Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager 4.1(3)

Cisco Unified IP Phone 7906G and 7911G

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-10008-01

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.

CONTENTS

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 xvii
- 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 xxiv

CHAPTER 1 **An Overview of the Cisco Unified IP Phone** 1-1

- Understanding the Cisco Unified IP Phones 7906G and 7911G 1-2
- What Networking Protocols Are Used? 1-4
- What Features are Supported? 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
Identifying Encrypted and Authenticated Phone Calls 1-15
Security Restrictions 1-16
Overview of Configuring and Installing Cisco Unified IP Phones 1-17
Configuring Cisco Unified IP Phones in Cisco Unified CallManager 1-17
Checklist for Configuring the Cisco Unified IP Phones 7906G and 7911G in Cisco Unified CallManager 1-18
Installing Cisco Unified IP Phones 1-22
Checklist for Installing the Cisco Unified IP Phones 7906G and 7911G 1-23

CHAPTER 2 **Preparing to Install the Cisco Unified IP Phone on Your Network** 2-1
Understanding Interactions with Other Cisco Unified Communications 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 Phones 7906G and 7911G 2-4
Power Outage 2-4
Power Guidelines 2-5
Obtaining Additional Information about Power 2-5
Understanding Phone Configuration Files 2-6
Understanding the Phone Startup Process 2-7
Adding Phones to the Cisco Unified CallManager Database 2-11
Adding Phones with Auto-Registration 2-12
Adding Phones with Auto-Registration and TAPS 2-13

Adding Phones with Cisco Unified CallManager Administration 2-14
Adding Phones with BAT 2-15
Determining the MAC Address of a Cisco Unified IP Phone 2-15

CHAPTER 3 **Setting Up the Cisco Unified IP Phone 3-1**
Before You Begin 3-1
Network Requirements 3-2
Cisco Unified CallManager Configuration 3-3
Safety 3-3
Understanding the Cisco Unified IP Phones 7906G and 7911G Components 3-5
Network and Access Ports 3-5
Handset 3-5
Speaker 3-6
Monitor Mode 3-6
Group Listen Mode 3-6
Headset 3-7
Audio Quality Subjective to User 3-8
Connecting a Headset 3-9
Installing the Cisco Unified IP Phone 3-9
Mounting the Phone to a Wall 3-15
Verifying the Phone Startup Process 3-16
Configuring Startup Network Settings 3-16
Configuring Security on the Cisco Unified IP Phone 3-17

CHAPTER 4 **Configuring Settings on the Cisco Unified IP Phone 4-1**
Configuration Menus on the Cisco Unified IP Phones 7906G and 7911G 4-1
Displaying a Configuration Menu 4-2
Unlocking and Locking Options 4-3
Editing the Values of an Option Setting 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 4-18
Locale Configuration Menu 4-19
UI Configuration Menu 4-20
Media Configuration Menu 4-20
Ethernet Configuration Menu 4-21
Security Configuration Menu 4-21
QoS Configuration Menu 4-23
Network Configuration 4-24

CHAPTER 5 **Configuring Features, Templates, Services, and Users** 5-1
Telephony Features Available for the Phone 5-2
Configuring Corporate and Personal Directories 5-13
Configuring Corporate Directories 5-13
Configuring Personal Directory 5-13
Modifying Phone Button Templates 5-14
Configuring Softkey Templates 5-14
Setting Up Services 5-15
Adding Users to Cisco Unified CallManager 5-16
Specifying Options that Appear on the User Options Web Pages 5-17

CHAPTER 6 **Customizing the Cisco Unified IP Phone** 6-1
Creating Custom Phone Rings 6-1
RingList.xml File Format Requirements 6-2
PCM File Requirements for Custom Ring Types 6-3
Configuring a Custom Phone Ring 6-3

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

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 Screen 7-3
Trust List Screen 7-5
Model Information Screen 7-6
Status Menu 7-7
Status Messages Screen 7-8
Network Statistics Screen 7-16
Firmware Versions Screen 7-19

CHAPTER 8 **Monitoring the Cisco Unified IP Phone Remotely 8-1**

Accessing the Web Page for a Phone 8-2
Disabling Web Page Access 8-3
Device Information 8-4
Network Configuration 8-7
Network Statistics 8-12
Device Logs 8-15
Streaming Statistics 8-16

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
Registering the Phone with Cisco Unified CallManager 9-4
Checking Network Connectivity 9-4
Verifying TFTP Server Settings 9-5
Verifying IP Addressing and Routing 9-5
Verifying DNS Settings 9-6
Verifying Cisco Unified CallManager Settings 9-6
Cisco Unified CallManager and TFTP Services Are Not Running 9-6
Creating a New Configuration File 9-7
Cisco Unified IP Phone Resets Unexpectedly 9-8
Verifying Physical Connection 9-9
Identifying Intermittent Network Outages 9-9
Verifying DHCP Settings 9-9
Checking Static IP Address Settings 9-10
Verifying 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 9-12
Resetting or Restoring the Cisco Unified IP Phone 9-15
Performing a Basic Reset 9-15
Performing a Factory Reset 9-16
Using the Quality Report Tool 9-17
Where to Go for More Troubleshooting Information 9-18
Cleaning the Cisco Unified IP Phone 9-18

APPENDIX A **Providing Information to Users** A-1

How Users Obtain Support for the Cisco Unified IP Phone A-1

How Users Get Copies of Cisco Unified IP Phone Manuals A-2

How Users Subscribe to Services and Configure Phone Features A-2

How Users Access a Voice Messaging System A-3

How Users Configure Personal Directory Entries A-4

APPENDIX B **Supporting International Users** B-1

APPENDIX C **Technical Specifications** C-1

Physical and Operating Environment Specifications C-1

Cable Specifications C-2

Network and Access Port Pinouts C-2

INDEX

Preface

Overview

Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager 4.1.3, Cisco Unified IP Phone 7906G and 7911G provides the information you need to understand, install, configure, manage, and troubleshoot the Cisco Unified IP Phones 7906G and 7911G in a Voice-over-IP (VoIP) network.

