll to the IP Address option, press the Edit softkey, and then enter a new IP Address. 4. Press the Validate softkey and then press the Save softkey.
Subnet Mask	Subnet mask used by the phone.	1. Unlock network configuration options. 2. Set the DHCP Enabled option to No. 3. Scroll to the Subnet Mask option, press the Edit softkey, and then enter a new subnet mask. 4. Press the Validate softkey and then press the Save softkey.

Table 4-2 **Network Configuration Menu Options (continued)**

Option	Description	To Change
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone. If you are not using DHCP in your network and you want to change this server, you must use the TFTP Server 1 option. If you set the Alternate TFTP option to yes, you must enter a non-zero value for the TFTP Server 1 option. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL file on the phone, you must unlock the CTL file before you can save changes to the TFTP Server 1 option. In this case, the phone will delete the CTL file when you save changes to the TFTP Server 1 option. For information about the CTL file, refer to <i>Cisco Unified CallManager Security Guide</i>. For information about unlocking the CTL file, see the “Security Configuration Menu” section on page 4-25.	1. Unlock the CTL file, if necessary. 2. If DHCP is enabled, set the Alternate TFTP option to Yes. 3. Scroll to the TFTP Server 1 option, press the Edit softkey, and then enter a new TFTP server IP address. 4. Press the Validate softkey, and then press the Save softkey.

Table 4-2 Network Configuration Menu Options (continued)

Option	Description	To Change
TFTP Server 2	Optional backup TFTP server that the phone uses if the primary TFTP server is unavailable. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL file on the phone, you must unlock the CTL file before you can save changes to the TFTP Server 2 option. In this case, the phone will delete the CTL file when you save changes to the TFTP Server 2 option. For information about the CTL file, refer to <i>Cisco Unified CallManager Security Guide</i>. For information about unlocking the CTL file, see to the “Security Configuration Menu” section on page 4-25.	1. Unlock the CTL file, if necessary. 2. Unlock network configuration options. 3. Enter an IP address for the TFTP Server 1 option. 4. Scroll to the TFTP Server 2 option, press the Edit softkey, and then enter a new backup TFTP server IP address. 5. Press the Validate softkey, and then press the Save softkey.
Default Router 1 Default Router 2 Default Router 3 Default Router 4 Default Router 5	Default router used by the phone (Default Router 1) and optional backup routers (Default Router 2–5).	1. Unlock network configuration options. 2. Set the DHCP Enabled option to No. 3. Scroll to the appropriate Default Router option, press the Edit softkey, and then enter a new router IP address. 4. Press the Validate softkey. 5. Repeat Steps 3 and 4 as needed to assign backup routers. 6. Press the Save softkey.

Table 4-2 **Network Configuration Menu Options (continued)**

Option	Description	To Change
DNS Server 1 DNS Server 2 DNS Server 3 DNS Server 4 DNS Server 5	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) used by the phone.	1. Unlock network configuration options. 2. Set the DHCP Enabled option to No. 3. Scroll to the appropriate DNS Server option, press the Edit softkey, and then enter a new DNS server IP address. 4. Press the Validate softkey. 5. Repeat Steps 3 and 4 as needed to assign backup DNS servers. 6. Press the Save softkey.
Operational VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member. If the phone has not received an auxiliary VLAN, this option indicates the Administrative VLAN. If neither the auxiliary VLAN nor the Administrative VLAN are configured, this option is blank.	The phone obtains its Operational VLAN ID via Cisco Discovery Protocol (CDP) from the switch to which the phone is attached. To assign a VLAN ID manually, use the Admin VLAN ID option.
Admin. VLAN ID	Auxiliary VLAN in which the phone is a member. Used only if the phone does not receive an auxiliary VLAN from the switch, ignored otherwise.	1. Unlock network configuration options. 2. Scroll to the Admin. VLAN ID option, press the Edit softkey, and then enter a new Admin VLAN setting. 3. Press the Validate softkey and then press the Save softkey.
DHCP Enabled	Indicates whether DHCP is being used by the phone.	1. Unlock network configuration options. 2. Scroll to the DHCP Enabled option and press the No softkey to disable DHCP, or press the Yes softkey to enable DHCP. 3. Press the Save softkey.

Table 4-2 **Network Configuration Menu Options (continued)**

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

Table 4-2 **Network Configuration Menu Options (continued)**

Option	Description	To Change
SW Port Configuration	Speed and duplex of the network port (labeled 10/100 SW on the 7961G and 7941G; labeled 10/100/100 SW on the 7961G-GE and 7941G-GE). Valid values: • Auto Negotiate • 10 Half—10-BaseT/half duplex • 10 Full—10-BaseT/full duplex • 100 Half—100-BaseT/half duplex • 100 Full—100-BaseT/full duplex • 1000 Full—1000-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to auto-negotiate. If you change the setting of this option, you must change the PC Port Configuration option to the same setting.	1. Unlock network configuration options. 2. Scroll to the SW Port Configuration option and then press the Edit softkey. 3. Scroll to the setting that you want and then press the Select softkey. 4. Press the Save softkey.

Table 4-2 **Network Configuration Menu Options (continued)**

Option	Description	To Change
PC Port Configuration	Speed and duplex of the access port (labeled 10/100 PC on the 7961G and 7941G; labeled 10/100/100 PC on the 7961G-GE and 7941G-GE). Valid values: • Auto Negotiate • 10 Half—10-BaseT/half duplex • 10 Full—10-BaseT/full duplex • 100 Half—100-BaseT/half duplex • 100 Full—100-BaseT/full duplex • 1000 Full—1000-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to auto-negotiate. If you change the setting of this option, you must change the SW Port Configuration option to the same setting.	1. Unlock network configuration options. 2. Scroll to the PC Port Configuration option and then press the Edit softkey. 3. Scroll to the setting that you want and then press the Select softkey. 4. Press the Save softkey.
PC VLAN	Allows the phone to interoperate with third-party switches that do not support a voice VLAN. The Admin VLAN ID option must be set before using this option.	1. Unlock network configuration options. 2. Make sure the Admin VLAN ID is set (see Admin VLAN ID above in this table). 3. Scroll to the PC VLAN option, press the Edit softkey, and then enter a new PC VLAN setting. 4. Press the Validate softkey and then press the Save softkey.

Related Topics

- [Displaying a Configuration Menu, page 4-2](#)
- [Unlocking and Locking Options, page 4-4](#)
- [Editing Values, page 4-4](#)
- [Overview of Options Configurable from a Phone, page 4-5](#)
- [Device Configuration Menu, page 4-15](#)

Device Configuration Menu

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

- [CallManager Configuration Menu, page 4-15](#)
- [HTTP Configuration Menu, page 4-17](#)
- [Locale Configuration Menu, page 4-18](#)
- [UI Configuration Menu, page 4-19](#)
- [Media Configuration Menu, page 4-21](#)
- [Ethernet Configuration Menu, page 4-24](#)
- [Security Configuration Menu, page 4-25](#)
- [QoS Configuration Menu, page 4-27](#)
- [Network Configuration Menu, page 4-27](#)

For instructions about how to access the Device Configuration menu and its sub-menus, see the “[Displaying a Configuration Menu](#)” section on [page 4-2](#).

CallManager Configuration Menu

The CallManager Configuration menu contains the options CallManager 1, CallManager 2, CallManager 3, CallManager 4, and CallManager 5. These options show Cisco Unified CallManager servers that are available for processing calls from the phone, in prioritized order.

To change these options, use Cisco Unified CallManager Administration.

For an available Cisco Unified CallManager server, an option on the CallManager Configuration menu will show the Cisco Unified CallManager server IP address or name and one of the following states:

- **Active**—Cisco Unified CallManager server from which the phone is currently receiving call-processing services.
- **Standby**—Cisco Unified CallManager server to which the phone switches if the current server becomes unavailable.
- **Blank**—No current connection to this Cisco Unified CallManager server.

An option may also display one of more of the following designations or options:

- **SRST designation**—Indicates a Survivable Remote Site Telephony router capable of providing Cisco Unified CallManager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified CallManager servers become unreachable. The SRST Cisco Unified CallManager always appears last in the list of servers, even if it is active.

You configure an SRST router address in the Cisco Unified CallManager Administration SRST Reference Configuration page (choose **System > SRST**). You configure an SRST reference in the Device Pool Configuration page (choose **System > Device Pool**).

- **TFTP designation**—Indicates that the phone was unable to register with a Cisco Unified CallManager listed in its configuration file and it registered with the TFTP server instead.
- **Authentication icon**—Appears as a shield  and indicates that the connection to the Cisco Unified CallManager is authenticated. For more information about authentication, refer to *Cisco Unified CallManager Security Guide*.
- **Encrypted icon**—Appears as a padlock  and indicates that the connection to the Cisco Unified CallManager is authenticated and encrypted. For more information about authentication and encryption, refer to *Cisco Unified CallManager Security Guide*.

HTTP Configuration Menu

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

Table 4-3 describes the options on the HTTP Configuration menu.

Table 4-3 *HTTP Configuration Menu Options*

Option	Description	To Change
Directories URL	URL of the server from which the phone obtains directory information.	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.	Use Cisco Unified CallManager Administration to modify > Device > Phone > Phone Configuration .
Messages URL	URL of the server from which the phone obtains message services.	Use Cisco Unified CallManager Administration to modify > Device > Phone > Phone Configuration .
Information URL	URL of the help text that appears on the phone.	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .
Authentication URL	URL that the phone uses to validate requests made to the phone web server.	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .
Proxy Server URL	URL of proxy server, which makes HTTP requests to non-local host addresses on behalf of the phone HTTP client and provides responses from the non-local host to the phone HTTP client.	Use Cisco Unified CallManager Administration to modify > Device > Phone > Phone Configuration .

Table 4-3 HTTP Configuration Menu Options (continued)

Option	Description	To Change
Idle URL	URL of an XML service that the phone displays when the phone has not been used for the time specified in the Idle URL Time option and no menu is open. For example, you could use the Idle URL option and the Idle URL Timer option to display a stock quote or a calendar on the LCD screen when the phone has not been used for 5 minutes.	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .
Idle URL Time	Number of seconds that the phone has not been used and no menu is open before the XML service specified in the Idle URL option is activated.	Use Cisco Unified CallManager Administration to modify > Device > Phone > Phone Configuration .

Locale Configuration Menu

The Locale Configuration menu displays information about the user locale and the network locale used by the phone. [Table 4-4](#) describes the options on this menu.

Table 4-4 Locale Configuration Menu Options

Option	Description	To Change
User Locale	User locale associated with the phone user. The user locale identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .
User Locale Version	Version of the user locale loaded on the phone.	Display only—cannot configure.
User Locale Char Set	Character set that the phone uses for the user locale.	Display only—cannot configure.

Table 4-4 *Locale Configuration Menu Options (continued)*

Option	Description	To Change
Network Locale	Network locale associated with the phone user. The network locale identifies a set of detailed information that supports the phone in a specific location, including definitions of the tones and cadences used by the phone.	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .
Network Locale Version	Version of the network locale loaded on the phone.	Display only—cannot configure.

UI Configuration Menu

The UI Configuration menu displays the status of various user interface features on the phone.

contains the option Auto Line Select Enabled. This option indicates whether the phone shifts the call focus to incoming calls on all lines.

When this option is set to No (disabled), the phone will only shift the call focus to incoming calls on the line that is in use. When this option is set to Yes, the phone will shift the call focus to the line with the most recent incoming call.

You can change this option on the Cisco Unified CallManager Administration Phone Configuration page. [Table 4-5](#) describes the options on this menu.

Table 4-5 *UI Configuration Menu Options*

Option	Description	To Change
Auto Call Select	Indicates whether the phone automatically shifts the call focus to an incoming call on the same line when the user is already on a call. When this option is enabled, the phone shifts the call focus to the most recent incoming call. When this option is disabled, all automatic focus changes, including Auto Line Select, are disabled regardless of their setting. Default: Enabled	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .
Auto Line Select	Indicates whether the phone shifts the call focus to incoming calls on all lines. When this option is disabled, the phone only shifts the call focus to incoming calls on the line that is in use. When this option is enabled, the phone shifts the call focus to the line with the most recent incoming call. Default: Disabled	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .

Table 4-5 UI Configuration Menu Options (continued)

Option	Description	To Change
BLF for Call Lists	Indicates whether the Busy Lamp Field (BLF) is enabled for call lists.	Use Cisco Unified CallManager Administration > System > Enterprise Parameters .
“more” Softkey Timer	Indicates the number of seconds that additional softkeys are displayed after the user presses more . If this timer expires before the user presses another softkey, the display reverts to the initial softkeys. Range: 5 to 30; 0 represents an infinite timer. Default: 5	Access the Phone Configuration page in Cisco Unified CallManager Administration.

Media Configuration Menu

The Media Configuration menu displays whether the headset, speakerphone, and video capability are enabled on the phone. This menu also displays options for recording tones that the phone may play to indicate that a call may be recorded. [Table 4-6](#) describes the options on this menu.

Table 4-6 Media Configuration Menu Options

Option	Description	To Change
Headset Enabled	Indicates whether the Headset button is enabled on the phone.	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .
Speaker Enabled	Indicates whether the speakerphone is enabled on the phone.	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .
Video Capability Enabled	Indicates whether the phone can participate in video calls when connected to an appropriately equipped computer.	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .

Table 4-6 Media Configuration Menu Options (continued)

Option	Description	To Change
Recording Tone	Indicates whether a recording tone (often referred to as a <i>beep tone</i>) is enabled or disabled for the phone. If the recording tone option is enabled, the phone plays the beep tone in both directions of every call, regardless of whether the call actually gets recorded. The beep tone first sounds when a call is answered. You may want to notify your users if you enable this option. Default: Disabled Related Parameters: • Recording Tone Local Volume • Recording Tone Remote Volume • Recording Tone Duration  Note Other related parameters—Beep tone frequency in hz, the length of the beep tone (called <i>duration</i>), and how often the beep tone plays (called <i>interval</i>)—are defined on a per-Network Locale basis in the xml file that defines tones. This xml file is usually named tones.xml or g3-tones.xml.	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .

Table 4-6 **Media Configuration Menu Options (continued)**

Option	Description	To Change
Recording Tone Local Volume	Indicates the loudness setting for the beep tone that is received by the party whose phone has the Recording Tone option enabled. This setting applies for each listening device (handset, speakerphone, headset). Range: 0 percent (no tone) to 100 percent (same level as current volume setting on the phone). Default: 100 See also: Recording Tone	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .

Table 4-6 Media Configuration Menu Options (continued)

Option	Description	To Change
Recording Tone Remote Volume	Indicates the loudness setting for the beep tone that the <i>remote party</i> receives. The <i>remote party</i> is the party who is on a call with the party whose phone has the Recording Tone option enabled. Range: 0 percent to 100 percent. (0 percent is -66 dBm and 100 percent is -3 dBm.) Default: 84 percent (-10dBm) See also: Recording Tone	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .
Recording Tone Duration	Indicates the length of time in milliseconds for which the beep tone plays. If the value you configure here is less than one third the interval, then this value overrides the default provided by the Network Locale. Range: 0 to 3000  Note For some Network Locales that use a complex cadence, this setting applies only to the first beep tone. See also: Recording Tone	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .

Ethernet Configuration Menu

The Ethernet Configuration menu includes the Span to PC Port option. This option indicates whether the phone will forward packets transmitted and received on the network port to the access port.

Enable this option if an application that requires monitoring of the phone's traffic is being run on the access port. These applications include monitoring and recording applications (common in call center environments) and network packet capture tools that are used for diagnostic purposes.

Use Cisco Unified CallManager Administration > **Device** > **Phone** > **Phone Configuration**.

Security Configuration Menu

The Security Configuration menu that you display from the Device Configuration menu displays settings that relate to security for the phone.



Note

The phone also has a Security Configuration menu that you access directly from the Settings menu. For information about the security options on that menu, see the [“Security Configuration Menu” section on page 4-29](#).

[Table 4-7](#) describes the options on the Security Configuration menu.

Table 4-7 **Security Configuration Menu Options**

Option	Description	To Change
PC Port Disabled	Indicates whether the access port on the phone is enabled (Yes) or disabled (No). Must be set to enabled for video support on the phone	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous Address Resolution Protocol (ARP) responses. Disabling the phone's ability to accept Gratuitous ARP will prevent applications that use this mechanism to monitor and record voice streams from working. If voice monitoring is not desired, set this option to No (disabled).	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .

Table 4-7 Security Configuration Menu Options (continued)

Option	Description	To Change
Voice VLAN Enabled	Indicates whether the phone allows a device attached to the access port to access the Voice VLAN. Setting this option to No (disabled) prevents the attached PC from sending and receiving data on the Voice VLAN. This setting also prevents the PC from receiving data sent and received by the phone. Set this setting to Yes (enabled) if an application that requires monitoring of the phone's traffic is running on the PC. These applications include monitoring and recording applications and network monitoring software.	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .
Security Mode	Displays the security mode that is set for the phone.	Use Cisco Unified CallManager Administration to modify.
Logging Display	For use by the Cisco Technical Assistance Center (TAC), if necessary.	

QoS Configuration Menu

The QoS Configuration menu displays information that relates to quality of service (QoS) for the phone. [Table 4-8](#) describes the options on this menu.

Table 4-8 *QoS Configuration Menu Options*

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

Related Topics

- [Displaying a Configuration Menu, page 4-2](#)
- [Network Configuration Menu, page 4-7](#)

Network Configuration Menu

The Network Configuration menu displays device-specific network configuration settings on the phone. [Table 4-9](#) describes the options in this menu.

Table 4-9 Network Configuration Menu Options

Option	Description	To Change
Load Server	Used to optimize installation time for phone firmware upgrades and offload the WAN by storing images locally, negating the need to traverse the WAN link for each phone's upgrade. You can set the Load Server to another TFTP server IP address or name (other than the TFTP Server 1 or TFTP Server 2) from which the phone firmware can be retrieved for phone upgrades. When the Load Server option is set, the phone contacts the designated server for the firmware upgrade. Note The Load Server option allows you to specify an alternate TFTP server for phone upgrades only. The phone continues to use TFTP Server 1 or TFTP Server 2 to obtain configuration files. The Load Server option does not provide management of the process and of the files, such as file transfer, compression, deletion, and so on.	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .

Table 4-9 Network Configuration Menu Options (continued)

Option	Description	To Change
RTP Control Protocol	Indicates whether the phone supports the Real Time Control Protocol. Settings include: Enabled Disabled—default If this feature is disabled, several call statistic values display as 0. For additional information, see the following sections: • Call Statistics Screen, page 7-17 • Streaming Statistics, page 8-13	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration.

- Related Topics**
- [Displaying a Configuration Menu, page 4-2](#)
 - [Network Configuration Menu, page 4-7](#)

Security Configuration Menu

The Security Configuration menu that you access directly from the Settings menu provides information about various security setting. It also provides access to the CTL File screen and the Trust List menu, if a CTL file is installed on the phone.

[Table 4-10](#) describes the options in this menu.



Note

The phone also has a Security Configuration menu that you access from the Device menu. For information about the security options on that menu, see the [“Security Configuration Menu” section on page 4-25](#).

Table 4-10 Security Menu Settings

Option	Description	To Change
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .
Security Mode	Displays the security mode that is set for the phone.	Use Cisco Unified CallManager Administration > Device > Phone > Phone Configuration .
MIC	Indicates whether a manufacturing installed certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).	For information about how to manage the MIC for your phone, refer to the “Using the Certificate Authority Proxy Function” chapter in <i>Cisco Unified CallManager Security Guide</i> .
LSC	Indicates whether a locally significant certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No).	For information about how to manage the LSC for your phone, refer to the “Using the Certificate Authority Proxy Function” chapter in <i>Cisco Unified CallManager Security Guide</i> .
CTL File	Displays the MD5 hash of the certificate trust list (CTL) file that is installed in the phone, and provides access to the CTL File menu. If no CTL file is installed on the phone, this field displays No. (If security is configured for the phone, the CTL file installs automatically when the phone reboots or resets.	For more information about this file, refer to the “Configuring the Cisco CTL Client” chapter in <i>Cisco Unified CallManager Security Guide</i> . If a CTL file is installed on the phone, also provides access to the CTL File screen. For more information, see “ CTL File Screen ” section on page 4-31.
Trust List	If a CTL file is installed on the phone, provides access to the Trust List menu.	For more information, see the “ Trust List Screen ” section on page 4-33.
CAPF Server	Displays the IP address and the port of the CAPF that the phone uses.	For more information about this server, refer to the “Using the Certificate Authority Proxy Function” section in <i>Cisco Unified CallManager Security Guide</i> .

Table 4-10 Security Menu Settings (continued)

Option	Description	To Change
802.1X Authentication	Allows you to enable 802.1X authentication for this phone.	See the “802.1X Authentication and Status” section on page 4-34.
802.1X Authentication Status	Displays real-time status progress of the 802.1X authentication transaction.	Display only—Cannot configure.

CTL File Screen

The CTL File screen includes the options described in [Table 4-11](#)

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

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

Table 4-11 **CTL File Settings**

Option	Description	To Change
CTL File	Displays the MD5 hash of the CTL file that is installed in the phone. If security is configured for the phone, the CTL file installs automatically when the phone reboots or resets. • A locked padlock icon  in this option indicates that the CTL file is locked. • An unlocked padlock icon  indicates that the CTL file is unlocked.	For more information about this file, refer to the “Configuring the Cisco CTL Client” section in <i>Cisco Unified CallManager Security Guide</i> .
CAPF Server	IP address of the CAPF used by the phone. Also displays a certificate icon  if a certificate is installed for this server.	For more information about this server, refer to the “Using the Certificate Authority Proxy Function” section in <i>Cisco Unified CallManager Security Guide</i> .
CallManager / TFTP Server	IP address of a Cisco Unified CallManager and TFTP server used by the phone. Also displays a certificate icon  if a certificate is installed for this server. If neither the primary TFTP (TFTP Server 1) server nor the backup TFTP server (TFTP Server 2) is listed in the CTL file, you must unlock the CTL file before you can save changes that you make to the TFTP Server 1 option or to the TFTP Server 2 option on the Network Configuration menu.	For information about changing these options, see the “Network Configuration Menu” section on page 4-7.

Unlocking the CTL File

To unlock the CTL file from the Security Configuration screen, follow these steps:

Procedure

- Step 1** Press ****#** to unlock options on the Security Configuration menu.
If you decide not to continue, press ****#** again to lock options on this menu.



Note If a password is configured on the phone, you must enter a password after pressing ****#**.

- Step 2** Highlight the CTL File option.

- Step 3** Press the **Unlock** softkey to unlock the CTL file.

After you change and save the TFTP Server 1 or the TFTP Server 2 option, the CTL file will be locked automatically.



Note When you press the **Unlock** softkey, it changes to **Lock**. If you decide not to change the TFTP Server 1 or TFTP Server 2 option, press the **Lock** softkey to lock the CTL file.

Trust List Screen

The Trust List menu displays information about all of the servers that the phone trusts and includes the options described in [Table 4-12](#).

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

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

Table 4-12 Trust List Menu Settings

Option	Description	To Change
CAPF Server	IP address of the CAPF used by the phone. Also displays a certificate icon  if a certificate is installed for this server.	For more information about this file, refer to the “Configuring the Cisco CTL Client” section in <i>Cisco Unified CallManager Security Guide</i> .
CallManager/TF TP Server	IP address of a Cisco Unified CallManager and TFTP server used by the phone. Also displays a certificate icon  if a certificate is installed for this server.	For more information about this file, refer to the “Configuring the Cisco CTL Client” section in <i>Cisco Unified CallManager Security Guide</i> .
SRST Router	IP address of the trusted SRST router that is available to the phone, if such a device has been configured in Cisco Unified CallManager Administration. Also displays a certificate icon  if a certificate is installed for this server.	For more information about this file, refer to the “Configuring the Cisco CTL Client” section in <i>Cisco Unified CallManager Security Guide</i> .

802.1X Authentication and Status

The 802.1X Authentication and 802.1X Authentication Status menus allow you to enable 802.1X authentication and monitor its progress. These options are described in [Table 4-13](#) and [Table 4-14](#).

You can access the 802.1X Authentication settings by pressing the **Settings** button and choosing **Security Configuration > 802.1X Authentication**.

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

Table 4-13 802.1X Authentication Settings

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

You can access the 802.1X Authentication Real-Time Stats by pressing the **Settings** button and choosing **Security Configuration > 802.1X Authentication Status**. To exit this menu, press the **Exit** key.

Table 4-14 802.1X Authentication Real-Time Status

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



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 CallManager, you must use the Cisco Unified CallManager 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 CallManager documentation provides detailed instructions for these procedures.

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

For information about setting up phones in non-English environments, see [Appendix B, “Supporting International Users.”](#)

This chapter includes following topics:

- [Telephony Features Available for the Cisco Unified IP Phone, page 5-2](#)
- [Configuring Corporate and Personal Directories, page 5-16](#)
- [Modifying Phone Button Templates, page 5-17](#)
- [Configuring Softkey Templates, page 5-18](#)

- [Setting Up Services, page 5-18](#)
- [Adding Users to Cisco Unified CallManager, page 5-19](#)
- [Managing the User Options Web Pages, page 5-20](#)

Telephony Features Available for the Cisco Unified IP Phone

After you add Cisco Unified IP Phones to Cisco Unified CallManager, 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 CallManager Administration. The Reference column lists Cisco Unified CallManager 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 7961G/7961G-GE and 7941G/7941G-GE Phone Guide*. For a comprehensive listing of features on the phone, refer to *Cisco Unified IP Phone Features A–Z*.



Note

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

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

Feature	Description	Configuration Reference
Abbreviated dialing	Allows users to speed dial a phone number by entering an assigned index code (1-99) on the phone keypad. Users assign index codes from the User Options web pages.	For more information, refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phone” chapter.

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

Feature	Description	Configuration Reference
Auto Answer	Connects incoming calls automatically after a ring or two. Auto Answer works with either the speaker-phone or headset.	For more information, refer to <i>Cisco Unified CallManager Administration Guide</i> , “Configuring Directory Numbers” chapter.
Auto-pickup	Allows a user to use one-touch, pickup functionality for call pickup, group call pickup, and other group call pickup.	For more information, refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Pickup Group Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Call Pickup and Group Call Pickup” chapter.
Barge	Allows a user to join a non-private call on a shared phone line. Barge features include cBarge and Barge. • cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features. • Barge adds a user to a call but does not convert the call into a conference. The phones support Barge in two conference modes: • Built-in conference bridge at the target device (the phone that is being barged). This mode uses the Barge softkey. • Shared conference bridge. This mode uses the cBarge softkey.	For more information, refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Barge and Privacy” chapter.

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

Feature	Description	Configuration Reference
Block external to external transfer	Prevents users from transferring an external call to another external number.	For more information, refer to <i>Cisco Unified CallManager Features and Services Guide</i> , “External Call Transfer Restrictions” chapter.
Busy Lamp Field (BLF) speed dial	Allows a user to monitor the call state of a directory number (DN) associated with a speed-dial button.	For more information, refer to <i>Cisco Unified CallManager Features and Services Guide</i> , “Presence” chapter.
Call display restrictions	Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call.	For more information, refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Understanding Route Plans” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Call Display Restrictions” chapter.
Call forward	Allows users to redirect incoming calls to another number (Call Forward All).	For more information, refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Configuring Directory Numbers” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter.

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

Feature	Description	Configuration Reference
Call forward configurable display	Allows you to specify information that appears on a phone when a call is forwarded. This information can include the caller name, caller number, redirected number, and original dialed number.	For more information, refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter.
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 allows the CFA target to reach the CFA initiator for important calls.	For more information, refer to <i>Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)</i> , “Cisco Unified CallManager System Guide” section, “Cisco Unified IP Phones” chapter.
Call park	Allows users to park (temporarily store) a call and then retrieve the call by using another phone in the Cisco Unified CallManager system.	For more information, refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Call Park” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Call Park” chapter.
Call pickup	Allows users to redirect a call that is ringing on another phone within their pickup group to their phone.	For more information, refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Pickup Group Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Call Pickup” chapter.

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

Feature	Description	Configuration Reference
Call waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. Displays incoming call information on the phone screen.	Requires no configuration.
Caller ID	Displays caller identification such as a phone number, name, or other descriptive text on the phone screen.	For more information, refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Configuring Cisco Unified IP Phones” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Understanding Route Plans” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Call Display Restrictions” chapter.
Cisco Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available.	For more information, refer to: • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Cisco Call Back” chapter.

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

Feature	Description	Configuration Reference
Cisco IP Manager Assistant (Cisco IPMA)	Enables managers and their assistants to work together more effectively by providing a call-routing service, enhancements to phone capabilities for the manager, and desktop interfaces that are primarily used by the assistant.	For more information, refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco IPMA Configuration Wizard” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco IP Manager Assistant” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Cisco IP Manager Assistant With Proxy Line Support” and “Cisco IP Manager Assistant With Shared Line Support” chapters.
Client matter codes (CMC)	Enables a user to specify that a call relates to a specific client matter.	For more information, refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Client Matter Codes” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Client Matter Codes and Forced Authorization Codes” chapter.
Conference	Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference, Join, cBarge, and Meet-Me.	For more information, refer to <i>Cisco Unified CallManager System Guide</i> , “Cisco Unified IP Phones” chapter.

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

Feature	Description	Configuration Reference
Configurable call forward display	Allows you to specify information that appears on a phone when a call is forwarded. This information can include the caller name, caller number, redirected number, and original dialed number.	For more information, refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter.
Direct transfer	Allows users to connect two calls to each other (without remaining on the line).	For more information, refer to <i>Cisco Unified CallManager System Guide</i> , “Cisco Unified IP Phones” chapter.
Extension Mobility Service	Allows a user temporarily to apply a phone number and user profile settings to a shared Cisco Unified IP Phone by logging into the Extension Mobility service on that phone. Extension Mobility can be useful if users work from a variety of locations within your company or if they share a workspace with coworkers.	For more information, refer to: • <i>Cisco Unified CallManager Features and Services Guide</i>, “Cisco Unified CallManager Extension Mobility” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified CallManager Extension Mobility and Phone Login Features” chapter.
Fast Dial Service	Allows a user to enter a Fast Dial code to place a call. Fast Dial codes can be assigned to phone numbers or Personal Address Book entries. (See “Services” in this table.)	For more information, refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Services Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phone Services” chapter.

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

Feature	Description	Configuration Reference
Forced authorization codes (FAC)	Controls the types of calls that certain users can place.	For more information, refer to: • <i>Cisco Unified CallManager System Guide</i>, “Forced Authorization Codes (FAC)” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Client Matter Codes and Forced Authorization Codes” chapter.
Group call pickup	Allows a user to answer a call ringing on a phone in another group by using a group pickup code.	For more information, refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Pickup Group Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Call Pickup” chapter.
Hold	Allows users to move connected calls from an active state to a held state.	Requires no configuration, unless you want to use music on hold; see “Music-on- hold” in this table for information.
Immediate Divert ⁺	Allows users to transfer incoming calls directly to the voice messaging system.	For more information, refer to: • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Immediate Diver” chapter.

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

Feature	Description	Configuration Reference
Immediate Divert—Enhanced	Allows users to transfer incoming calls directly to their voice messaging system or to the voice messaging system of the original called party.	For more information, refer to: <i>Cisco Unified CallManager Features and Services Guide</i> section of the <i>Cisco Unified CallManager New and Changed Information Guide</i> , "Immediate Divert" chapter.
Join	Allows user to join two or more calls that are on one line to create a conference call and remain on the call.	For more information: • See the “Configuring Softkey Templates” section on page 5-18. • Refer to <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter.
Malicious caller identification (MCID)	Allows users to notify the system administrator about suspicious calls that are received.	For more information refer to: • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Malicious Call Identification” chapter.
Meet-Me conference	Allows a user to host a Meet-Me conference in which other participants call a predetermined number at a scheduled time.	For more information refer to <i>Cisco Unified CallManager Administration Guide</i> , “Meet-Me Number/Pattern Configuration” chapter.

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

Feature	Description	Configuration Reference
Message waiting Indicator	A light on the handset that indicates that indicates that a user has one or more new voice messages.	For more information refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Message Waiting Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Voice Mail Connectivity to Cisco Unified CallManager” chapter.
Multilevel Precedence and Preemption (MLPP)	Provides a method of prioritizing calls within your phone system. Use this feature when users work in an environment where they need to make and receive urgent or critical calls.	For more information refer to <i>Cisco Unified CallManager Features and Services Guide</i> , “Multilevel Precedence and Preemption” chapter.
Music-on- hold	Plays music while callers are on hold.	For more information refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Music On Hold Audio Source Configuration” and “Music On Hold Server Configuration” chapters. • <i>Cisco Unified CallManager System Guide</i>, “Music on Hold” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Music On Hold” chapter.
Onhook call transfer	Allows a user to press a single Transfer softkey and then go onhook to complete a call transfer.	For more information refer to <i>Cisco Unified CallManager System Guide</i> , “Cisco Unified IP Phones” chapter.

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

Feature	Description	Configuration Reference
Other group pickup	Allows a user to answer a call ringing on a phone in another group that is associated with the user's group. (See also “ Call pickup ” and “ Group call pickup ” in this table.)	For more information refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Pickup Group Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Call Pickup” chapter.
Presence-enabled directories	Allows a user to monitor the call state of another directory number (DN) listed in call logs, speed-dials, and corporate directories. The Busy Lamp Field (BLF) for the DN displays the call state.	For more information, refer to <i>Cisco Unified CallManager Features and Services Guide</i> , “Presence” chapter.
Privacy	Prevents users who share a line from adding themselves to a call and from viewing information on their phone screens about the other user's call.	For more information refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i> “Barge and Privacy” chapter.
Quality Reporting Tool (QRT)	Allows users to use the QRT softkey on a phone to submit information about problem phone calls. QRT can be configured for either of two user modes, depending upon the amount of user interaction desired with QRT.	For more information refer to: • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Quality Report Tool” chapter.