Because of the complexity of a unified communications 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 for a list of related documentation.

Audience

Network engineers, system administrators, or telecom engineers should review this guide to learn the steps required to properly set up the Cisco Unified IP Phones 7906G and 7911G 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 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 unified communications 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 6, "Customizing the Cisco Unified IP Phone"	Explains how to customize phone ring sounds, background images, and the phone idle display at your site.
Chapter 7, "Viewing Security Information, 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"	Explains how to obtain status information about the phone using the phone's web page.
Chapter 9, "Troubleshooting and Maintenance"	Provides tips for troubleshooting the Cisco Unified IP Phone.
Appendix A, "Providing Information to Users"	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 Phones 7906G and 7911G

- *Cisco Unified IP Phone 7906G Installation Guide*
- *Cisco Unified IP Phone 7911G Installation Guide*
- *Cisco Unified IP Phone 7906G and 7911G Phone Guide*
- *Cisco Unified IP Phone 7911G Feature Enhancements*
- *Cisco Unified IP Phone Features A–Z*
- *Regulatory Compliance and Safety Information for the Cisco Unified IP Phone 7900 Series*
- *Installing the Universal Wall Mount Kit for the Cisco Unified IP Phone*
- *Customizing Your Cisco Unified IP Phone on the Web*

Cisco Unified CallManager Administration

- *Cisco Unified CallManager Administration Guide*
- *Cisco Unified CallManager System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified CallManager Serviceability System Guide*
- *Bulk Administration Tool User Guide for Cisco Unified CallManager*

Cisco Unified IP Phones Services and Features

- *Cisco Unified CallManager Features and Services Guide*

Security Features

- *Cisco Unified CallManager Security Guide*

Unified Communications Network Design

- *Cisco Unified Communications Solution Reference Network Design (SRND) for Cisco Unified CallManager 4.0*

Other Documentation

- *Installing and Configuring the Cisco Customer Directory Configuration Plugin*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

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 comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

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:

- 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 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 at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

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 (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI 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.

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 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 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

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *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 for networking professionals to 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

- 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:

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

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

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

Warnings use the following 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 figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto 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 أخر 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.

SAČUVAJTE 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 כד 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 Phones 7906G and 7911G provide voice communication over an Internet Protocol (IP) network. It functions much like a standard digital business telephone, allowing you to place and receive phone calls and to access features such as mute, hold, transfer, and speed dial. In addition, because the phone is connected to your data network, it offers enhanced productivity features, including access to network information, XML applications, and customizeable features.

The Cisco Unified IP Phone, like other network devices, must be configured and managed. The phone encodes G.711a, G.711µ, G.729a, G.729ab, and decodes all variants of G.711 and G.729. The phone also supports wideband (16bits, 16kHz) audio.

This chapter includes the following topics:

- Understanding the Cisco Unified IP Phones 7906G and 7911G, page 1-2
- What Networking Protocols Are Used?, page 1-4
- What Features are Supported?, page 1-7
- Understanding Security Features for Cisco Unified IP Phones, page 1-10
- Overview of Configuring and Installing Cisco Unified IP Phones, page 1-17

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 Phones 7906G and 7911G

The Cisco Unified IP Phones 7906G and 7911G are basic IP phone designed for cubicles, classrooms, factory floors, warehouses, lobbies, and any other location where the phone either complements the user's set of communication devices or is seldom used. The Cisco Unified IP Phones 7906G and 7911G:

- Provides a graphical display with dynamic softkeys, icons, and scrollable directories for easy access to a core set of business features
- Supports up to six calls on one directory number
- Supports inline power for both Cisco inline power or IEEE 802.3af Power over Ethernet
- Supports enhanced security features including:
  - Manufacturing and field installable certificates
  - Secure Media and Signaling
  - Authenticated Configuration
- Supports enhanced calling features plus audio and text XML applications
- Figure 1-1 shows the main components of the Cisco Unified IP Phones 7906G and 7911G.

Figure 1-1 Cisco Unified IP Phones 7906G and 7911G

1	Phone screen	Displays phone features such as phone number, call status, and softkeys.
2	Cisco Unified IP Phone series	Indicates your Cisco Unified IP Phone model series.
3	Softkeys	Each softkey activates a softkey option displayed on your phone screen
4	Navigation button 	Allows you to scroll through menu items and highlight items. When the phone is on-hook, displays your Speed Dials.
5	Applications menu button	Displays the Applications menu that provides access to a voice messaging system, phone logs and directories, settings, and services.

6	Hold button 	Places the active call on hold, resumes a call on hold, and switches between an active call and a call on hold.
7	Keypad	Allows you to dial phone numbers, enter letters, and choose menu items.
8	Volume button 	Controls the handset, headset, speaker, and ringer volume.
9	Handset	Functions like a traditional handset. The light strip at the top of the handset blinks when the phone rings and stays lit if there is a new voice message (depending on your voice messaging system).
10	Footstand	Allows the phone to stand at a convenient angle on a desk or table. Also may be removed for wall mounting to mounting screws or to a Cisco Unified IP Phone wall mount kit.

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 supported networking protocols on the Cisco Unified IP Phones 7906G and 7911G.