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 a button.	Requires no configuration.
Ring setting	Identifies ring type used for a line when a phone has another active call.	For more information refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Configuring Directory Numbers” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Custom Phone Rings” chapter. • “Creating Custom Phone Rings” section on page 6-2.
Services	Allows you to use the Cisco Unified IP Phone Services Configuration menu in Cisco Unified CallManager Administration to define and maintain the list of phone services to which users can subscribe.	For more information refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phone Services” chapter.
Services URL button	Allows users to access services from a programmable button rather than by using the Services menu on a phone.	For more information refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phone Services” chapter.

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

Feature	Description	Configuration Reference
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 refer to <i>Cisco Unified CallManager System Guide</i> , “Cisco Unified IP Phones” chapter.
Speed-dialing	Dials a specified number that has been previously stored.	For more information refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter.
Time-of-Day Routing	Restricts access to specified telephony features by time period.	For more information refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Time Period Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Time-of-Day Routing” chapter.
Transfer	Allows users to redirect connected calls from their phones to another number.	Requires no configuration.

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

Feature	Description	Configuration Reference
Video mode	Allows a user to select the video display mode for viewing a video conference, depending on the modes configured in the system.	For more information: • See the “Configuring Softkey Templates” section on page 5-18. • Refer to <i>Cisco Unified CallManager Administration Guide</i>, “Conference Bridge Configuration” chapter. • Refer to <i>Cisco Unified CallManager System Guide</i>, “Understanding Video Telephony” chapter.
Video Support	Enable video support on the phone.	For more information refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Conference Bridge Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Understanding Video Telephony” chapter. • <i>Cisco VT Advantage Administration Guide</i>, “Overview of Cisco VT Advantage” chapter.
Voice messaging system	Enables callers to leave messages if calls are unanswered.	For more information refer to: • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Voice-Mail Port Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Voice Mail Connectivity to Cisco Unified CallManager” chapter.

Configuring Corporate and Personal Directories

The **Directories** button on the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE gives users access to several directories. These directories can include:

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

To support this feature, you must configure corporate directories. See the [“Configuring Corporate Directories” section on page 5-16](#) for more information.

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

To support this feature, you must provide the user with software to configure the personal directory. See the [“Configuring Personal Directory” section on page 5-17](#) for more information.

Configuring Corporate Directories

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

To install and set up these features, refer to the *Installing and Configuring the Cisco Unified Customer Directory Configuration Plugin* document. This document guides you through the configuration process for integrating Cisco Unified CallManager with Microsoft Active Directory and Netscape Directory Server.

After the LDAP directory configuration completes, users can use the Corporate Directory service on your Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE to look up users in the corporate directory.

Configuring Personal Directory

Personal Directory consists of the following features:

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

Users can access Personal Directory features by these methods:

- From a web browser—Users can access the PAB and Fast Dials features from the Cisco Unified CallManager User Options web pages
- From the Cisco Unified IP Phone—Users can choose **Directories > Personal Directory** to access the PAB and Fast Dials features from their phones
- From a Microsoft Windows application—Users can use the TABSynch tool to synchronize their PABs with Microsoft Outlook.

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

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

Modifying Phone Button Templates

Phone button templates let you assign features to line/speed dial buttons.

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

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

The standard Cisco Unified IP Phone 7961G/7961G-GE template uses buttons 1 and 2 for lines and uses buttons 3 through 6 as speed dials or for access to services. Access other phone features, such as call park, call forward, redial, hold, resume, voice messaging system, conferencing, and so on using softkeys on the Cisco Unified IP Phone 7961G/7961G-GE.

The standard Cisco Unified IP Phone 7941G/7941G-GE template uses buttons 1 and 2 for lines. Access phone features, such as call park, call forward, redial, hold, resume, voice messaging system, conferencing, and so on, using softkeys on the Cisco Unified IP Phone 7941G/7941G-GE.

Configuring Softkey Templates

Using Cisco Unified CallManager Administration, you can manage softkeys associated with applications that are supported by the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE. Cisco Unified CallManager supports two types of softkey templates: standard and nonstandard. Standard softkey templates include Standard User, Standard Feature, Standard IPMA Assistant, Standard IPMA Manager, and Standard IPMA Shared Mode Manager. An application that supports softkeys can have one or more standard softkey templates associated with it. You can modify a standard softkey template by making a copy of it, giving it a new name, and making updates to that copied softkey template. You can also modify a nonstandard softkey template.

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

Setting Up Services

The **Services** button on the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE gives users access to Cisco Unified IP Phone Services. You can also assign services to the programmable buttons on the phone (refer to *Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE Phone Guide* for

more information). These services comprise XML applications that enable the display of interactive content with text and graphics on the phone. Examples of services include local movie times, stock quotes, and weather reports.

Before a user can access any service,

- You must use Cisco Unified CallManager Administration to configure available services.
- The user must subscribe to services using the Cisco Unified CallManager User Options application. This web-based application provides a graphical user interface (GUI) for limited, end-user configuration of IP Phone applications.

Before you set up services, gather the URLs for the sites you want to set up and verify that users can access those sites from your corporate IP telephony network.

To set up these services, choose **Device > Device Settings > Phone Services** from Cisco Unified CallManager Administration. Refer to *Cisco Unified CallManager Administration Guide* and to *Cisco Unified CallManager System Guide* for more information.

After you configure these services, verify that your users have access to the Cisco Unified CallManager User Options web-based application, from which they can select and subscribe to configured services. See the [“How Users Subscribe to Services and Configure Phone Features”](#) section on page A-4 for a summary of the information that you must provide to end users.

**Note**

To configure extension mobility services for users, refer to the *Cisco Unified CallManager Features and Services Guide*.

Adding Users to Cisco Unified CallManager

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

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

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

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

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

Refer to the *Cisco Unified CallManager Administration Guide* for more information about adding users. Refer to the *Cisco Unified CallManager System Guide* for details about user information.

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

Refer to *Cisco Unified CallManager Bulk Administration Guide* for details.

Managing the User Options Web Pages

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

Giving Users Access to the User Options Web Pages

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

For additional information, refer to *Cisco Unified CallManager Administration Guide*, “End User Configuration” section.

Specifying Options that Appear on the User Options Web Pages

Most options on the User Options web pages appear by default. However, two options that do not appear by default are:

- Show Ring Settings
- Show Line Text Label Settings

You can control the options that appear on the User Options web pages by using enterprise parameter settings in Cisco Unified CallManager Administration.

**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 CallManager Administration, choose **System > Enterprise Parameters**.

The Enterprise Parameters Configuration page 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 appears on the User Options web pages (default).

False—Option does not appear on the User Options web pages.



Customizing the Cisco Unified IP Phone

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

This chapter includes these topics:

- [Customizing and Modifying Configuration Files, page 6-1](#)
- [Creating Custom Phone Rings, page 6-2](#)
- [Creating Custom Background Images, page 6-5](#)

Customizing and Modifying Configuration Files

You can modify configuration files (for example, edit the xml files) and add customized files (for example, custom ring tones, call back tones, phone backgrounds) to the TFTP directory. You can modify files and add customized files to the TFTP directory in Cisco IPT Platform Administration, from the TFTP Server File Upload page. Refer to *Cisco IP Telephony Platform Administration Guide* for information about how to upload files to the TFTP folder on a Cisco Unified CallManager server.

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

- admin:file
 - file list*

- file view*
- file search*
- file get*
- file dump*
- file tail*
- file delete*

Creating Custom Phone Rings

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

For more information, see the “Cisco TFTP” chapter in *Cisco Unified CallManager System Guide, Release 5.0(1)* and the “Software Upgrades” chapter in *Cisco IP Telephony Platform Administration Guide*.

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

- [Ringlist.xml File Format Requirements, page 6-2](#)
- [PCM File Requirements for Custom Ring Types, page 6-3](#)
- [Configuring a Custom Phone Ring, page 6-4](#)

Ringlist.xml File Format Requirements

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

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

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

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

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

**Note**

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

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

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

PCM File Requirements for Custom Ring Types

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

- Raw PCM (no header)
- 8000 samples per second
- 8 bits per sample

- uLaw compression
- Maximum ring size—16080 samples
- Minimum ring size—240 samples
- Number of samples in the ring is evenly divisible by 240.
- Ring starts and ends at the zero crossing.
- To create PCM files for custom phone rings, you can use any standard audio editing packages that support these file format requirements.

Configuring a Custom Phone Ring

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

Procedure

-
- Step 1** Create a PCM file for each custom ring (one ring per file). Ensure the PCM files comply with the format guidelines that are listed in the [“PCM File Requirements for Custom Ring Types”](#) section on page 6-3.
 - Step 2** Upload the new PCM files that you created to the Cisco TFTP server for each Cisco Unified CallManager in your cluster. For more information, see the “Software Upgrades” chapter in *Cisco IP Telephony Platform Administration Guide*.
 - Step 3** Use a text editor to edit the Ringlist.xml file. See the [“Ringlist.xml File Format Requirements”](#) section on page 6-2 for information about how to format this file and for a sample Ringlist.xml file.
 - Step 4** Save your modifications and close the Ringlist.xml file.
 - Step 5** To cache the new Ringlist.xml file, stop and start the TFTP service by using Cisco Unified CallManager Serviceability or disable and re-enable the “Enable Caching of Constant and Bin Files at Startup” TFTP service parameter (located in the Advanced Service Parameters).
-

Creating Custom Background Images

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

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

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

- [List.xml File Format Requirements, page 6-5.](#)
- [PNG File Requirements for Custom Background Images, page 6-6.](#)
- [Configuring a Background Image, page 6-7](#)

List.xml File Format Requirements

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

For more information, see the “Cisco TFTP” chapter in *Cisco Unified CallManager System Guide, Release 5.0(1)* and the “Software Upgrades” chapter in *Cisco IP Telephony Platform Administration Guide*.

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

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

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

List.xml Example

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

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

PNG File Requirements for Custom Background Images

Each background image requires two PNG files:

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



Tip

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

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

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

**Tip**

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

Configuring a Background Image

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

Procedure

- Step 1** Create two PNG files for each image (a full size version and a thumbnail version). Ensure the PNG files comply with the format guidelines that are listed in the [“PNG File Requirements for Custom Background Images”](#) section on page 6-6.
- Step 2** Upload the new PNG files that you created in the following folder to the TFTP server for each Cisco Unified CallManager in the cluster. For more information, see the “Software Upgrades” chapter in the *Cisco IP Telephony Platform Administration Guide*.
-  **Note** Cisco recommends that you also store backup copies of custom image files in another location. You can use these backup copies if the customized files are overwritten when you upgrade Cisco Unified CallManager.
- Step 3** Use a text editor to edit the List.xml file. See the [“List.xml File Format Requirements”](#) section on page 6-5 for the location of this file, formatting requirements, and a sample file.

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

**Note**

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

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

Configuring Wideband Headset Codec

The user can configure a setting called Wideband Headset in the Audio Preferences menu on the phone (choose  > User Preferences > Audio Preferences > Wideband Headset). This setting is Disabled by default, and should be enabled only if the user's headset supports wideband.

If Cisco Unified CallManager has been configured to use G.722 (G.722 is enabled by default for Cisco Unified IP Phone Models 7941G, 7941G-GE, 7961G, 7961G-GE, 7970G, and 7971G-GE; other phone models may not support it), and the far endpoint also supports G.722, the call will be connected using the G.722 codec in place of G.711. This occurs regardless of whether the user has enabled a wideband headset, but if the headset is enabled, the headset user may notice greater audio sensitivity during the call. Greater sensitivity means improved audio clarity but also means that more background noise can be heard by the far endpoint—noise such as rustling papers or nearby conversations. Even without a wideband headset, some users may prefer the additional sensitivity of G.722; conversely, some users may be distracted by the additional sensitivity of G.722.

Two parameters in Cisco Unified CallManager Administration affect whether wideband is supported for this Cisco Unified CallManager server and/or a specific phone:

- Advertise G.722 Codec—Choose **Cisco Unified CallManager Administration > System > Enterprise Parameters**. The default value of this enterprise parameter is *True*, which means that all Cisco Unified IP Phone Models 7941G, 7941G-GE, 7961G, 7961G-GE, 7970G, and 7971G-GE that are registered to this Cisco Unified CallManager will advertise G.722 to Cisco Unified CallManager. If each endpoint in the attempted call supports G.722 in its capabilities set, Cisco Unified CallManager will choose that codec for the call. For more information, see the *Cisco Unified CallManager 5.1 Release Notes*.
- Advertise G.722 Codec—Choose **Cisco Unified CallManager Administration > Device > Phone**. The default value of this product-specific parameter is to use the value specified in the enterprise parameter. If you want to override this on a per-phone basis, choose *Enabled* or *Disabled* in the Advertise G.722 Codec parameter on the Product Specific Configuration area of the Phone Configuration window.



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

This chapter describes how to use the following menus on the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE to view model information, status messages, and network statistics for the phone:

- Model Information screen—Displays hardware and software information about the phone.
- Status menu—Provides access to screens that display the status messages, network statistics, firmware versions, and Expansion Module information.
- Call Statistics screen—Displays counters and statistics for the current call. For more information, see the [“Call Statistics Screen” section on page 7-17](#).

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

You can also obtain much of this information, and obtain other related information, remotely through the phone’s web page. For more information, see [Chapter 8, “Monitoring the Cisco Unified IP Phone Remotely.”](#)

For more information about troubleshooting the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE, see [Chapter 9, “Troubleshooting and Maintenance.”](#)

This chapter includes these topics:

- [Model Information Screen, page 7-2](#)

- [Status Menu, page 7-3](#)
- [Call Statistics Screen, page 7-17](#)

Model Information Screen

The Model Information screen includes the options described in [Table 7-1](#).

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

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

Table 7-1 **Model Information Settings**

Option	Description	To Change
Model Number	Model number of the phone.	Display only—cannot configure.
MAC Address	MAC address of the phone.	Display only—cannot configure.
Load File	Identifier of the factory-installed load running on the phone.	Display only—cannot configure.
Boot Load ID	Identifier of the factory-installed load running on the phone.	Display only—cannot configure.
Serial Number	Serial number of the phone.	Display only—cannot configure.
CTL File	Displays the MD5 hash of the certificate trust list (CTL) file that is installed in the phone. If no CTL file is installed on the phone, this field displays No. (If security is configured for the phone, the CTL file installs automatically when the phone reboots or resets.	For more information about this file, refer to <i>Cisco Unified CallManager Security Guide</i> .
MIC	Indicates whether a manufacturing installed certificate (used for the security features) is installed on the phone or is not installed on the phone.	For more information about how to manage the MIC for your phone, refer to the “Using the Certificate Authority Proxy Function” section in <i>Cisco Unified CallManager Security Guide</i> .

Table 7-1 **Model Information Settings (continued)**

Option	Description	To Change
LSC	Indicates whether a locally significant certificate (used for the security features) is installed on the phone or is not installed on the phone.	For more information about how to manage the LSC for your phone, refer to the “Using the Certificate Authority Proxy Function” section in <i>Cisco Unified CallManager Security Guide</i> .
Call Control Protocol	Indicates the call processing protocol used by the phone.	See the “Using Cisco Unified IP Phones with Different Protocols” section on page 2-17.

Status Menu

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

- **Status Messages**—Displays the Status Messages screen, which shows a log of important system messages. For more information, see the [“Status Messages Screen”](#) section on page 7-4.
- **Network Statistics**—Displays the Network Statistics screen, which shows Ethernet traffic statistics. For more information, see the [“Network Statistics Screen”](#) section on page 7-13.
- **Firmware Versions**—Displays the Firmware Versions screen, which shows information about the firmware running on the phone. For more information, see the [“Firmware Versions Screen”](#) section on page 7-15.
- **Expansion Modules**—Displays the Expansion Module(s) screen, which shows information about the Cisco Unified IP Phone Expansion Module 7914, if connected to the phone. For more information, see the [“Expansion Module Status Screen”](#) section on page 7-16.
- **802.1X Authentication Status**—Displays the time-stamped authentication successes and failures. For more information, see the [“Supporting 802.1X Authentication on Cisco Unified IP Phones”](#) section on page 1-18.

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

To exit the Status menu, press the **Exit** softkey.

Status Messages Screen

The Status Messages screen displays up to the 10 most recent status messages that the phone has generated. You can access this screen at any time, even if the phone has not finished starting up. [Table 7-2](#) describes the status messages that might appear. This table also includes actions you can take to address errors that are indicated.

To display the Status Messages screen, follow these steps:

Procedure

- Step 1** Press the **Settings** button.
- Step 2** Select **Status**.
- Step 3** Select **Status Messages**.

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

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

Table 7-2 Status Messages on the Cisco Unified IP Phone

Message	Description	Possible Explanation and Action
BootP server used	The phone obtained its IP address from a BootP server rather than a DHCP server.	None. This message is informational only.

Table 7-2 **Status Messages on the Cisco Unified IP Phone (continued)**

Message	Description	Possible Explanation and Action
CFG file not found	The name-based and default configuration file was not found on the TFTP Server.	The configuration file for a phone is created when the phone is added to the Cisco Unified CallManager database. If the phone has not been added to the Cisco Unified CallManager database, the TFTP server generates a <code>CFG File Not Found</code> response. - Phone is not registered with Cisco Unified CallManager. You must manually add the phone to Cisco Unified CallManager if you are not allowing phones to auto-register. See the “Adding Phones with Cisco Unified CallManager Administration” section on page 2-15 for details. - If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. - If you are using static IP addresses, check configuration of the TFTP server. See the “Network Configuration Menu” section on page 4-7 for details on assigning a TFTP server.
CFG TFTP Size Error	The configuration file is too large for file system on the phone.	Power cycle the phone.
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 7-2 **Status Messages on the Cisco Unified IP Phone (continued)**

Message	Description	Possible Explanation and Action
CTL Installed	A certificate trust list (CTL) file is installed in the phone.	None. This message is informational only. For more information about the CTL file, refer to <i>Cisco Unified CallManager Security Guide</i> .
CTL update failed	The phone could not update its certificate trust list (CTL) file.	Problem with the CTL file on the TFTP server. For more information, refer to <i>Cisco Unified CallManager Security Guide</i> .
DHCP timeout	DHCP server did not respond.	• Network is busy—The errors should resolve themselves when the network load reduces. • No network connectivity between the DHCP server and the phone—Verify the network connections. • DHCP server is down—Check configuration of DHCP server. • Errors persist—Consider assigning a static IP address. See the “Network Configuration Menu” section on page 4-7 for details on assigning a static IP address.
Disabled	802.1X Authentication is disabled on the phone.	You can enable 802.1X using the Settings > Security Configuration > 802.1X Authentication option on the phone. For more information, see the “ 802.1X Authentication and Status ” section on page 4-34.

Table 7-2 **Status Messages on the Cisco Unified IP Phone (continued)**

Message	Description	Possible Explanation and Action
DNS timeout	DNS server did not respond.	• Network is busy—The errors should resolve themselves when the network load reduces. • No network connectivity between the DNS server and the phone—Verify the network connections. • DNS server is down—Check configuration of DNS server.
DNS unknown host	DNS could not resolve the name of the TFTP server or Cisco Unified CallManager.	• Verify that the host names of the TFTP server or Cisco Unified CallManager are configured properly in DNS. • Consider using IP addresses rather than host names.
Duplicate IP	Another device is using the IP address assigned to the phone.	• If the phone has a static IP address, verify that you have not assigned a duplicate IP address. See the “Network Configuration Menu” section on page 4-7 section for details. • If you are using DHCP, check the DHCP server configuration.

Table 7-2 **Status Messages on the Cisco Unified IP Phone (continued)**

Message	Description	Possible Explanation and Action
Error update locale	One or more localization files could not be found in the TFTPPath directory or were not valid. The locale was not changed.	Check that the following files are located within subdirectories in the TFTPPath directory: • Located in subdirectory with same name as network locale: – tones.xml • Located in subdirectory with same name as user locale: – glyphs.xml – dictionary.xml – kate.xml – dictionary.xml
Failed	The phone attempted an 802.1X transaction but authentication failed.	Authentication typically fails because of one of the following: • No shared secret is configured in the phone or authentication server • The shared secret configured in the phone and the authentication server do not match • Phone has not been configured in the authentication server

Table 7-2 **Status Messages on the Cisco Unified IP Phone (continued)**

Message	Description	Possible Explanation and Action
File auth error	An error occurred when the phone tried to validate the signature of a signed file. This message includes the name of the file that failed.	- The file is corrupted. If the file is a phone configuration file, delete the phone from the Cisco Unified CallManager database using Cisco Unified CallManager Administration. Then add the phone back to the Cisco Unified CallManager database using Cisco Unified CallManager Administration. - There is a problem with the CTL file and the key for the server from which files are obtained is bad. In this case, run the CTL client and update the CTL file, making sure that the proper TFTP servers are included in this file.
File not found	The phone cannot locate on the TFTP server the phone load file that is specified in the phone configuration file.	Make sure that the phone load file is on the TFTP server and that the entry in the configuration file is correct.
IP address released	The phone has been configured to release its IP address.	The phone remains idle until it is power cycled or you reset the DHCP address. See the “Network Configuration Menu” section on page 4-7 for details.
Load auth failed	The phone could not load a configuration file.	The configuration file that the phone received from the server identified in this message is corrupt. Make sure that a good version of the configuration file exists on that server.
Load auth failed	A signed phone load file has been modified or renamed.	Make sure that the phone load file that the phone is downloading has not been altered or renamed.
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 CallManager, choose Device > Phone). Verify that the load ID is entered correctly.

Table 7-2 **Status Messages on the Cisco Unified IP Phone (continued)**

Message	Description	Possible Explanation and Action
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 CallManager, choose Device > Phone). Re-enter the load displayed on the phone. See the “Firmware Versions Screen” section on page 7-15 to verify the phone setting.
Load Server is invalid	Indicates an invalid TFTP server IP address or name in the Load Server option.	The Load Server setting is not valid. The Load Server specifies a TFTP server IP address or name from which the phone firmware can be retrieved for upgrades on the phones. Check the Load Server entry (from Cisco Unified CallManager Administration choose Device > Phone).
No default router	DHCP or static configuration did not specify a default router.	• If the phone has a static IP address, verify that the default router has been configured. See the “Network Configuration Menu” section on page 4-7 section for details. • If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.
No DNS server IP	A name was specified but DHCP or static IP configuration did not specify a DNS server address.	• If the phone has a static IP address, verify that the DNS server has been configured. See the “Network Configuration Menu” section on page 4-7 section for details. • If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.

Table 7-2 **Status Messages on the Cisco Unified IP Phone (continued)**

Message	Description	Possible Explanation and Action
No CTL installed	A certificate trust list (CTL) file is not installed in the phone.	Occurs if security is not configured or, if security is configured, because the CTL file does not exist on the TFTP server. For more information, refer to <i>Cisco Unified CallManager Security Guide</i> .
Programming Error	The phone failed during programming.	Attempt to resolve this error by power cycling the phone. If the problem persists, contact Cisco technical support for additional assistance.
Successful—MD5	The phone attempted an 802.1X transaction and authentication achieved.	The phone achieved 802.1X authentication.
TFTP access error	TFTP server is pointing to a directory that does not exist.	- If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. - If you are using static IP addresses, check configuration of TFTP server. See the “Network Configuration Menu” section on page 4-7 for details on assigning a TFTP server.
TFTP file not found	The requested load file (.bin) was not found in the TFTPPath directory.	Check the load ID assigned to the phone (from Cisco Unified CallManager, choose Device > Phone). Verify that the TFTPPath directory contains a .bin file with this load ID as the name.
TFTP error	The phone does not recognize an error code provided by the TFTP server.	Contact the Cisco TAC.

Table 7-2 **Status Messages on the Cisco Unified IP Phone (continued)**

Message	Description	Possible Explanation and Action
TFTP server not authorized	The specified TFTP server could not be found in the phone's CTL.	- The DHCP server is not configured properly and is not server the correct TFTP server address. In this case, update the TFTP server configuration to specify the correct TFTP server. - 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.	- Network is busy—The errors should resolve themselves when the network load reduces. - No network connectivity between the TFTP server and the phone—Verify the network connections. - TFTP server is down—Check configuration of TFTP server.
Timed Out	Supplicant attempted 802.1X transaction but timed out to due the absence of an authenticator.	Authentication typically times out if 802.1X is not configured on the switch.
Version error	The name of the phone load file is incorrect.	Make sure that the phone load file has the correct name.

Table 7-2 *Status Messages on the Cisco Unified IP Phone (continued)*

Message	Description	Possible Explanation and Action
XmlDefault.cnf.xml, or .cnf.xml corresponding to the phone device name	Name of the configuration file.	None. This is an informational message indicating the name of the configuration file for the phone.

Network Statistics Screen

The Network Statistics screen displays information about the phone and network performance. [Table 7-3](#) describes the information that appears in this screen.

To display the Network Statistics screen, follow these steps:

Procedure

- Step 1** Press the **Settings** button.
- Step 2** Select **Status**.
- Step 3** Select **Status > Network Statistics**.

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

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

Table 7-3 *Network Statistics Message Information*

Item	Description
Rx Frames	Number of packets received by the phone
Tx Frames	Number of packets sent by the phone
Rx Broadcasts	Number of broadcast packets received by the phone

Table 7-3 Network Statistics Message Information

Item	Description
One of the following values: Initialized TCP-timeout CM-closed-TCP TCP-Bad-ACK CM-reset-TCP CM-aborted-TCP CM-NAKed KeepaliveTO Failback Phone-Keypad Phone-Re-IP Reset-Reset Reset-Restart Phone-Reg-Rej Load Rejected HC CM-ICMP-Unreach Phone-Abort	Cause of the last reset of the phone
Elapsed Time	Amount of time that has elapsed since the phone last rebooted
Port 1	Link state and connection of the PC port (for example, Auto 100 Mb Full-Duplex means that the PC port is in a link up state and has auto-negotiated a full-duplex, 100-Mbps connection)
Port 2	Link state and connection of the Network port
DHCP BOUND	Phone is bound to the DHCP server, DHCP parameters are acceptable, and the phone has received a DHCPACK message.

Firmware Versions Screen

The Firmware Versions screen displays information about the firmware version that is running on the phone. [Table 7-4](#) describes the information that is displayed on this screen.

To display the Firmware Version screen, follow these steps:

Procedure

-
- Step 1** Press the **Settings** button.
- Step 2** Select **Status**.
- Step 3** Select **Firmware Versions**.
-

To exit the Firmware Version screen, press the **Exit** softkey.

Table 7-4 *Firmware Version Information*

Item	Description
Load File	Load file running on the phone
App Load ID	Identifies the JAR file running on the phone
JVM Load ID	Identifies the Java Virtual Machine (JVM) running on the phone
OS Load ID	Identifies the operating system running on the phone
Boot Load ID	Identifies the factory-installed load running on the phone
DSP Load ID	Identifies the digital signal processor (DSP) software version used
Expansion Module 1	Identifies the load running on the Expansion Module(s), if connected to the phone
Expansion Module 2	

Expansion Module Status Screen

The Expansion Module Status screen displays information about each Cisco Unified IP Phone Expansion Module 7914 that is connected to the phone.

Table [Table 7-5](#) explains the information that is displayed on this screen for each connected expansion module. You can use this information to troubleshoot the expansion module, if necessary. In the Expansion Module Stats screen, a statistic preceded by “A” is for the first expansion module. A statistic preceded by “B” is for the second expansion module.

To display the Expansion Module Stats screen, follow these steps:

Procedure

-
- Step 1** Press the **Settings** button.
 - Step 2** Select **Status**.
 - Step 3** Select **Expansion Module**.
-

To exit the Expansion Module screen, press the **Exit** softkey.

Table 7-5 *Expansion Module Statistics*

Item	Description
Link State	Overall expansion module status
RX Discarded Bytes	Number of bytes discarded due to errors
RX Length Err	Number of packets discarded due to improper length
RX Checksum Err	Number of packets discarded due to invalid checksum information
RX Invalid Message	Number of packets that have been discarded because a message was invalid or unsupported
TX Retransmit	Number of packets that have been retransmitted to the expansion module
TX Buffer Full	Number of packets discarded because the expansion module was not able to accept new messages

Call Statistics Screen

The Call Statistics screen displays counters statistics and voice quality metrics in these ways:

- During call—You can view the call information by pressing the ? button twice rapidly.
- After the call—You can view the call information captured during the last call by displaying the Call Statistics screen.



Note You can also remotely view the call statistics information by using a web browser to access the Streaming Statistics web page. This web page contains additional RTCP statistics not available on the phone. For more information about remote monitoring, see [Chapter 8, “Monitoring the Cisco Unified IP Phone Remotely.”](#)

A single call can have multiple voice streams, but data is captured for only the last voice stream. A voice stream is a packet stream between two endpoints. If one endpoint is put on hold, the voice stream stops even though the call is still connected. When the call resumes, a new voice packet stream begins, and the new call data overwrites the former call data.

To display the Call Statistics screen for information about the last voice stream, follow these steps:

Procedure

-
- | | |
|---------------|-----------------------------------|
| Step 1 | Press the Settings button. |
| Step 2 | Select Status . |
| Step 3 | Select Call Statistics . |
-

To exit the Call Statistics screen, press the **Exit** softkey.

The Call Statistics Screen displays the items shown in [Table 7-6](#).

Table 7-6 **Call Statistics**

Item	Description
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 Codec	Type of audio encoding used for the transmitted stream.
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 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.
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see the “Monitoring the Voice Quality of Calls” section on page 9-21. Note The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score observed from start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 gives 4.5 • G.729 A /AB gives 3.7

Table 7-6 ***Call Statistics (continued)***

Item	Description
MOS LQK Version	Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency	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.
Rcvr Size	RTP packet size, in milliseconds, for the received stream.
Rcvr Discarded	RTP packets received from network but discarded from jitter buffers.



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 configuration information
- Network statistics
- Device logs
- Streaming statistics

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

You can also obtain much of this information directly from a phone. For more information, see [Chapter 7, “Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone.”](#)

For more information about troubleshooting the Cisco Unified IP Phone, [Chapter 9, “Troubleshooting and Maintenance.”](#)

This chapter includes these topics:

- [Accessing the Web Page for a Phone, page 8-2](#)
- [Disabling and Enabling Web Page Access, page 8-3](#)
- [Device Information, page 8-4](#)
- [Network Configuration, page 8-6](#)

- [Network Statistics](#), page 8-10
- [Device Logs](#), page 8-13
- [Streaming Statistics](#), page 8-13

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 8-3 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 CallManager by choosing **Device > Phone**. Phones registered with Cisco Unified CallManager display the IP address on the Find and List Phones web page and at the top of the Phone Configuration web page.
 - On the Cisco Unified IP Phone, press the **Settings** button, choose **Network Configuration**, and then scroll to the IP Address option.
- Step 2** Open a web browser and enter the following URL, where *IP_address* is the IP address of the Cisco Unified IP Phone:
- `http://IP_address`

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 8-4.
- **Network Configuration**—Displays network configuration information and information about other phone settings. For more information, see the [“Network Configuration”](#) section on page 8-6.

- **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 8-10](#).
 - **Access (Port)**—Displays information about network traffic to and from the PC port on the phone. For more information, see the [“Network Statistics” section on page 8-10](#).
 - **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 8-10](#).
- **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 8-13](#).
 - **Core Dumps**—Includes hyperlinks to individual dump files. For more information, see the [“Device Logs” section on page 8-13](#).
 - **Status Messages**—Displays up to the 10 most recent status messages that the phone has generated since it was last powered up. For more information, see the [“Device Logs” section on page 8-13](#).
 - **Debug Display**—Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting. For more information, see the [“Device Logs” section on page 8-13](#).
- **Streaming Statistics**—Includes the following hyperlinks
 - **Stream 1, Stream 2, and Stream 3**—Display a variety of streaming statistics. For more information, see the [“Streaming Statistics” section on page 8-13](#).

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 CallManager User Options web pages.

To disable access to the web pages for a phone, follow these steps from Cisco Unified CallManager Administration:

-
- Step 1** Choose **Device > Phone**.
 - Step 2** Specify the criteria to find the phone and click **Find**, or click **Find** to display a list of all phones.
 - Step 3** Click the device name to open the Phone Configuration window for the device.
 - Step 4** Scroll down to the Product Specific Configuration section. From the Web Access drop-down list box, choose **Disabled**.
 - Step 5** Click **Update**.



Note Some features, such as Cisco Quality Report Tool, do not function properly without access to the phone web pages. Disabling web access also affects any serviceability application that relies on web access, such as CiscoWorks.

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 8-1](#) 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 8-2, and then click the **Device Information** hyperlink.

Table 8-1 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
Version	Version of the firmware running on the phone
Expansion Module 1	Phone load ID for the first Cisco Unified IP Phone Expansion Module 7914, if connected to the phone
Expansion Module 2	Phone load ID for the second Cisco Unified IP Phone Expansion Module 7914, if connected to the phone
Hardware Revision	Revision value of the phone hardware
Serial Number	Serial number of the phone
Model Number	Model number of the phone
Message Waiting	Indicates if there is a voice message waiting on any line for this phone
UDI	Displays the following Cisco Unique Device Identifier (UDI) information about the phone: • Device Type—Indicates hardware type. For example, phone displays for all phone models • Device Description—Displays the name of the phone associated with the indicated model type • Product Identifier—Specifies the phone model • Version Identifier¹—Represents the hardware version of the phone • Serial Number—Displays the phone's unique serial number
Time	Time obtained from the Date/Time Group in Cisco Unified CallManager to which the phone belongs

Table 8-1 **Device Information Area Items (continued)**

Item	Description
Time Zone	Timezone obtained from the Date/Time Group in Cisco Unified CallManager to which the phone belongs
Date	Date obtained from the Date/Time Group in Cisco Unified CallManager to which the phone belongs

1. The Version Identifier field might display blank if using an older model Cisco Unified IP Phone because the hardware does not provide this information.