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 information about DHCP configurations, refer to the "Cisco TFTP" chapter in the *Cisco Unified CallManager System Guide*.
HyperText Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the World Wide Web.	The Cisco Unified IP Phones use HTTP for the XML services and for troubleshooting purposes.

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

Networking Protocol	Purpose	Usage Notes
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communicate using IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnets, and 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.
Secure Real-Time Transport Protocol (SRTP)	SRTP is available in addition to RTP. SRTP adds security by encrypting media streams during data transport.	For SRTP to work, the phone or phones being called must also support SRTP or else those phones cannot decrypt the secure media stream.
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.
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.

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

Networking Protocol	Purpose	Usage Notes
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the Cisco Unified IP Phone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server. If more than one TFTP server is running in your network, you must manually assign a TFTP server to each phone locally.
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	Cisco Unified IP Phones receive and process UDP messages.

Related Topics

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

What Features are Supported?

The Cisco Unified IP Phones 7906G and 7911G function much like traditional analog phones, allowing you to place and receive telephone calls. In addition to traditional telephony features, each Cisco 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 1-8
- Configuring Telephony Features, page 1-9
- Configuring Network Parameters Using the Cisco Unified IP Phone, page 1-9
- Providing Users with Feature Information, page 1-10

Feature Overview

Cisco Unified IP Phones provide core business features, 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, see the "Telephony Features Available for the 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. 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-workers contact information directly from their IP phones. Or, you can also use XML to enable users to access information such as weather, stocks, quote of the day, and other web-based information. For information about configuring such services, see the "Configuring Corporate and Personal Directories" section on page 5-13 and the "Setting Up Services" section on page 5-15.

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 Security Information, 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 certain 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 Phone" section on page 5-2 and *Cisco Unified CallManager Administration Guide* for additional information.

For more information about the Cisco Unified CallManager Administration application, refer to Cisco Unified CallManager documentation, including *Cisco Unified CallManager System 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 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 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 Security Information, 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/ip_clmgr/english/index.htm.

From this site, you can view and order various user guides, including wallet cards. For complete ordering information, see the "Obtaining Documentation" section on page xiv.

In addition to providing users with documentation, it is important to inform them of available Cisco Unified IP Phone features—including features 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."

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 Unified Communications 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, encrypts media streams between Cisco Unified IP phones, and encrypts call signaling between Cisco Unified CallManager and the 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 *Cisco Unified CallManager Security Guide*.
Security features supported on the Cisco Unified IP Phone	See the "Overview of Supported Security Features" section on page 1-12.
Restrictions regarding security features	See the "Security Restrictions" section on page 1-16.
Identifying phone calls for which security is implemented	See the "Identifying Encrypted and Authenticated Phone Calls" section on page 1-15.
Transport Layer Security (TLS) connection	• See the "What Networking Protocols Are Used?" section on page 1-4. • See the "Understanding Phone Configuration Files" section on page 2-6.
Security and the phone startup process	See the "Understanding the Phone Startup Process" section on page 2-7.
Security and phone configuration files	See the "Understanding Phone Configuration Files" section on page 2-6.
Changing the TFTP Server 1 or TFTP Server 2 option on the phone when security is implemented	See 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 on the phone	See the "Security Configuration Menu" section on page 4-21.
Items on the Security Configuration screen on the phone	See the "Security Configuration Menu" section on page 7-2.
Unlocking the certificate trust list (CTL) file	See the "CTL File Screen" section on page 7-3.
Disabling access to a phone's web pages	See the "Disabling Web Page Access" section on page 8-3.

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

Topic	Reference
Troubleshooting	• See the "Troubleshooting Cisco Unified IP Phone Security" section on page 9-12. • See the *Cisco Unified CallManager Security Guide*, Troubleshooting chapter.
Deleting the CTL file from the phone	See the "Resetting or Restoring the Cisco Unified IP Phone" section on page 9-15.
Resetting or restoring the phone	See the "Resetting or Restoring the Cisco Unified IP Phone" section on page 9-15.

Overview of Supported Security Features

This section provides an overview of the security features that the phone supports. 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, press the **Applications Menu button** and choose **Settings > Security Configuration**. For more information, see the "Security Configuration Menu" section on page 7-2.

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 *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 Certificate Authority Proxy Function (CAPF). Alternatively, you can install an Locally Significant Certificate (LSC) from the Security Configuration menu on the phone. See the "Configuring Security on the Cisco Unified IP Phone" section on page 3-17 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 configured in authenticated or encrypted mode unless they can be authenticated by the Cisco Unified CallManager. Phones in non-secure mode are not authenticated because no TLS session is established.
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 Phones 7906G and 7911G contains a unique 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	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.

Table 1-3 Overview of Security Features (continued)

Feature	Description
Optional disabling of the web server functionality for a phone	You can prevent access to a phone's web page, which displays a variety of operational statistics for the phone.
Phone hardening	Additional security options, which you control from Cisco Unified CallManager Administration: • Disabling PC port (applies to 7911G only) • Disabling Gratuitous Address Resolution Protocol (GARP) • Disabling PC Voice VLAN access (applies to 7911G only) • 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.

Related Topics

- Identifying Encrypted and Authenticated Phone Calls, page 1-15
- Device Configuration Menu, page 4-15
- Security Restrictions, page 1-16

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 LCD 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 end-to-end, the call progress icon to the right of the call duration timer in the phone LCD screen changes to the following 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 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 a non-IP call leg, for example, PSTN, the call will be nonsecure even though it is encrypted within the IP network and has a lock icon associated with it.

Related Topic

- Understanding Security Features for Cisco Unified IP Phones, page 1-10
- Security Restrictions, page 1-16

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 barge initiator's phone.

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.

Overview of Configuring and Installing Cisco Unified IP Phones

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

After you have set up the unified communications 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 1-17
- Installing Cisco Unified IP Phones, page 1-22

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 2-11.

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

Checklist for Configuring the Cisco Unified IP Phones 7906G and 7911G in Cisco Unified CallManager

Table 1-4 provides an overview and checklist of configuration tasks for the Cisco Unified IP Phones 7906G and 7911G in Cisco Unified CallManager. The list presents tasks in 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 Phones 7906G and 7911G 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 – Calling search space and location information (if used) – Number of lines, associated directory numbers (DNs), and partitions 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 the *Cisco Unified CallManager System Guide,* Cisco Unified IP Phone chapter. See the "Telephony Features Available for the Phone" section on page 5-2.
2. Customize phone button templates (if required).	Adds Privacy feature to meet user needs.	Refer to the *Cisco Unified CallManager Administration Guide*, Phone Button Template Configuration chapter. See the "Modifying Phone Button Templates" section on page 5-14.

Table 1-4 Checklist for Configuring the Cisco Unified IP Phones 7906G and 7911G in Cisco Unified CallManager (continued)

Task	Purpose	For More Information
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 the *Cisco Unified CallManager Administration Guide*, Cisco Unified IP Phone Configuration chapter. For information about Product Specific Configuration fields, refer to "I" Button Help in the Phone Configuration window.
4. Add and configure the directory number on the phone by completing these required fields in the Directory Number Configuration window. – Directory number – 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 the *Cisco Unified CallManager Administration Guide*, 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 Phone" section on page 5-2.

Table 1-4 Checklist for Configuring the Cisco Unified IP Phones 7906G and 7911G in Cisco Unified CallManager (continued)

Task	Purpose	For More Information
5. Customize softkey templates (optional).	Adds, deletes, or changes order of softkey features that display on the user's phone to meet feature usage needs.	Refer to the *Cisco Unified CallManager Administration Guide*, Softkey Template Configuration chapter. See the "Configuring Softkey Templates" section on page 5-14.
6. Assign speed-dial numbers (optional).	Adds speed-dial numbers, **Note** Users can change speed-dial settings on their phones with Cisco Unified IP Phone User Options.	Refer to the *Cisco Unified CallManager Administration Guide*, Cisco Unified IP Phone Configuration chapter, "Configuring Speed-Dial Buttons" section.
7. Configure Cisco Unified IP Phone services and assign services (optional).	Provides IP Phone services. **Note** Users can add or change services on their phones with the Cisco Unified IP Phone User Options.	Refer to the *Cisco Unified CallManager Administration Guide*, Cisco Unified IP Phone Services Configuration chapter. See the "Setting Up Services" section on page 5-15.

Table 1-4 Checklist for Configuring the Cisco Unified IP Phones 7906G and 7911G in Cisco Unified CallManager (continued)

Task	Purpose	For More Information
8. Add user information by configuring required fields (optional). – Name (last) – User ID – Password (for User Options web pages) – PIN (for use with Extension Mobility	Adds user information to the global directory for Cisco Unified CallManager. **Note** To search for a user in the Corporate Directory, you must add users to Cisco Unified CallMana ger.	Refer to the *Cisco Unified CallManager Administration Guide*, Adding a New User chapter. See the "Adding Users to Cisco Unified CallManag er" section on page 5-16.
9. 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 the *Cisco Unified CallManager Administration Guide*, 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 footstand, handset, cables, and other accessories.

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 Phones 7906G and 7911G

Table 1-5 provides an overview and checklist of installation tasks for the Cisco Unified IP Phone 7906G and 7911G. The list presents tasks in a suggested order to guide you through the phone installation 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 1-5 Checklist for Installing the Cisco Unified IP Phones 7906G and 7911G

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 Phones 7906G and 7911G" 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.
3. Monitor the phone startup process.	Verifies that phone is configured properly	See the "Verifying the Phone Startup Process" section on page 3-16.

Table 1-5 Checklist for Installing the Cisco Unified IP Phones 7906G and 7911G (continued)

Task	Purpose	For More Information
4. Configure these network settings on the phone by choosing **Settings > Network Configuration**. **Note** Unlock the phone settings before making these changes from the phone. To enable DHCP: **a.** Set DHCP Enabled to **Yes**. **b.** To use an alternate TFTP server, set Alternate TFTP Server to **Yes**. Enter **IP address** for TFTP Server 1. To disable DHCP: **a.** Set DHCP Enabled to **No**. **b.** Enter static **IP address** for phone. **c.** Enter subnet mask. **d.** Enter default router IP addresses. **e.** Enter domain name where phone resides. **f.** 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 3-16. See the "Network Configuration Menu" section on page 4-7.
5. 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 3-17.

Table 1-5 Checklist for Installing the Cisco Unified IP Phones 7906G and 7911G (continued)

Task	Purpose	For More Information
6. Make calls with the Cisco Unified IP Phone.	Verifies that the phone and features work correctly.	Refer to the *Cisco Unified IP Phones 7906G and 7911G Guide*.
7. Provide information to end users about how to use their phones and how to configure their phone options.	Ensures that users have adequate information to successfully use their Cisco Unified IP Phones.	See Appendix A, "Providing Information to Users."

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 Communications and network components, including Cisco Unified CallManager, DNS and DHCP servers, TFTP servers, and media resources.