Network Configuration

The Network Configuration area on a phone's web page displays network configuration information and information about other phone settings. [Table 8-2](#) describes these items.

You can view and set many of these items from the Network Configuration Menu and the Device Configuration Menu on the Cisco Unified IP Phone. For more information, see [Chapter 5, “Configuring Features, Templates, Services, and Users.”](#)

To display the Network Configuration area, access the web page for the phone as described in the [“Accessing the Web Page for a Phone”](#) section on [page 8-2](#), and then click the **Network Configuration** hyperlink.

Table 8-2 **Network Configuration Area Items**

Item	Description
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address.
BOOTP Server	Indicates whether the phone obtains its configuration from a Bootstrap Protocol (BootP) server.
MAC Address	Media Access Control (MAC) address of the phone.
Host Name	Host name that the DHCP server assigned to the phone.
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.
IP Address	Internet Protocol (IP) address of the phone.

Table 8-2 **Network Configuration Area Items (continued)**

Item	Description
Subnet Mask	Subnet mask used by the phone.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone.
Default Router 1–5	Default router used by the phone (Default Router 1) and optional backup routers (Default Router 2–5).
DNS Server 1–5	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) used by the phone.
Operational VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member.
Admin. VLAN ID	Auxiliary VLAN in which the phone is a member.
CallManager 1–5	Host names or IP addresses, in prioritized order, of the Cisco Unified CallManager 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 CallManager functionality, if such a router is available. For an available server, an item will show the Cisco Unified CallManager server IP address and one of the following states: • Active—Cisco Unified CallManager server from which the phone is currently receiving call-processing services. • Standby—Cisco Unified CallManager server to which the phone switches if the current server becomes unavailable. • Blank—No current connection to this Cisco Unified CallManager server. An item may also include the Survivable Remote Site Telephony (SRST) designation, which identifies an SRST router capable of providing Cisco Unified CallManager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified CallManager servers become unreachable. The SRST Cisco Unified CallManager 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 CallManager.
Information URL	URL of the help text that appears on the phone.
Directories URL	URL of the server from which the phone obtains directory information.

Table 8-2 **Network Configuration Area Items (continued)**

Item	Description
Messages URL	URL of the server from which the phone obtains message services.
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.
DHCP Enabled	Indicates whether DHCP is being used by the phone.
DHCP Address Released	Indicates the setting of the DHCP Address Released option on the phone's Network Configuration menu.
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.
Idle URL	URL that the phone displays when the phone has not been used for the time specified by Idle URL Time and no menu is open.
Idle URL Time	Number of seconds that the phone has not been used and no menu is open before the XML service specified by Idle URL is activated.
Proxy Server URL	URL of proxy server, which makes HTTP requests to non-local host addresses on behalf of the phone HTTP client and provides responses from the non-local host to the phone HTTP client.
Authentication URL	URL that the phone uses to validate requests made to the phone web server.
SW Port Configuration	Speed and duplex of the switch port, where: • A—Auto Negotiate • 10H—10-BaseT/half duplex • 10F—10-BaseT/full duplex • 100H—100-BaseT/half duplex • 100F—100-BaseT/full duplex • 1000H—1000-BaseT/half duplex • 1000F—1000-BaseT/full duplex • No Link—No connection to the switch port

Table 8-2 **Network Configuration Area Items (continued)**

Item	Description
PC Port Configuration	Speed and duplex of the switch port, where: • A—Auto Negotiate • 10H—10-BaseT/half duplex • 10F—10-BaseT/full duplex • 100H—100-BaseT/half duplex • 100F—100-BaseT/full duplex • 1000H—1000-BaseT/half duplex • 1000F—1000-BaseT/full duplex • No Link—No connection to the PC port
TFTP Server 2	Backup TFTP server that the phone uses if the primary TFTP server is unavailable.
User Locale	User locale associated with the phone user. Identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
Network Locale	Network locale associated with the phone user. Identifies a set of detailed information to support the phone in a specific location, including definitions of the tones and cadences used by the phone.
Headset Enabled	Indicates whether the Headset button is enabled on the phone.
User Locale Version	Version of the user locale loaded on the phone.
Network Locale Version	Version of the network locale loaded on the phone.
PC Port Disabled	Indicates whether the PC port on the phone is enabled or disabled.
Speaker Enabled	Indicates whether the speakerphone is enabled on the phone.
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.
Video Capability Enabled	Indicates whether the phone can participate in video calls when connected to an appropriately equipped PC.
Voice VLAN Enabled	Indicates whether the phone allows a device attached to the PC port to access the Voice VLAN.

Table 8-2 **Network Configuration Area Items (continued)**

Item	Description
Auto Line Select	Indicates whether the phone shifts the call focus to incoming calls on all lines.
DSCP for Call Control	DSCP IP classification for call control signaling.
DSCP for Configuration	DSCP IP classification for any phone configuration transfer.
DSCP for Services	DSCP IP classification for phone-based services.
Security Mode	Displays the security mode that is set for the phone.
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.
Span to PC Port	Indicates whether the phone will forward packets transmitted and received on the network port to the access port.
PC VLAN	VLAN used to identify and remove 802.1P/Q tags from packets sent to the PC.

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 8-2.

- Ethernet Information—Displays information about Ethernet traffic. [Table 8-3](#) describes the items in this area.
- Access—Displays information about network traffic to and from the PC port (10/100/1000 PC) on the phone. [Table 8-4](#) describes the items in this area.
- Network—Displays information about network traffic to and from the network port (10/100/1000 SW) on the phone. [Table 8-4](#) describes the items in this area.

Table 8-3 Ethernet Information Items

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

Table 8-4 Access Area and Network Items

Item	Description
Rx totalPkt	Total number of packets received by the phone
Rx crcErr	Total number of packets received with CRC failed
Rx alignErr	Total number of packets received between 64 and 1522 bytes in length that have a bad FCS
Rx multicast	Total number of multicast packets received by the phone
Rx broadcast	Total number of broadcast packets received by the phone
Rx unicast	Total number of unicast packets received by the phone
Rx shortErr	Total number of FCS error packets or Align error packets received that are less than 64 bytes in size
Rx shortGood	Total number of good packets received that are less than 64 bytes size
Rx longGood	Total number of good packets received that are greater than 1522 bytes in size
Rx longErr	Total number of FCS error packets or Align error packets received that are greater than 1522 bytes in size
Rx size64	Total number of packets received, including bad packets, that are between 0 and 64 bytes in size

Table 8-4 Access Area and Network Items (continued)

Item	Description
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
Neighbor IP Address	IP address of the neighbor device
Neighbor Port	Neighbor device port to which the phone is connected

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 8-2.

- **Console Logs**—Includes hyperlinks to individual log files. The console log files include debug and error messages received on the phone.
- **Core Dumps**—Includes hyperlinks to individual dump files. The core dump files include data from a phone crash.
- **Status Messages**—Displays up to the 10 most recent status messages that the phone has generated since it was last powered up. You can also see this information from the Status Messages screen on the phone. [Table 7-2](#) describes the status messages that can appear.
- **Debug Display**—Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting.

Streaming Statistics

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

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

To display a Streaming Statistics area, access the web page for the phone as described in the [“Accessing the Web Page for a Phone”](#) section on page 8-2, and then click the **Stream 1**, the **Stream 2**, or the **Stream 3** hyperlink.

[Table 8-5](#) describes the items in the Streaming Statistics areas.

Table 8-5 Streaming Statistics Area Items

Item	Description
Remote Address	IP address and UDP port of the destination of the stream.
Local Address	IP address and UPD port of the phone.
Start Time	Internal time stamp indicating when Cisco Unified CallManager 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.

Table 8-5 Streaming Statistics Area Items (continued)

Item	Description
Rcvr Packets	Total number of RTP data packets received by the phone since starting receiving data on this connection. Includes packets received from different sources if this is a multicast call. The value displays as 0 if the connection was set to send-only mode.
Rcvr Octets	Total number of payload octets received in RTP data packets by the device since starting reception on the connection. Includes packets received from different sources if this is a multicast call. The value displays as 0 if the connection was set to send-only mode.
MOS LQK	Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see the “Monitoring the Voice Quality of Calls” section on page 9-21. Note The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score observed from start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss: • G.711 gives 4.5 • G.729 A /AB gives 3.7
MOS LQK Version	Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.

Table 8-5 Streaming Statistics Area Items (continued)

Item	Description
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency ¹	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.
Max Jitter	Maximum value of instantaneous jitter, in milliseconds.
Sender Size	RTP packet size, in milliseconds, for the transmitted stream.
Sender Reports Received ¹	Number of times RTCP Sender Reports have been received.
Sender Report Time Received ¹	Last time at which an RTCP Sender Report was received.
Rcvr Size	RTP packet size, in milliseconds, for the received stream.
Rcvr Discarded	RTP packets received from network but discarded from jitter buffers.
Rcvr Reports Received ¹	Number of times RTCP Receiver Reports have been received.
Rcvr Report Time Received ¹	Last time at which an RTCP Receiver Report was received.

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



Troubleshooting and Maintenance

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

For additional troubleshooting information, refer to the *Using the 79xx Status Information For Troubleshooting* tech note. That document is available to registered Cisco.com users at this URL:

http://www.cisco.com/warp/customer/788/AVVID/telecaster_trouble.html

If you need additional assistance to resolve an issue, see the “[Obtaining Technical Assistance](#)” section on page xx.

This chapter includes these topics:

- [Resolving Startup Problems](#), page 9-2
- [Cisco Unified IP Phone Resets Unexpectedly](#), page 9-8
- [Troubleshooting Cisco Unified IP Phone Security](#), page 9-12
- [General Troubleshooting Tips](#), page 9-14
- [General Troubleshooting Tips for the Cisco Unified IP Phone Expansion Module 7914](#), page 9-17
- [Resetting or Restoring the Cisco Unified IP Phone](#), page 9-17
- [Using the Quality Report Tool](#), page 9-21
- [Monitoring the Voice Quality of Calls](#), page 9-21
- [Where to Go for More Troubleshooting Information](#), page 9-24
- [Cleaning the Cisco Unified IP Phone](#), page 9-24

Resolving Startup Problems

After installing a Cisco Unified IP Phone into your network and adding it to Cisco Unified CallManager, the phone should start up as described in the [“Verifying the Phone Startup Process” section on page 3-17](#). 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 9-2](#)
- [Symptom: The Cisco Unified IP Phone Does Not Register with Cisco Unified CallManager, page 9-3](#)
- [Symptom: Cisco Unified IP Phone Unable to Obtain IP Address, page 9-8](#)

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 3-17](#) and the LCD screen should display information. If the phone does not go through the startup process, the cause may be faulty cables, bad connections, network outages, lack of power, and so on. Or, the phone may not be functional.

To determine whether the phone is functional, follow these suggestions to systematically eliminate these other potential problems:

1. Verify that the network port is functional:
 - Exchange the Ethernet cables with cables that you know are functional.
 - Disconnect a functioning Cisco Unified IP Phone from another port and connect it to this network port to verify the port is active.
 - Connect the Cisco Unified IP Phone that will not start up to a different network port that is known to be good.
 - Connect the Cisco Unified IP Phone that will not start up directly to the port on the switch, eliminating the patch panel connection in the office.

2. Verify that the phone is receiving power:
 - If you are using external power, verify that the electrical outlet is functional.
 - If you are using in-line power, use the external power supply instead.
 - If you are using the external power supply, switch with a unit that you know to be functional.
3. If the phone still does not start up properly, power up the phone with the handset off-hook. When the phone is powered up in this way, it attempts to launch a backup software image.
4. If the phone still does not start up properly, perform a factory reset of the phone. For instructions, see the [“Performing a Factory Reset” section on page 9-19](#).

If after attempting these solutions, the LCD screen on the Cisco Unified IP Phone does not display any characters after at least five minutes, contact a Cisco technical support representative for additional assistance.

Symptom: The Cisco Unified IP Phone Does Not Register with Cisco Unified CallManager

If the phone proceeds past the first stage of the startup process (LED buttons flashing on and off) but continues to cycle through the messages displaying on the LCD screen, the phone is not starting up properly. The phone cannot successfully start up unless it is connected to the Ethernet network and it has registered with a Cisco Unified CallManager server.

These sections can assist you in determining the reason the phone is unable to start up properly:

- [Identifying Error Messages, page 9-4](#)
- [Checking Network Connectivity, page 9-4](#)
- [Verifying TFTP Server Settings, page 9-4](#)
- [Verifying IP Addressing and Routing, page 9-5](#)
- [Verifying DNS Settings, page 9-5](#)
- [Verifying Cisco Unified CallManager Settings, page 9-5](#)
- [Cisco Unified CallManager and TFTP Services Are Not Running, page 9-6](#)

- [Creating a New Configuration File, page 9-7](#)
- [Checking Network Connectivity, page 9-4](#)

In addition, problems with security may prevent the phone from starting up properly. See the [“Troubleshooting Cisco Unified IP Phone Security” section on page 9-12](#) for more information.

Identifying Error Messages

As the phone cycles through the startup process, you can access status messages that might provide you with information about the cause of a problem. See the [“Status Messages Screen” section on page 7-4](#) for instructions about accessing status messages and for a list of potential errors, their explanations, and their solutions.

Checking Network Connectivity

If the network is down between the phone and the TFTP server or Cisco Unified CallManager, the phone cannot start up properly. Ensure that the network is currently running.

Verifying TFTP Server Settings

You can determine the IP address of the TFTP server used by the phone by pressing the **Settings** button on the phone, choosing **Network Configuration**, and scrolling to the **TFTP Server 1** option.

If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option. See the [“Network Configuration Menu” section on page 4-7](#).

If you are using DHCP, the phone obtains the address for the TFTP server from the DHCP server. Check the IP address configured in Option 150.

You can also enable the phone to use an alternate TFTP server. Such a setting is particularly useful if the phone was recently moved from a from one location to another. See the [“Network Configuration Menu” section on page 4-7](#) 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 **Settings** button, choose **Network Configuration**, and look at the following options:

- **DHCP Server**—If you have assigned a static IP address to the phone, you do not need to enter a value for the DHCP Server option. However, if you are using a DHCP server, this option must have a value. If it does not, check your IP routing and VLAN configuration. Refer to the *Troubleshooting Switch Port and Interface Problems* document, available at this URL: <http://www.cisco.com/warp/customer/473/53.shtml>
- **IP Address, Subnet Mask, Default Router**—If you have assigned a static IP address to the phone, you must manually enter settings for these options. See the “**Network Configuration Menu**” section on page 4-7 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/warp/customer/473/100.html#41>

Verifying DNS Settings

If you are using DNS to refer to the TFTP server or to Cisco Unified CallManager, you must ensure that you have specified a DNS server. Verify this setting by pressing the **Settings** button on the phone, choosing **Network Configuration**, and scrolling to the **DNS Server 1** option. You should also verify that there is a CNAME entry in the DNS server for the TFTP server and for the Cisco Unified CallManager system.

You must also ensure that DNS is configured to do reverse look-ups.

Verifying Cisco Unified CallManager Settings

On the Cisco Unified IP Phone, press the **Settings** button, choose **Network Configuration**, and look at the **CallManager 1–5** options. The Cisco Unified IP Phone attempts to open a TCP connection to all the Cisco Unified CallManager servers that are part of the assigned Cisco Unified CallManager group. If none of

these options contain IP addresses or show Active or Standby, the phone is not properly registered with Cisco Unified CallManager. See the [“Checking Network Connectivity” section on page 9-4](#) for tips on resolving this problem.

Cisco Unified CallManager and TFTP Services Are Not Running

If the Cisco Unified 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 that other phones and devices are unable to start up properly.

If the Cisco Unified 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 CallManager Administration, choose **Serviceability** from the Navigation drop-down list.
 - Step 2** Choose **Tools > Control Center - Network Services**.
 - Step 3** Choose the primary Cisco Unified CallManager server from the Server drop-down list.

The page displays the service names for the server that you chose, the status of the services, and a service control panel to start or stop a service.
 - Step 4** If a service has stopped, click its radio button and then click the **Start** button.

The Service Status symbol changes from a square to an arrow.
-

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 CallManager, choose **Device > Phone > Find** to locate the phone experiencing problems.
- Step 2** Choose **Delete** to remove the phone from the Cisco Unified CallManager database.
- Step 3** Add the phone back to the Cisco Unified CallManager database. See the [“Adding Phones to the Cisco Unified CallManager Database”](#) section on page 2-12 for details.
- Step 4** Power cycle the phone.