This chapter provides an overview of the interaction between the Cisco Unified IP Phones 7906G and 7911G and other key components of the Voice-over-IP (VoIP) network, and focuses on the interactions between the Cisco Unified IP Phones 7906G and 7911G and Cisco Unified CallManager, TFTP server, and switches. It includes these topics:

- Understanding Interactions with Other Cisco Unified Communications Products, page 2-2
- Understanding the Phone Startup Process, page 2-7
- Providing Power to the Cisco Unified IP Phones 7906G and 7911G, page 2-4
- Understanding Phone Configuration Files, page 2-6
- Adding Phones to the Cisco Unified CallManager Database, page 2-11
- Determining the MAC Address of a Cisco Unified IP Phone, page 2-15

Understanding Interactions with Other Cisco Unified Communications Products

To function in the unified communications 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 these 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 Cisco Unified Communications system—the phones, the access gateways, and the resources necessary for such features as call conferencing and route planning. Cisco Unified CallManager also provides authentication and encryption if configured for the communications system.

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 1-10.

Note If the Cisco Unified IP Phone model that you want to configure does not appear in the Phone Type drop-down list in Cisco Unified 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 Phone, page 5-2

Understanding How the Cisco Unified IP Phone Interacts with the VLAN

The Cisco Unified IP Phone 7911G has an internal Ethernet switch, which enables forwarding of packets to the phone and to the network port and access port on the back of the phone. The Cisco Unified IP Phone 7906G has an Ethernet port, which enables forwarding of packets to the phone and to the network port.

If a computer is connected to the access port (Cisco Unified IP Phone 7911G), the computer and the phone share the same physical link to the switch and the same port on the switch. This shared physical link affects the VLAN configuration on the network in the following ways:

- Although current VLANs might be configured on an IP subnet basis, additional IP addresses may not be available to assign the phone to the same subnet as other devices that connect to the same port.
- Data traffic present on the data/native VLAN may reduce the quality of Voice-over-IP traffic.
- Network security may necessitate the isolation of the VLAN voice traffic from the VLAN data traffic.

You can resolve these issues by isolating the voice traffic onto a separate VLAN, so that the switch port to which the phone is connected uses separate VLANs for the following types of traffic:

- 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, 7911G only)

Isolating the phones on a separate, auxiliary VLAN improves the quality of the voice traffic and allows a large number of phones to be added to an existing network in which 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 2-7
- Network Configuration Menu, page 4-7

Providing Power to the Cisco Unified IP Phones 7906G and 7911G

The Cisco Unified IP Phones 7906G and 7911G 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.

These sections provide more information about powering a phone:

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

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.

Power Guidelines

Table 2-1 provides guidelines that apply to external power and to PoE power for the Cisco Unified IP Phones 7906G and 7911G.

Table 2-1 Guidelines for Powering the Cisco Unified IP Phones 7906G and 7911G

Power Type	Guidelines
External power—Provided through a Cisco external power supply	The CP-PWR-CUBE-3 external power supply may be used with the Cisco Unified IP Phones 7906G and 7911G.
PoE power—Provided by a switch through the Ethernet cable attached to the phone	• The Cisco Unified IP Phones 7906G and 7911G support both Cisco inline power and IEEE 802.3af Power over Ethernet. • 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.

Obtaining Additional Information about Power

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

- Cisco switches that work with the Cisco Unified IP Phones 7906G and 7911G
- The Cisco IOS releases that support bidirectional power negotiation
- Other requirements and restrictions regarding power

Table 2-2 Related Documentation for Power

Document Topics	URL
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.

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 these 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 SEP*mac_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 goes through a standard startup process, as described in Table 2-3. Depending on your specific network configuration, not all of these steps may occur on your Cisco Unified IP Phone.

Table 2-3 Cisco Unified IP Phone Startup Process

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.	See the "Providing Power to the Cisco Unified IP Phone s 7906G and 7911G" section on page 2-4. See the "Resolving Startup Problems" section on 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.	See the "Resolving Startup Problems" section on page 9-2.
3. Configuring VLAN.	If the Cisco Unified IP Phone is connected to a Cisco switch, the switch next informs the phone of the voice VLAN defined on the switch port. The phone needs to know its VLAN membership before it can proceed with the Dynamic Host Configuration Protocol (DHCP) request for an IP address. If a third-party switch is used and VLANs are configured, the VLAN on the phone must be manually configured.	See the "Network Configuration Menu" section on page 4-7. See the "Resolving Startup Problems" section on 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.	See the "Network Configuration Menu" section on page 4-7. See the "Resolving Startup Problems" section on page 9-2.

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

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.	See the "Network Configuration Menu" section on page 4-7. See the "Resolving Startup Problems" section on 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.	Refer to the *Cisco Unified CallManager Security Guide*, "Configuring the Cisco CTL Client" chapter.

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

Step	Description	Related Topics
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.	See the "Understanding Phone Configuration Files" section on page 2-6. See the "Resolving Startup Problems" section on page 9-2.
8. Contacting Cisco Unified Call Manager.	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.	See the "Resolving Startup Problems" section on 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 2-12
- Adding Phones with Auto-Registration and TAPS, page 2-13
- Adding Phones with Cisco Unified CallManager Administration, page 2-14
- Adding Phones with BAT, page 2-15

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

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

Method	Requires MAC Address?	Notes
Auto-registration	No	Provides no control over directory number assignment to phone. Not available when security or encryption is enabled.
Auto-registration with TAPS	No	Requires auto-registration and the Bulk Administration Tool (BAT); updates the Cisco Unified CallManager database with the MAC address and DNs for the device when user calls TAPS from the phone.

Table 2-4 Methods for Adding Phones to the Cisco Unified CallManager Database (continued)

Method	Requires MAC Address?	Notes
Using the Cisco Unified Call Manager Administration	Yes	Must add phones individually.
Using BAT	Yes	Can add groups of same model of phone. Can schedule when phones are added to the Cisco CallManager database.