Note

- When you remove a phone from the Cisco Unified CallManager database, its configuration file is deleted from the Cisco Unified CallManager TFTP server. The phone's directory number or numbers remain in the Cisco Unified CallManager 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 CallManager database. You can use the Route Plan Report to view and delete unassigned reference numbers. Refer to *Cisco Unified CallManager 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 CallManager 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 CallManager

A Cisco Unified IP Phone can register with a Cisco Unified CallManager server only if the phone has been added to the server or if auto-registration is enabled. Review the information and procedures in the [“Adding Phones to the Cisco Unified CallManager Database” section on page 2-12](#) to ensure that the phone has been added to the Cisco Unified CallManager database.

To verify that the phone is in the Cisco Unified CallManager database, choose **Device > Phone > Find** from Cisco Unified CallManager Administration to search for the phone based on its MAC Address. For information about determining a MAC address, see the [“Determining the MAC Address for a Cisco Unified IP Phone” section on page 2-19](#).

If the phone is already in the Cisco Unified CallManager database, its configuration file may be damaged. See the [“Creating a New Configuration File” section on page 9-7](#) for assistance.

Symptom: Cisco Unified IP Phone Unable to Obtain IP Address

If a phone is unable to obtain an IP address when it starts up, the phone may be not be on the same network or VLAN as the DHCP server, or the switch port to which the phone is connected may be disabled. Make sure that the network or VLAN to which the phone is connected has access to the DHCP server, and make sure that the switch port is enabled.

Cisco Unified IP Phone Resets Unexpectedly

If users report that their phones are resetting during calls or while idle on their desk, you should investigate the cause. If the network connection and Cisco Unified CallManager 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 CallManager. These sections can help you identify the cause of a phone resetting in your network:

- [Verifying the Physical Connection, page 9-9](#)
- [Identifying Intermittent Network Outages, page 9-9](#)

- [Verifying DHCP Settings, page 9-9](#)
- [Checking Static IP Address Settings, page 9-10](#)
- [Verifying the Voice VLAN Configuration, page 9-10](#)
- [Verifying that the Phones Have Not Been Intentionally Reset, page 9-10](#)
- [Eliminating DNS or Other Connectivity Errors, page 9-11](#)

Verifying the Physical Connection

Verify that the Ethernet connection to which the Cisco Unified IP Phone is connected is up. For example, check if 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 [“Network Configuration Menu” section on page 4-7](#) 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. Cisco Unified IP Phones send messages with request type 151 to renew their DHCP address leases. If the DHCP server expects messages with request type 150, the lease will be denied, forcing the phone to restart and request a new IP address from the DHCP server.

Checking Static IP Address Settings

If the phone has been assigned a static IP address, verify that you have entered the correct settings. See the [“Network Configuration Menu” section on page 4-7](#) for more information.

Verifying the Voice VLAN Configuration

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

Isolating the phones on a separate auxiliary VLAN increases the quality of the voice traffic. See the [“Understanding How the Cisco Unified IP Phone Interacts with the VLAN” section on page 2-3](#) for details.

Verifying that the Phones Have Not Been Intentionally Reset

If you are not the only administrator with access to Cisco Unified CallManager, 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 CallManager to reset by pressing the **Settings** button on the phone and choosing **Status > Network Statistics**. If the phone was recently reset one of these messages appears:

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

Eliminating DNS or Other Connectivity Errors

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

Procedure

- Step 1** Use the **Erase** softkey to reset phone settings to their default values. See the [“Resetting or Restoring the Cisco Unified IP Phone” section on page 9-17](#) for details.
- Step 2** Modify DHCP and IP settings:
- Disable DHCP. See the [“Network Configuration Menu” section on page 4-7](#) for instructions.
 - Assign static IP values to the phone. See the [“Network Configuration Menu” section on page 4-7](#) for instructions. Use the same default router setting used for other functioning Cisco Unified IP Phones.
 - Assign a TFTP server. See the [“Network Configuration Menu” section on page 4-7](#) for instructions. Use the same TFTP server used for other functioning Cisco Unified IP Phones.
- Step 3** On the Cisco Unified CallManager server, verify that the local host files have the correct Cisco Unified CallManager server name mapped to the correct IP address.
- Step 4** From Cisco Unified CallManager, 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 CallManager, choose **Device > Phone > Find** and verify that you have assigned the correct MAC address to this Cisco Unified IP Phone. For information about determining a MAC address, see the [“Determining the MAC Address for a Cisco Unified IP Phone” section on page 2-19](#).
- Step 6** Power cycle the phone.
-

Troubleshooting Cisco Unified IP Phone Security

[Table 9-1](#) provides troubleshooting information for the security features on the Cisco Unified IP Phone. For information relating to the solutions for any of these issues, and for additional troubleshooting information about security and encryption, refer to *Cisco Unified CallManager Security Guide*.

Table 9-1 ***Cisco Unified IP Phone Security Troubleshooting***

Problem	Possible Cause
Device authentication error.	CTL file does not have a Cisco Unified CallManager certificate or has an incorrect certificate.
Phone cannot authenticate CTL file.	The security token that signed the updated CTL file does not exist in the CTL file on the phone.
Phone cannot authenticate any of the configuration files other than the CTL file.	Bad TFTP record.
Phone reports TFTP authorization failure.	- The TFTP address for the phone does not exist in the CTL file. - If you created a new CTL file with a new TFTP record, the existing CTL file on the phone may not contain a record for the new TFTP server.
Phone does not register with Cisco Unified CallManager.	The CTL file does not contain the correct information for the Cisco Unified CallManager server.
Phone does not request signed configuration files.	The CTL file does not contain any TFTP entries with certificates.

Table 9-1 Cisco Unified IP Phone Security Troubleshooting (continued)

Problem	Possible Cause
802.1X Enabled on Phone but Not Authenticating	
Phone cannot obtain a DHCP-assigned IP address	These errors typically indicate that 802.1X is enabled on the phone, but the phone is unable to authenticate. 1. Verify that you have properly configured the required components “Supporting 802.1X Authentication on Cisco Unified IP Phones” section on page 1-18. 2. Confirm that the shared secret is configured on the phone (see the “Security Configuration Menu” section on page 4-25 for more information). – If the shared secret is configured, verify that you have the same shared secret entered on the authentication server. – If the shared secret is not configured, enter it and ensure that it matches the one on the authentication server.
Phone does not register with Cisco Unified CallManager	
Phone status display as “Configuring IP” or “Registering”	
802.1X Authentication Status displays as “Held” (see the “ 802.1X Authentication and Status ” section on page 4-34).	
Status menu displays 802.1x status as “Failed” (see the “ Call Statistics Screen ” section on page 7-17).	
802.1X Not Enabled	
Phone cannot obtain a DHCP-assigned IP address	These errors typically indicate that 802.1X is not enabled on the phone. To enable it, see the “Security Configuration Menu” section on page 4-25 for information on enabling 802.1X on the phone.
Phone does not register with Cisco Unified CallManager	
Phone status display as “Configuring IP” or “Registering”	
802.1X Authentication Status displays as “Disabled” (see the “ 802.1X Authentication and Status ” section on page 4-34).	
Status menu displays DHCP status as timing out (see the “ Call Statistics Screen ” section on page 7-17).	

Table 9-1 *Cisco Unified IP Phone Security Troubleshooting (continued)*

Problem	Possible Cause
Factory Reset Deleted 802.1X Shared Secret	
Phone cannot obtain a DHCP-assigned IP address	These errors typically indicate that the phone has completed a factory reset while 802.1X was enabled. A factory reset deletes the shared secret, which is required for 802.1X authentication and network access. To resolve this, you have two options: • Temporarily disable 802.1X on the switch. • Temporarily move the phone to a network environment that is not using 802.1X authentication. Once the phone starts up normally in one of these conditions, you can access the 802.1X configuration menus and re-enter the shared secret.
Phone does not register with Cisco Unified CallManager	
Phone status display as “Configuring IP” or “Registering”	
Cannot access phone menus to verify 802.1X status	

General Troubleshooting Tips

[Table 9-2](#) provides general troubleshooting information for the Cisco Unified IP Phone.

Table 9-2 *Cisco Unified IP Phone Troubleshooting*

Summary	Explanation
Daisy-chaining IP phones.	Do not connect an IP phone to another IP phone through the access port. Each IP phone should directly connect to a switch port. If you connect IP phones together in a line (daisy-chaining), a problem with one phone can affect all subsequent phones in the line. Also, all phones on the line share bandwidth.
Poor quality when calling digital cell phones using the G.729 protocol.	In Cisco Unified CallManager, 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.

Table 9-2 **Cisco Unified IP Phone Troubleshooting (continued)**

Summary	Explanation
Prolonged broadcast storms cause IP phones to reset, or be unable to make or answer a call.	A prolonged Layer 2 broadcast storm (lasting several minutes) on the voice VLAN may cause IP phones to reset, lose an active call, or be unable to initiate or answer a call. Phones may not come up until a broadcast storm ends.
Moving a network connection from the phone to a workstation.	If you are powering your phone through the network connection, you must be careful if you decide to unplug the phone's network connection and plug the cable into a desktop computer.  Caution The computer's network card cannot receive power through the network connection; if power comes through the connection, the network card can be destroyed. To protect a network card, wait 10 seconds or longer after unplugging the cable from the phone before plugging it into a computer. This delay gives the switch enough time to recognize that there is no longer a phone on the line and to stop providing power to the cable.
Changing the telephone configuration.	By default, the network configuration options are locked to prevent users from making changes that could impact their network connectivity. You must unlock the network configuration options before you can configure them. See the “Unlocking and Locking Options” section on page 4-4 for details.
Phone resetting.	The phone resets when it loses contact with the Cisco Unified CallManager software. This lost connection can be due to any network connectivity disruption, including cable breaks, switch outages, and switch reboots.
LCD display issues.	If the display appears to have rolling lines or a wavy pattern, it might be interacting with certain types of older fluorescent lights in the building. Moving the phone away from the lights, or replacing the lights, should resolve the problem.
Dual-Tone Multi-Frequency (DTMF) delay.	When you are on a call that requires keypad input, if you press the keys too quickly, some of them might not be recognized.

Table 9-2 Cisco Unified IP Phone Troubleshooting (continued)

Summary	Explanation
Codec mismatch between the phone and another device.	The RxType and the TxType statistics show the codec that is being used for a conversation between this Cisco Unified IP phone and the other device. The values of these statistics should match. If they do not, verify that the other device can handle the codec conversation or that a transcoder is in place to handle the service. See the “Call Statistics Screen” section on page 7-17 for information about displaying these statistics.
Sound sample mismatch between the phone and another device.	The RxSize and the TxSize statistics show the size of the voice packets that are being used in a conversation between this Cisco Unified IP phone and the other device. The values of these statistics should match. See the “Call Statistics Screen” section on page 7-17 for information about displaying these statistics.
Gaps in voice calls.	Check the AvgJtr and the MaxJtr statistics. A large variance between these statistics might indicate a problem with jitter on the network or periodic high rates of network activity. See the “Call Statistics Screen” section on page 7-17 for information about displaying these statistics.
Loopback condition.	A loopback condition can occur when the following conditions are met: • The SW Port Configuration option in the Network Configuration menu on the phone is set to 10 Half (10-BaseT / half duplex) • The phone receives power from an external power supply • The phone is powered down (the power supply is disconnected) In this case, the switch port on the phone can become disabled and the following message will appear in the switch console log: HALF_DUX_COLLISION_EXCEED_THRESHOLD To resolve this problem, re-enable the port from the switch.

Table 9-2 *Cisco Unified IP Phone Troubleshooting (continued)*

Summary	Explanation
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.

General Troubleshooting Tips for the Cisco Unified IP Phone Expansion Module 7914

[Table 9-3](#) provides general troubleshooting information for the Cisco Unified IP Phone Expansion Module 7914.

Table 9-3 *Cisco Unified IP Phone Expansion Module 7914 Troubleshooting*

Problem	Solution
No display on the Cisco Unified IP Phone Expansion Module 7914.	Verify that all of the cable connections are correct. Verify that you have power to the Cisco Unified IP Phone Expansion Module 7914
Lighted buttons on the first Cisco Unified IP Phone Expansion Module 7914 are all red.	Verify that the Cisco Unified IP Phone Expansion Module 7914 is defined in Cisco Unified CallManager.
Lighted buttons on the second Cisco Unified IP Phone Expansion Module 7914 are all amber.	Verify that the Cisco Unified IP Phone Expansion Module 7914 is defined in Cisco Unified CallManager.

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 9-18](#)
- [Performing a Factory Reset, page 9-19](#)

Performing a Basic Reset

Performing a basic reset of a Cisco Unified IP Phone provides a way to recover if the phone experiences an error and provides a way to reset or restore various configuration and security settings.

[Table 9-4](#) describes the ways to perform a basic reset. You can reset a phone with any of these operations after the phone has started up. Choose the operation that is appropriate for your situation.

Table 9-4 Basic Reset Methods

Operation	Performing	Explanation
Restart phone	Press the Services, Settings, or Directories button and then press **#** .	Resets any user and network configuration changes that you have made, but that the phone has not written to its Flash memory, to previously-saved settings, then restarts the phone.
Erase softkey	From the Settings menu, unlock phone options (see the “Unlocking and Locking Options” section on page 4-4). Then press the Erase softkey.	Resets user and network configuration settings to their default values, deletes the CTL file from the phone, and restarts the phone.
	From the Network Configuration menu, unlock phone options (see the “Unlocking and Locking Options” section on page 4-4). Then press the Erase softkey.	Resets network configuration settings to their default values and resets the phone. (This method causes DHCP to reconfigure the IP address of the phone.)
	From the Security Configuration menu, unlock phone options (see the “Unlocking and Locking Options” section on page 4-4). Then press the Erase softkey.	Deletes the CTL file from the phone and restarts the phone.

Performing a Factory Reset

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

- CTL file—Erased
- LSC—Erased
- User configuration settings—Reset to default values
- Network configuration settings—Reset to default values
- Call histories—Erased

- Locale information—Reset to default values
- Phone application—Erased (phone recovers by loading the term61.default.loads file or the term41.default.loads file, depending on the phone model)

Before you perform a factory reset, ensure that the following conditions are met:

- The phone must be on a DHCP-enabled network.
- A valid TFTP server must be set in DHCP option 150 or option 66 on the DHCP server.
- The term61.default.loads file or the term41.default.loads and the files specified in that file should be available on the TFTP server that is specified by the DHCP packet.

To perform a factory reset of a phone, perform the following steps:

Procedure

- Step 1** Unplug the power cable from the phone and then plug it back in.
The phone begins its power up cycle.
- Step 2** While the phone is powering up, and before the Speaker button flashes on and off, press and hold #.
Continue to hold # until each line button flashes on and off in sequence in amber.
- Step 3** Release # and press **123456789*0#**.
You can press a key twice in a row, but if you press the keys out of sequence, the factory reset will not take place.
After you press these keys, the line buttons on the phone flash red and the phone goes through the factory reset process.
Do not power down the phone until it completes the factory reset process and the main screen appears.
-

Using the Quality Report Tool

The Quality Report Tool (QRT) is a voice quality and general problem-reporting tool for the Cisco Unified IP Phone. The QRT feature is installed as part of the Cisco Unified CallManager installation.

You can configure users' Cisco Unified IP Phones with QRT. When you do so, users can report problems with phone calls by pressing the QRT softkey. This softkey is available only when the Cisco Unified IP Phone is in the Connected, Connected Conference, Connected Transfer, and/or OnHook states.

When a user presses the **QRT** softkey, a list of problem categories appears. The user selects the appropriate problem category and this feedback is logged in an XML file. Actual information logged depends on the user selection and whether the destination device is a Cisco Unified IP Phone.

For more information about using QRT, refer to *Cisco Unified CallManager Serviceability Administration Guide*, *Cisco Unified CallManager Serviceability System Guide*, and *Cisco CallManager Features and Services Guide*.

Monitoring the Voice Quality of Calls

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

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

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

**Note**

Concealment ratio and concealment seconds are primary measurements based on frame loss while MOS LQK scores project a “human-weighted” version of the same information on a scale from 5 (excellent) to 1 (bad) for measuring listening quality.

Listening quality scores (MOS LQK) relate to the clarity or sound of the received voice signal. Conversational quality scores (MOS CQ such as G.107) include impairment factors, such as delay, that degrade the natural flow of conversation.

For information about configuring voice quality metrics for phones, refer to the “Phone Features” section in the “Cisco Unified IP Phone” chapter in the *Cisco Unified CallManager System Guide*.

You can access voice quality metrics from the Cisco Unified IP Phone by using the Call Statistics screen (see the [“Call Statistics Screen”](#) section on page 7-17) or remotely by using Streaming Statistics (see [Chapter 8, “Monitoring the Cisco Unified IP Phone Remotely”](#)).

Using Voice Quality Metrics

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

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

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

- G.711 codec gives 4.5 score
- G.719A/ AB gives 3.7 score

**Note**

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

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

Troubleshooting Tips

When you observe significant and persistent changes to metrics, use [Table 9-5](#) for general troubleshooting information:

Table 9-5 *Changes to Voice Quality Metrics*

Metric Change	Condition
MOS LQK scores decrease significantly	Network impairment from packet loss or high jitter: • Average MOS LQK decreases could indicate widespread and uniform impairment. • Individual MOS LQK decreases indicate bursty impairment. Cross-check with Conceal Ratio and Conceal Seconds for evidence of packet loss and jitter.
MOS LQK scores decrease significantly	• Check to see if the phone is using a different codec than expected (RxType and TxType). • Check to see if the MOS LQK version changed after a firmware upgrade.
Conceal Ratio and Conceal Seconds increase significantly	• Network impairment from packet loss or high jitter.
Conceal Ratio is near or at zero, but the voice quality is poor	• Noise or distortion in the audio channel such as echo or audio levels. • Tandem calls that undergo multiple encode/decode such as calls to a cellular network or calling card network. • Acoustic problems coming from a speaker-phone, handsfree cellular phone or wireless headset. Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.

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

Where to Go for More Troubleshooting Information

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

- Cisco Unified IP Phone Troubleshooting Resources:

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

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

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

Cleaning the Cisco Unified IP Phone

To clean your Cisco Unified IP phone, use only a dry soft cloth to gently wipe the phone and the LCD screen. Do not apply liquids or powders directly on the phone. As with all non-weather-proof electronics, liquids and powders can damage the components and cause failures.



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-2](#)
- [How Users Access the Online Help System on the Cisco Unified IP Phone, page A-2](#)
- [How Users Get Copies of Cisco Unified IP Phone Manuals, page A-3](#)
- [How Users Subscribe to Services and Configure Phone Features, page A-4](#)
- [How Users Access a Voice Messaging System, page A-4](#)
- [How Users Configure Personal Directory Entries, page A-5](#)

How Users Obtain Support for the Cisco Unified IP Phone

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

Giving Users Access to the User Options Web Pages

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

- *Cisco Unified CallManager Administration Guide*, "User Group Configuration" chapter
- *Cisco Unified CallManager System Guide*, "Roles and User Groups" chapter

How Users Access the Online Help System on the Cisco Unified IP Phone

The Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE provide access to a comprehensive online help system. To view the main help menu on a phone, press the **?** button on your phone and wait for several seconds for the menu to appear. If you are already in Help, press **Main**.

Main menu topics include:

- About Your Cisco Unified IP Phone—Descriptive information about the phone model

- How do I...?—Procedures and information about commonly-used phone tasks
- Calling Features—Descriptions and procedures for using calling features, such as conference and transfer
- Help—Tips on using and accessing Help

You can also use the ? button to obtain information about softkeys, menu items, and the help system itself. Refer to *Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE Phone Guide* for more information.

How Users Get Copies of Cisco Unified IP Phone Manuals

You should provide end users with access to user documentation for the Cisco Unified IP Phones. *Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE Phone Guide* includes detailed user instructions for key phone features.

There are several Cisco Unified IP Phone models available, so to assist users in finding the appropriate documentation on the Cisco website, Cisco recommends that you provide links to the current documentation. If you do not want to or cannot send users to the Cisco website, Cisco suggests that you download the PDF files and provide them to end users on your website.

Documentation is also available on the CD-ROM titled *Cisco Unified CallManager Design, Installation, and Operation Guides*, which is distributed with Cisco Unified CallManager releases.

For a list of available documentation for Cisco Unified IP Phones, go to this URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm

For a list of available documentation for Cisco Unified CallManager, go to this URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm

For more information about viewing or ordering documentation, see the “Obtaining Documentation” section on page xvi.

How Users Subscribe to Services and Configure Phone Features

End users can perform a variety of activities using the Cisco Unified CallManager User Options web pages. These activities include subscribing to services, setting up speed dial and call forwarding numbers, configuring ring settings, and creating a personal address book. Keep in mind that configuring settings on a phone 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/CCMUser/`, where *server_name* is the host on which the web server is installed.
- A user ID, default password, and default PIN are needed to access the application.

These settings correspond to the values you entered when you added the user to Cisco Unified CallManager (see the [“Adding Users to Cisco Unified CallManager” section on page 5-19](#)).

- A brief description of what a web-based, graphical user interface application is, and how to access it with a web browser.
- An overview the tasks that users can accomplish using the web page.

How Users Access a Voice Messaging System

Cisco Unified CallManager 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 CallManager to configure the **Messages** button on the Cisco Unified IP Phone.

- Initial password for accessing the voice messaging system.

Make sure that you have configured a default voice messaging system password for all users.

- How the phone indicates that voice messages are waiting.

Make sure that you have used Cisco Unified CallManager to set up a message waiting indicator (MWI) method.

How Users Configure Personal Directory Entries

Users can configure personal directory entries on the Cisco Unified IP Phone. To configure personal directory, users must have access to the following:

- User Options pages.

Make sure that users know how to access their User Options pages. See the [“How Users Subscribe to Services and Configure Phone Features” section on page A-4](#) for details.

- Cisco Unified IP Phone Address Book Synchronizer.

Make sure to provide users with the installer for this application. To obtain the installer, choose **Application > Plugins** from Cisco Unified CallManager and click **Cisco IP Phone Address Book Synchronizer**.

See the [“Installing and Configuring the Cisco Unified IP Phone Address Book Synchronizer” section on page A-5](#) for information about installing the Cisco Unified IP Phone Address Book Synchronizer.

Installing and Configuring the Cisco Unified IP Phone Address Book Synchronizer

Use this tool to synchronize data stored in your Microsoft Windows, Microsoft Outlook, or Microsoft Outlook Express address book(s) with the Cisco Unified CallManager directory and Personal Address Book service.

Installing the Synchronizer

- Step 1** Get the Cisco Unified IP Phone Address Book Synchronizer installer file from your system administrator.
- Step 2** Double-click the TabSyncInstall.exe file provided by your system administrator. The Welcome to Cisco Unified IP Phone Address Book Synchronizer window appears.
- Step 3** Click **Next**.
The License Agreement window appears.
- Step 4** Read the license agreement information, and click **Yes** to accept.
The Choose Destination Location window appears.
- Step 5** Choose the directory in which you want to install the application and click **Next**.
The Start Copying Files window appears.
- Step 6** Verify that you have chosen the correct directory, and click **Next**.
The installation wizard installs the application to your computer. When the installation is complete, the InstallShield Wizard Complete window appears.
- Step 7** Click **Finish**.
- Step 8** To complete the process, you must next configure the Synchronizer.
-

Configuring the Synchronizer

- Step 1** Open the Cisco Unified IP Phone Address Book Synchronizer.
If you accepted the default installation directory, you can open the application by choosing **Start > Programs > Cisco > IP Phone Address Synchronizer**.
- Step 2** To configure user information, click the **Password** button.
The Cisco Unified IP Phone User window appears.
- Step 3** Enter the Cisco Unified IP Phone user name and password and click **OK**.
- Step 4** To configure synchronization rules, click the **Rules Options** button.
- Step 5** Choose the synchronization method that you want to use and click **OK**.

- Step 6** To configure Cisco Unified CallManager information, click the **CCM Server** button.
- The Configure Cisco Unified CallManager Web Server window appears.
- Step 7** Enter the IP address or host name of the Cisco Unified CallManager and click **OK**.
- If you do not have this information, contact your system administrator.
- Step 8** Click the **Password** button.
- The Cisco Unified IP Phone User window appears.
- Step 9** Enter your user identification and password for the Cisco Unified IP Phone User Options application.
- Step 10** To start the directory synchronization process, click the **Synchronize** button.
- The Synchronization Status window provides information on the status of the address book synchronization. If you chose the user intervention for duplicate entries rule and you have duplicate address book entries, the Duplicate Selection window appears. Choose the entry that you want to include in your Personal Address Book and click **OK**.
- When synchronization completes, click **Exit** to close the Cisco Unified IP Phone Address Book Synchronizer.
-



Supporting International Users

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

- [Adding Language Overlays to Phone Buttons, page B-1](#)
- [Installing the Cisco Unified CallManager Locale Installer, page B-2](#)

Adding Language Overlays to Phone Buttons

To support the needs of international users, the button labels on the Cisco Unified IP Phones exhibit icons rather than text to indicate the purposes of the buttons. You can purchase language-specific text overlays to add to a phone. To order these language-specific overlays, go to this website:

<http://www.overlaypro.com/cisco/>



Note

Phone overlays are available only for languages in which the Cisco Unified IP Phone software has been localized. All languages may not be immediately available, so continue to check the website for updates.

Installing the Cisco Unified CallManager Locale Installer

If you are using Cisco Unified IP Phones in a locale other than English, you must install the locale-specific version of the Cisco Unified CallManager Locale Installer on every Cisco Unified CallManager 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 CallManager Locale Installer at <http://www.cisco.com/kobayashi/sw-center/telephony/callmgr/locale-installer.shtml>.

For more information, refer to the “Locale Installation” section in the *Cisco IP Telephony Platform 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 7961G/7961G-GE and 7941G/7941G-GE.

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

Physical and Operating Environment Specifications

[Table C-1](#) shows the physical and operating environment specifications for the Cisco Unified IP Phone 7961G/7961G-GE and 7941G/7941G-GE.

Table C-1 *Physical and Operating Specifications*

Specification	Value or Range
Operating temperature	32° to 104°F (0° to 40°C)
Operating relative humidity	10% to 95% (non-condensing)
Storage temperature	14° to 140°F (–10° to 60°C)
Height	8 in. (20.32 cm)
Width	10.5 in. (26.67 cm)
Depth	6 in. (15.24 cm)
Weight	3.5 lb (1.6 kg)

Table C-1 *Physical and Operating Specifications (continued)*

Specification	Value or Range
Power	100-240 VAC, 50-60 Hz, 0.5 A—when using the AC adapter 48 VDC, 0.2 A—when using the in-line power over the network cable
Cables	Two (2) pair of Category 3 for 10-Mbps cables Two (2) pair of Category 5 for 100-Mbps cables
Distance Requirements	As supported by the Ethernet Specification, it is assumed that most Cisco Unified IP Phones should be within 330 feet (100m) of a phone closet.

Cable Specifications

- RJ-9 jack (4-conductor) for handset and headset connection.
- RJ-45 jack for the LAN 10/100BaseT connection (labeled 10/100 SW on the Cisco Unified IP Phone 7961G and 7941G; labeled 10/100/1000 SW on the Cisco Unified IP Phone 7961G-GE and 7941G-GE).
- RJ-45 jack for a second 10/100BaseT compliant connection (labeled 10/100 PC on the Cisco Unified IP Phone 7961G and 7941G; labeled 10/100/1000 PC on the Cisco Unified IP Phone 7961G-GE and 7941G-GE).
- 48-volt power connector.

Network and Access Port Pinouts

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

Network Port Connector

Table C-2 describes the network port connector pinouts.

Table C-2 **Network Port Connector Pinouts**

Pin Number	Function
1	TD+
2	TD–
3	RD+
4	Not used
5	Not used
6	RD–
7	Not used
8	Not used

Access Port Connector

Table C-3 describes the access port connector pinouts.

Table C-3 **Access Port Connector Pinouts**

Pin Number	Function
1	RD+
2	RD–
3	TD+
4	Not Used
5	Not Used
6	TD–
7	Not Used
8	Not Used



Symbols

"more" Softkey Timer [4-21](#)

Numerics

802.1X

authentication server [1-19](#)

authenticator [1-19](#)

description [1-6](#)

network components [1-19](#)

supplicant [1-19](#)

Troubleshooting [9-13, 9-14](#)

802.1X Authentication menu

about [4-31](#)

options

Device Authentication [4-35](#)

EAP-MD5 [4-35](#)

Device ID [4-35](#)

Realm [4-35](#)

Shared Secret [4-35](#)

802.1X Authentication Status menu

about [4-31](#)

states [4-36](#)

A

abbreviated dialing [5-2](#)

AC adapter, connecting to [3-9](#)

access, to phone settings [3-20, 4-3](#)

access port

configuring [4-14](#)

connecting [3-10](#)

disabled [4-25](#)

forwarding packets to [4-24, 8-10](#)

purpose [3-5](#)

access to phone settings [4-2](#)

Access web page [8-3, 8-10](#)

adding

Cisco Unified IP Phones manually [2-15](#)

Cisco Unified IP Phones using
auto-registration [2-13](#)

Cisco Unified IP Phones using
auto-registration with TAPS [2-15](#)

Cisco Unified IP Phones using BAT [2-16](#)

users to Cisco Unified CallManager [5-19](#)

Admin. VLAN ID [4-11](#)

Alternate TFTP [4-12](#)

authenticated call [1-17](#)

authentication [1-11, 3-19](#)

authentication server, in 802.1X [1-19](#)

Authentication URL [4-17](#)
 authenticator, in 802.1X [1-19](#)
 auto answer [5-3](#)
 Auto Call Select [4-20](#)
 Auto Line Select [4-20](#)
 Auto Line Select Enabled [4-19](#)
 auto-pickup [5-3](#)
 auto-registration
 using [2-13](#)
 using with TAPS [2-15](#)
 auxiliary VLAN [2-4](#)

B

background image
 configuring [6-7](#)
 creating [6-5](#)
 custom [6-5](#)
 List.xml file [6-5](#)
 PNG file [6-5](#), [6-6](#)
 barge [1-18](#), [5-3](#)
 BAT (Bulk Administration Tool) [2-16](#)
 BLF for Call Lists [4-21](#)
 block external to external transfer [5-4](#)
 BootP [1-5](#)
 BOOTP Server [4-7](#)
 Bootstrap Protocol (BootP) [1-5](#)
 Busy Lamp Field (BLF) speed dial [5-4](#)

C

cable lock, connecting to phone [3-14](#)
 call
 authenticated [1-17](#)
 encrypted [1-17](#)
 call display restrictions [5-4](#)
 caller ID [5-6](#)
 call forward [5-4](#)
 desination override [5-5](#)
 display, configuring [5-5](#)
 call forward display, configuring [5-8](#)
 CallManager 1-5 [4-15](#)
 CallManager Configuration menu [4-15](#)
 call park [5-5](#)
 call pickup [5-5](#)
 Call Statistics screen [7-1](#), [7-17](#)
 call waiting [5-6](#)
 CAPF (Certificate Authority Proxy Function) [1-15](#), [3-20](#)
 cell phone interference [1-2](#)
 certificate trust list file
 See CTL file
 Cisco Call Back [5-6](#)
 Cisco Discovery Protocol
 See CDP
 Cisco IP Manager Assistant (Cisco IPMA) [5-7](#)
 Cisco Unified CallManager
 adding phone to database of [2-12](#)
 interactions with [2-2](#)

- required for Cisco Unified IP Phones [3-2](#)
- verifying settings [9-5](#)
- Cisco Unified CallManager Administration
 - adding telephony features using [5-2](#)
- Cisco Unified IP Phone
 - adding manually to Cisco Unified CallManager [2-15](#)
 - adding to Cisco Unified CallManager [2-12](#)
 - cleaning [9-24](#)
 - configuration checklist [1-22](#)
 - configuration requirements [1-21](#)
 - configuring user services [5-18](#)
 - installation checklist [1-27](#)
 - installation overview [1-21, 1-26](#)
 - installation requirements [1-21](#)
 - modifying phone button templates [5-17](#)
 - mounting to wall [3-15](#)
 - power [2-4](#)
 - registering [2-12](#)
 - registering with Cisco Unified CallManager [2-13, 2-15, 2-16](#)
 - resetting [9-17](#)
 - technical specifications [C-1](#)
 - using LDAP directories [5-16](#)
 - web page [8-1](#)
- Cisco Unified IP Phone Expansion Module 7914
 - attaching to phone [3-12](#)
 - troubleshooting [9-17](#)
- cleaning the Cisco Unified IP Phone [9-24](#)
- Clear softkey [7-4, 7-13](#)
- client matter codes [5-7](#)
- conference [5-7](#)
- configurable call forward display [5-5, 5-8](#)
- configuration file
 - creating [9-7](#)
 - encrypted [1-15](#)
 - modifying [6-1](#)
 - overview [2-8](#)
 - XmlDefault.cnf.xml [2-9](#)
- configuring
 - from a Cisco Unified IP Phone [4-4](#)
 - LDAP directories [5-16](#)
 - overview [1-21](#)
 - personal directories [5-17](#)
 - phone button templates [5-17](#)
 - softkey templates [5-18](#)
 - user features [5-19](#)
- connecting
 - handset [3-9](#)
 - headset [3-9](#)
 - to AC adapter [3-9](#)
 - to a computer [3-10](#)
 - to the network [3-10](#)
- CTL file
 - deleting from phone [9-18](#)
 - requesting [2-11](#)
 - unlocking [4-32](#)

custom phone rings

about [6-2](#)

creating [6-2, 6-4, 6-7](#)

PCM file requirements [6-3](#)

D

daisy chaining [9-14](#)

data VLAN [2-4](#)

Debug Display web page [8-3, 8-13](#)

Default Router 1-5 [4-10](#)

Device Authentication [4-35](#)

device authentication [1-14](#)

Device Configuration menu

displaying [4-2](#)

editing values [4-4](#)

overview [4-1](#)

sub-menus [4-15](#)

Device Information web page [8-2, 8-4](#)

DHCP

description [1-5](#)

troubleshooting [9-9](#)

DHCP Address Released [4-12](#)