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 Cisco Unified Communications 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 Auto-registration works best when you are adding fewer than 100 phones to your network. If you need to add more than 100 phones, use the Bulk Administration Tool (BAT). See the "Adding Phones with BAT" section on page 2-15.

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 2-13
- Adding Phones with Cisco Unified CallManager Administration, page 2-14
- Adding Phones with BAT, page 2-15

Adding Phones with Auto-Registration and TAPS

The Tool for Auto-Registered Phones Support (TAPS) 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 Auto-registration with TAPS works best when you are adding fewer than 100 phones to your network. If you need to add more than 100 phones, use the Bulk Administration Tool (BAT). See the "Adding Phones with BAT" section on page 2-15.

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 Unified 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 *Bulk Administration Tool User Guide for Cisco Unified CallManager* for more information about BAT and about TAPS.

Related Topics

- Adding Phones with Auto-Registration, page 2-12
- Adding Phones with Cisco Unified CallManager Administration, page 2-14
- Adding Phones with BAT, page 2-15

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 of a Cisco Unified IP Phone" section on page 2-15.

After you have collected MAC addresses, choose **Device > Add a New Device** in Cisco Unified CallManager Administration 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 2-12
- Adding Phones with Auto-Registration and TAPS, page 2-13
- Adding Phones with BAT, page 2-15

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 of a Cisco Unified IP Phone" section on page 2-15.

For more information about using BAT, refer to *Cisco Unified CallManager Administration Guide* and to *Bulk Administration Tool User Guide for Cisco Unified CallManager*.

Related Topics

- Adding Phones with Auto-Registration, page 2-12
- Adding Phones with Auto-Registration and TAPS, page 2-13
- Adding Phones with Cisco Unified CallManager Administration, page 2-14

Determining the MAC Address of a Cisco Unified IP Phone

You can determine the MAC address for a phone in any of these ways:

- From the phone, press the **Applications Menu** button, then choose **Settings > 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 helps you install the Cisco Unified IP Phones 7906G and 7911G on a Cisco Unified Communications network, and includes these topics:

- Before You Begin, page 3-1
- Installing the Cisco Unified IP Phone, page 3-9
- Mounting the Phone to a Wall, page 3-15
- Verifying the Phone Startup Process, page 3-16
- Configuring Startup Network Settings, page 3-16
- Configuring Security on the Cisco Unified IP Phone, page 3-17

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 3-3
- Network and Access Ports, page 3-5

- Handset, page 3-5
- Speaker, page 3-6
- Installing the Cisco Unified IP Phone, page 3-9

Network Requirements

For the Cisco Unified IP Phones 7906G and 7911G to successfully operate as a Cisco Unified IP Phone endpoint in your network, your network must meet these requirements:

- Working Voice-over-IP (VoIP) Network
  - VoIP configured on your Cisco routers and gateways
  - Cisco Unified CallManager Release 3.3(5) or higher installed in your network and configured to handle call processing

Note The minimum firmware release that must be installed on the phone is 7.2(1) for the Cisco Unified IP Phone 7911G and 7.2(3) for Cisco Unified IP Phone 7906G.

Note Cisco Unified Call Manager 4.0 and 5.0(1) do not support the Cisco Unified IP Phone 7906G.

- 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 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 2-11.

You must use Cisco Unified CallManager to configure and assign features to the Cisco Unified IP Phones. See the "Telephony Features Available for the 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 5-16 for details.

Safety

Review the following warnings before installing the Cisco Unified IP Phones 7906G and 7911G. 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 connecting the system to the power source.** Statement 1004

Warning **Only trained and qualified personnel should be allowed to install or replace this equipment.** Statement 49

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

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.** Statement 1021

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

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

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, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).** Statement 13

Warning **The device is designed to work with TN power systems.** Statement 19

Warning **The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.** Statement 66

Understanding the Cisco Unified IP Phones 7906G and 7911G Components

The Cisco Unified IP Phones 7906G and 7911G include these components on the phone or as accessories for the phone:

- Network and Access Ports, page 3-5
- Handset, page 3-5
- Speaker, page 3-6
- Headset, page 3-7

Network and Access Ports

The following ports are available on the Cisco Unified IP Phones 7906G and 7911G:

- Network port—Labeled 10/100 SW. Use the network port to connect the phone to the network. You must use a straight-through cable on this port. The phone can also obtain inline power from the Cisco Catalyst switch over this connection. See the "Providing Power to the Cisco Unified IP Phones 7906G and 7911G" section on page 2-4 for details.
- Access port (Cisco Unified IP Phone 7911G only)—Labeled 10/100 PC. Use the access port to connect a network device, such as a computer, to the phone. You must use a straight-through cable on this port.

Each port supports 10/100 Mbps half- or full-duplex connections to external devices. The speed and connection type are set through auto-negotiation. You can use either Category 3 or 5 cabling for 10-Mbps connections, but you must use Category 5 for 100 Mbps connections.

See Figure 3-3 for the connection ports available on the back of the Cisco Unified IP Phones 7906G and 7911G.

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.

Speaker

The Cisco Unified IP Phones 7906G and 7911G include a speaker that you can use to monitor calls. You can enable either the Monitor mode or Group Listen mode to allow users to listen on the speaker.

The speaker is enabled by default. You must disable the speaker 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.

Monitor Mode

In Monitor mode, users can only listen to a call on the speaker. To speak to the other party on the call, users must pick up the handset.

Monitor mode is enabled by default if the speaker is enabled on Cisco Unified CallManager Administration.

From the phone, users can turn on the Monitor function with the **Monitor** softkey, and turn off this function with the **MonOff** softkey or by picking up the handset.

Group Listen Mode

In Group Listen mode, both the handset and speaker can be active at the same time. During a call, one user can talk into the handset while other users can listen over the speaker.

Enabling Group Listen Mode on Cisco Unified CallManager

Group Listen mode is disabled by default. To enable this mode, you must do so from the Phone Configuration page in Cisco Unified CallManager Administration.

Note In addition to enabling Group Listen mode, the speaker must be enabled for Group Listen functionality.

From Cisco Unified CallManager Administration, choose **Device > Phone** and locate the phone you want to modify. In the Phone Configuration web page for the phone (Product Specific Configuration section), check the **Enable Group Listen** check box.

If Group Listen mode is enabled, the Monitor feature softkeys are not available on the phone.

Activating Group Listen on the Phone

Group Listen softkeys are displayed if Group Listen mode is enabled by the administrator on Cisco Unified CallManager. However, these softkeys cannot be configured by using the Cisco Unified CallManager softkey template.

- **GListen**—Activates Group Listen on the phone. Displayed when Group Listen mode is enabled by the administrator but not activated on the phone. Once Group Listen is activated on the phone (by pressing **GListen**), users can deactivate it by hanging up the handset or by pressing **GLOff**.
- **GLOff**—Deactivates Group Listen on the phone. Displayed when Group Listen mode is enabled by the administrator and activated on the phone.

Note If Group Listen mode is enabled in Cisco Unified CallManager, the **GListen** and **GLOff** softkeys replace the **Monitor** and **MonOff** softkeys on the phone.

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.

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 the Cisco Unified IP Phone Power Cube 3 (CP-PWR-CUBE-3).

Audio Quality Subjective to 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, see:

http://www.vxicorp.com/cisco

http://www.plantronics.com/cisco

Connecting a Headset

To connect a headset to the Cisco Unified IP Phone, plug it into the RJ-9 Handset port on the back of the phone. Depending on headset manufacturer's recommendations, an external amplifier may be required. Refer to headset manufacturer's product documentation for details.

You can use the headset with all of the features on the Cisco Unified IP Phone, including using the Volume button.

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, Figure 3-3, and Figure 3-4 for a graphical overview of the procedures that follow.

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

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

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

Procedure	Notes	Reference
1. Connect the footstand to the back of the phone. See Figure 3-1 and Figure 3-2. **Note** Figure 3-1 shows the Cisco Unified IP Phone 7911G. The procedure for connecting the footstand is the same for the Cisco Unified IP Phone 7906G.	—	—
2. Connect the handset to the Handset port.	—	—
3. Connect the power supply to the Cisco DC Adapter port (DC48V).	Optional. When connecting phones powered by an external power supply, you must connect the power supply to the phone before connecting the Ethernet cable to the phone. When disconnecting the phone, you must disconnect the Ethernet cable before disconnecting the power supply.	See the "Providing Power to the Cisco Unified IP Phones 7906G and 7911G" section on page 2-4.
4. Connect a Category 3 or 5 straight-through Ethernet cable from the switch to the 10/100 SW port.	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.
5. (Cisco Unified IP Phone 7911G only) Connect a Category 3 or 5 straight-through Ethernet cable from another network device, such as a desktop computer, to the 10/100 PC port.	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 Connecting the Footstand (Cisco Unified IP Phone Model 7906G Shown)

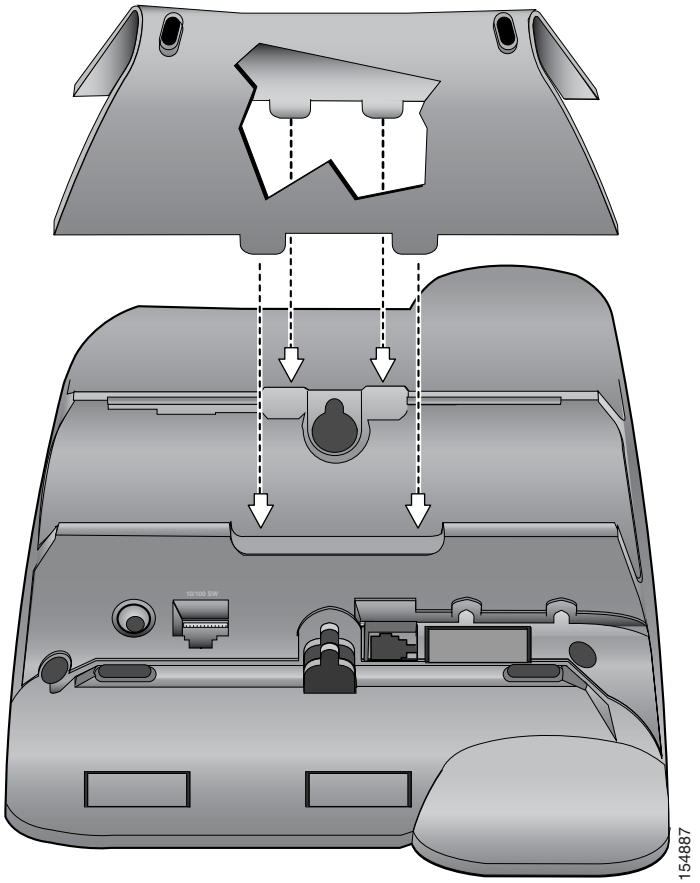


Figure 3-2 Connecting the Footstand (Cisco Unified IP Phone Model 7911G Shown)