DHCP Enabled [4-11](#)

DHCP Server [4-7](#)

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

Directories URL [4-17](#)

directory numbers, assigning manually [2-15](#)

direct transfer [5-8](#)

DNS server

troubleshooting [9-11](#)

verifying settings [9-5](#)

DNS Server 1-5 [4-11](#)

documentation, for users [A-3](#)

Domain Name [4-8](#)

Domain Name System (DNS) [4-8](#)

Domain Name System (DNS) server [4-11](#)

DSCP For Call Control [4-27](#)

DSCP For Configuration [4-27](#)

DSCP For Services [4-27](#)

E

EAP-MD5 [4-35](#)

editing, configuration values [4-4](#)

encrypted call [1-17](#)

encrypted configuration files [1-15](#)

encryption [1-11](#)

media [1-15](#)

Erase softkey [9-18](#)

error messages, used for troubleshooting [9-4](#)

Ethernet Configuration menu

about [4-24](#)

options

Span to PC Port [4-24](#)

Ethernet Information web page [8-3, 8-10](#)

extension mobility [5-8](#)

external power [2-5, 2-6](#)

F

fast dial service [5-8](#)

feature buttons

directories [1-4](#)

help [1-4](#)

messages [1-4](#)

services [1-4](#)

settings [1-4](#)

features

configuring on phone, overview [1-10](#)

configuring with Cisco Unified CallManager,
overview [1-10](#)

informing users about, overview [1-11](#)

file authentication [1-14](#)

file format

List.xml [6-5](#)

RingList.xml [6-2](#)

firmware, verifying version [7-15](#)

Firmware Versions screen [7-15](#)

footstand

button, identifying [1-4](#)

using to adjust phone height [3-14](#)

forced authorization codes [5-9](#)

G

G.729 [1-1](#)

G.729a [1-1](#)

G.729ab [1-1](#)

G.729b [1-1](#)

GARP Enabled [4-25](#)

group call pickup [5-9](#)

H

handset

connecting [3-9](#)

light strip [1-4](#)

headset

audio quality [3-7, 3-8](#)

connecting [3-7](#)

disabling [3-8](#)

quality [3-8](#)

support [3-6](#)

using [3-6](#)

headset button [1-4](#)

Headset Enabled [4-21](#)

headset port [3-9](#)

height, adjusting [3-14](#)

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

hold [5-9](#)

Host Name [4-7](#)

HTTP, description [1-6](#)

HTTP Configuration menu

about [4-17](#)

options

Authentication URL [4-17](#)

Directories URL [4-17](#)

Idle URL [4-18](#)

Idle URL Time [4-18](#)

Information URL [4-17](#)

Messages URL [4-17](#)

Proxy Server URL [4-17](#)

Services URL [4-17](#)

Hypertext Transfer Protocol

See HTTP

I

idle display

timeout [4-18](#)

XML service [4-18](#)

Idle URL [4-18](#)

Idle URL Time [4-18](#)

image authentication [1-14](#)

immediate divert [5-9](#)

Immediate Divert enhanced feature [5-10](#)

Information URL [4-17](#)

installing

Cisco Unified CallManager
configuration [3-2](#)

network requirements [3-2](#)

preparing [2-12](#)

requirements, overview [1-21](#)

interference, cell phone [1-2](#)

Internet Protocol (IP) [1-6](#)

IP Address [4-8](#)

IP address, troubleshooting [9-5](#)

J

join [5-10](#)

K

keypad, description [1-4](#)

L

language overlays [B-1](#)

LDAP directories, using with Cisco Unified IP
Phone [5-16](#)

light strip [1-4](#)

line buttons, identifying [1-3](#)

List.xml file [6-5](#)

Locale Configuration menu

about [4-18](#)

options

Network Locale [4-19](#)

Network Locale Version [4-19](#)

User Locale [4-18](#)

User Locale Char Set [4-18](#)

User Locale Version [4-18](#)

Locale Installer [B-2](#)

localization

Installing the Cisco Unified CallManager
Locale Installer [B-2](#)

phone button overlays for [B-1](#)

Logging Display [4-26](#)

M

MAC address [2-19, 4-7](#)

malicious caller identification (MCID) [5-10](#)

manufacturing installed certificate (MIC) [1-15](#)

Media Configuration menu

- about [4-21](#)
- options
 - Headset Enabled [4-21](#)
 - Recording Tone [4-22](#)
 - Recording Tone Duration [4-24](#)
 - Recording Tone Local Volume [4-23](#)
 - Recording Tone Remote Volume [4-24](#)
 - Speaker Enabled [4-21](#)
 - Video Capability Enabled [4-21](#)

media encryption [1-15](#)

meet-me conference [5-10](#)

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

Messages URL [4-17](#)

message waiting [5-11](#)

metrics, voice quality [7-18, 8-15](#)

MIC [1-15](#)

Model Information screen [7-1](#)

multilevel precedence and preemption (MLPP) [5-11](#)

music-on-hold [5-11](#)

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

N

native VLAN [2-4](#)

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

Network Configuration menu

- about [4-7](#)
- displaying [4-2](#)
- editing values [4-4](#)
- locking options [4-4](#)
- options
 - Admin. VLAN ID [4-11](#)
 - Alternate TFTP [4-12](#)
 - BOOTP Server [4-7](#)
 - Default Router 1-5 [4-10](#)
 - DHCP Address Released [4-12](#)
 - DHCP Enabled [4-11](#)
 - DHCP Server [4-7](#)
 - DNS Server 1-5 [4-11](#)
 - Domain Name [4-8](#)
 - Host Name [4-7](#)
 - IP Address [4-8](#)
 - MAC Address [4-7](#)
 - Operational VLAN ID [4-11](#)
 - PC Port Configuration [4-14](#)
 - Subnet Mask [4-8](#)
 - SW Port Configuration [4-13](#)
 - TFTP Server 1 [4-9](#)
 - TFTP Server 2 [4-10](#)

overview [4-1](#)

unlocking options [4-4](#)

Network Configuration web page [8-2, 8-6](#)

network connections, access port [3-5](#)

network connectivity, verifying [9-4](#)

networking protocol

802.1X [1-6](#)

BootP [1-5](#)

CDP [1-5](#)

DHCP [1-5](#)

HTTP [1-6](#)

IP [1-6](#)

RTCP [1-7](#)

RTP [1-6](#)

SCCP [1-7](#)

SIP [1-7](#)

TCP [1-7](#)

TFTP [1-7](#)

TLS [1-7](#)

UDP [1-8](#)

Network Locale [4-19](#)

Network Locale Version [4-19](#)

network outages, identifying [9-9](#)

network port

configuring [4-13](#)

connecting to [3-10](#)

network requirements, for installing [3-2](#)

network statistics [7-13, 8-10](#)

Network Statistics screen [7-13](#)

Network web page [8-3, 8-10](#)

O

on hook call transfer [5-11](#)

Operational VLAN ID [4-11](#)

other group pickup [5-12](#)

P

padlock icon [4-4](#)

PCM file requirements, for custom ring types [6-3](#)

PC Port Configuration [4-14](#)

PC Port Disabled [4-25](#)

personal directories, configuring [5-17](#)

phone button templates [5-17](#)

phone hardening [1-16](#)

phone lines, buttons for [1-3](#)

phone settings access [4-2](#)

physical connection, verifying [9-9](#)

PNG file [6-5, 6-6](#)

PoE [2-6, 2-7](#)

ports

access [3-5](#)

network [3-5](#)

power

external [2-4, 2-5, 2-6](#)

for the phone [2-4](#)

outage [2-7](#)

PoE [2-6, 2-7](#)

power over Ethernet

See PoE

power source

power injector [2-5, 2-6](#)

presence-enabled directories [5-12](#)

privacy [5-12](#)

programmable buttons, description [1-3](#)

Proxy Server URL [4-17](#)

Q

QoS Configuration menu

about [4-27](#)

options

DSCP For Call Control [4-27](#)

DSCP For Configuration [4-27](#)

DSCP For Services [4-27](#)

QRT softkey [5-12, 9-21](#)

Quality Reporting Tool (QRT) [5-12, 9-21](#)

R

Real-Time Control Protocol

See RTCP

Real-Time Transport Protocol

See RTP

Recording Tone [4-22](#)

Recording Tone Duration [4-24](#)

Recording Tone Local Volume [4-23](#)

Recording Tone Remote Volume [4-24](#)

redial [5-13](#)

reset, factory [9-19](#)

resetting

basic [9-18](#)

Cisco Unified IP phone [9-17](#)

continuously [9-8](#)

intentionally [9-10](#)

methods [9-18](#)

ring activity [5-13](#)

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

RingList.xml file format [6-2](#)

S

SCCP [1-7](#)

secure SRST reference [1-15](#)

securing the phone with a cable lock [3-14](#)

security

CAPF (Certificate Authority Proxy
Function) [1-15, 3-20](#)

configuring on phone [3-19](#)

device authentication [1-14](#)

encrypted configuration file [1-15](#)

file authentication [1-14](#)

image authentication [1-14](#)

Locally Significant Certificate (LSC) [3-19](#)

media encryption [1-15](#)

phone hardening [1-16](#)

secure SRST reference [1-15](#)

- security profiles [1-15, 1-17](#)
- signaling authentication [1-14](#)
- signaling encryption [1-15](#)
- troubleshooting [9-12](#)
- Security Configuration menu
 - options
 - 802.1X Authentication [4-31](#)
 - 802.1X Authentication Status [4-31](#)
 - GARP Enabled [4-25](#)
 - Logging Display [4-26](#)
 - PC Port Disabled [4-25](#)
 - Security Mode [4-26](#)
 - Voice VLAN Enabled [4-26](#)
 - Web Access Enabled [4-26](#)
- Security Configuration menu (on Device menu)
 - about [4-29](#)
- Security Configuration menu (on Settings menu)
 - about [4-25](#)
- Security Mode [4-26](#)
- security profiles [1-15, 1-17](#)
- services
 - configuring for users [5-18](#)
 - description [5-13](#)
 - subscribing to [5-19](#)
- services button, description of [1-4](#)
- Services URL [4-17](#)
- Services URL button [5-13](#)
- settings button, description of [1-4](#)
- Settings menu access [3-20, 4-3](#)
- shared line [5-14](#)
- signaling authentication [1-14](#)
- signaling encryption [1-15](#)
- SIP
 - description [1-7](#)
- softkey buttons
 - description of [1-4](#)
- softkey templates, configuring [5-18](#)
- Span to PC Port [4-24](#)
- Speaker button, disabling [3-6](#)
- Speaker Enabled [4-21](#)
- speakerphone [1-4](#)
- speed dial, buttons [1-3](#)
- speed dialing [5-2, 5-14](#)
- SRST [4-16, 8-7](#)
- startup problems [9-2](#)
- startup process
 - accessing TFTP server [2-11](#)
 - configuring VLAN [2-10](#)
 - contacting Cisco Unified CallManager [2-12](#)
 - loading stored phone image [2-10](#)
 - obtaining IP address [2-10](#)
 - obtaining power [2-10](#)
 - requesting configuration file [2-11](#)
 - requesting CTL file [2-11](#)
 - understanding [2-9](#)
- statistics
 - call [7-17](#)
 - network [8-10](#)

- streaming [8-13](#)
- Status menu [7-1, 7-3](#)
 - options
 - 802.1X Authentication Status [7-3](#)
- status messages [7-4](#)
- Status Messages screen [7-4](#)
- Status Messages web page [8-3, 8-13](#)
- Stream 0 web page [8-13](#)
- Stream 1 web page [8-3, 8-13](#)
- Stream 2 web page [8-3, 8-13](#)
- Stream 3 web page [8-3, 8-13](#)
- streaming statistics [8-13](#)
- Subnet Mask [4-8](#)
- supplicant, in 802.1X [1-19](#)
- Survivable Remote Site Telephony
 - See SRST
- switch
 - Cisco Catalyst [2-3](#)
 - internal Ethernet [2-3](#)
- SW Port Configuration [4-13](#)

T

- TAPS (Tool for Auto-Registered Phones Support) [2-15](#)
- TCP [1-7](#)
- technical specifications, for Cisco Unified IP Phone [C-1](#)
- telephony features
 - abbreviated dialing [5-2](#)
 - auto answer [5-3](#)
 - auto-pickup [5-3](#)
 - barge [1-18, 5-3](#)
 - block external to external transfer [5-4](#)
 - Busy Lamp Field (BLF) speed dial [5-4](#)
 - call display restrictions [5-4](#)
 - caller ID [5-6](#)
 - call forward [5-4](#)
 - call park [5-5](#)
 - call pickup [5-5](#)
 - call waiting [5-6](#)
 - Cisco Call Back [5-6](#)
 - Cisco IP Manager Assistant (Cisco IPMA) [5-7](#)
 - client matter codes [5-7](#)
 - conference [5-7](#)
 - configurable call forward display [5-5, 5-8](#)
 - direct transfer [5-8](#)
 - extension mobility [5-8](#)
 - fast dial service [5-8](#)
 - forced authorization codes [5-9](#)
 - group call pickup [5-9](#)
 - hold [5-9](#)
 - immediate divert [5-9](#)
 - join [5-10](#)
 - malicious caller identification (MCID) [5-10](#)
 - meet-me conference [5-10](#)
 - multilevel precedence and preemption (MLPP) [5-11](#)
 - music-on-hold [5-11](#)

- on hook call transfer [5-11](#)
- other group pickup [5-12](#)
- presence-enabled directories [5-12](#)
- privacy [5-12](#)
- redial [5-13](#)
- ring activity [5-13](#)
- services [5-13](#)
- Services URL button [5-13](#)
- shared line [5-14](#)
- speed dialing [5-14](#)
- Time-of-Day Routing [5-14](#)
- transfer [5-14](#)
- video mode [5-15](#)
- video support [5-15](#)
- voice messaging system [5-15](#)
- TFTP
 - description [1-7](#)
 - troubleshooting [9-4](#)
- TFTP Server 1 [4-9](#)
- TFTP Server 2 [4-10](#)
- time, displayed on phone [3-2](#)
- Time-of-Day Routing [5-14](#)
- TLS [2-9](#)
- transfer [5-14](#)
- Transmission Control Protocol
 - See TCP
- Transport Layer Security
 - See TLS
- Trivial File Transfer Protocol
 - See TFTP
- troubleshooting
 - Cisco Unified CallManager settings [9-5](#)
 - Cisco Unified IP Phone Expansion Module 7914 [9-17](#)
 - DHCP [9-9](#)
 - DNS [9-11](#)
 - DNS settings [9-5](#)
 - IP addressing and routing [9-5](#)
 - network connectivity [9-4](#)
 - network outages [9-9](#)
 - phones resetting [9-10](#)
 - physical connection [9-9](#)
 - security [9-12](#)
 - services on Cisco Unified CallManager [9-6](#)
 - TFTP settings [9-4](#)
 - VLAN configuration [9-10](#)

U

- UI Configuration menu
 - description [4-19](#)
 - options
 - Auto Call Select [4-20](#)
 - Auto Line Select [4-20](#)
 - BLF for Call Lists [4-21](#)
 - uncompressed wideband [1-1](#)
- Unlock softkey [4-33](#)
- User Datagram Protocol
 - See UDP

User Locale [4-18](#)

User Locale Char Set [4-18](#)

User Locale Version [4-18](#)

User Options web page

description [5-20](#)

giving users access to [5-20, A-2](#)

specifying options that appear [5-20](#)

users

accessing voice messaging system [A-4](#)

adding to Cisco Unified CallManager [5-19](#)

configuring personal directories [A-5](#)

documentation for [A-3](#)

providing support to [A-2](#)

required information [A-1](#)

subscribing to services [A-4](#)

V

Video Capability Enabled [4-21](#)

video mode [5-15](#)

video support [5-15](#)

VLAN

auxiliary, for voice traffic [2-4](#)

configuring [4-11](#)

configuring for voice networks [2-3](#)

native, for data traffic [2-4](#)

verifying [9-10](#)

VLAN, interaction with [2-3](#)

voice messaging system [5-15](#)

voice messaging system, accessing [A-4](#)

voice quality metrics [7-18, 8-15](#)

voice VLAN [2-4](#)

Voice VLAN Enabled [4-26](#)

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

W

wall mounting, Cisco Unified IP Phone [3-15](#)

Web Access Enabled [4-26](#)

web page

about [8-1](#)

Access [8-3, 8-10](#)

accessing [8-2](#)

Debug Display [8-3, 8-13](#)

Device Information [8-2, 8-4](#)

disabling access to [8-3](#)

Ethernet Information [8-3, 8-10](#)

Network [8-3, 8-10](#)

Network Configuration [8-6](#)

Network Configuration web page [8-2](#)

preventing access to [8-3](#)

Status Messages [8-3, 8-13](#)

Stream 0 [8-13](#)

Stream 1 [8-3, 8-13](#)

Stream 2 [8-3, 8-13](#)

Stream 3 [8-3, 8-13](#)

Wideband Headset setting [6-8](#)

X

XmlDefault.cnf.xml [2-9](#)