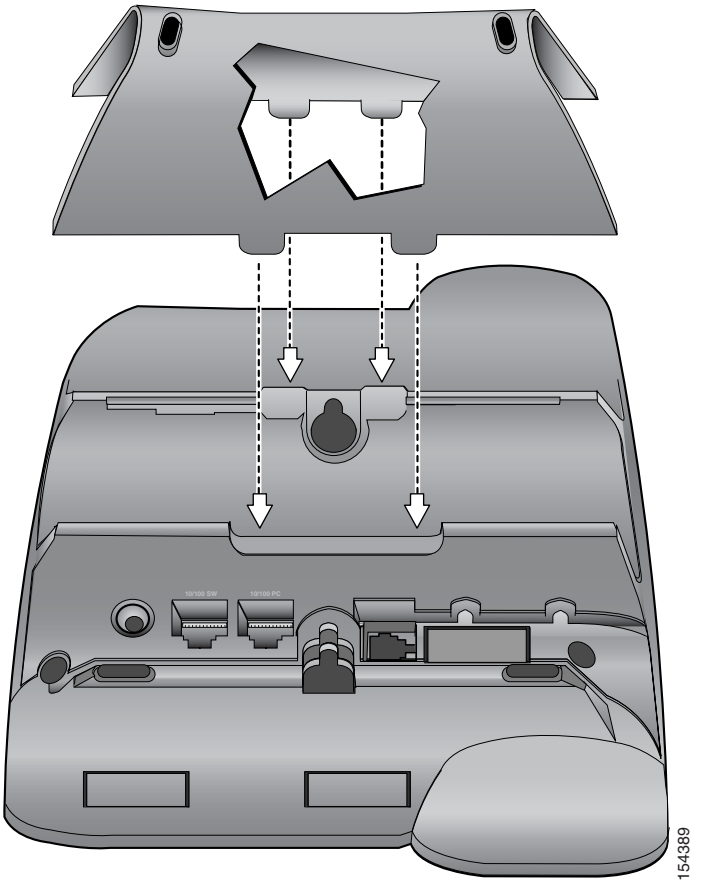
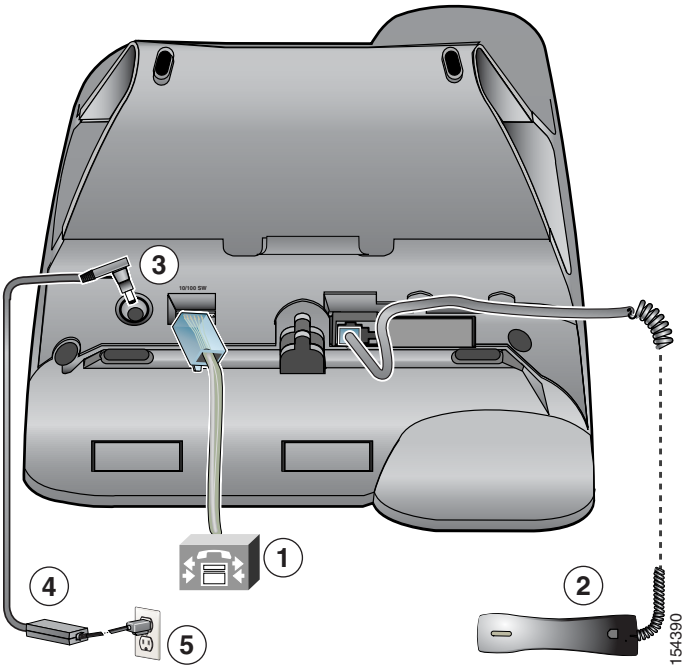
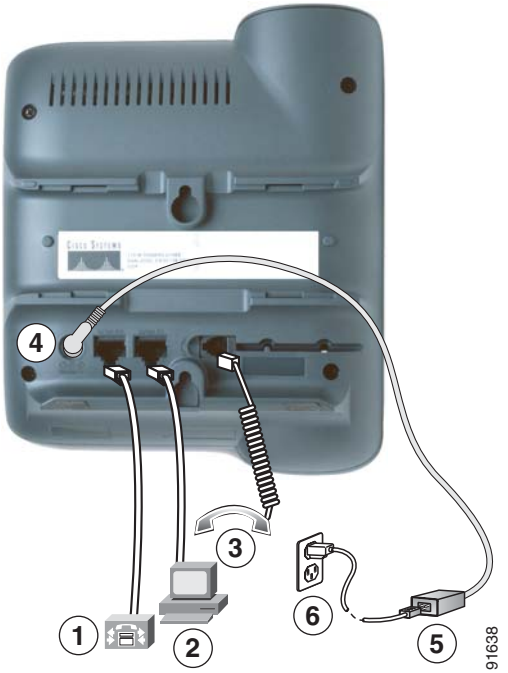


Figure 3-3 Cisco Unified IP Phone Model 7906G Cable Connections



1	Network port (10/100 SW)	**4**	AC-to-DC power supply
2	Handset port	**5**	AC power cord
3	DC Adapter port (DC48V)		

Figure 3-4 Cisco Unified IP Phone Model 7911G Cable Connections



1	Network port (10/100 SW)	**4**	DC Adapter port (DC48V)
2	Access port (10/100 PC)	**5**	AC-to-DC power supply
3	Handset port	**6**	AC power cord

Related Topics

- Before You Begin, page 3-1
- Mounting the Phone to a Wall, page 3-15
- Configuring Startup Network Settings, page 3-16

Mounting the Phone to a Wall

You can mount the Cisco Unified IP Phone on a wall using the back of the phone 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 phones.) If you attach the phone to a wall using the back of the phone 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

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 the *Installing the Universal Wall Mount Kit for the Cisco Unified IP Phone* document.

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

Procedure

Step 1 Remove the footstand if it is attached to the phone.

Step 2 Insert two screws into a wall stud, matching them to the two screw holes on the back of the phone.

The keyholes fit standard phone jack mounts.

Step 3 Hang the phone on the wall.

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 these steps.

1. These buttons blink or flash on and off:
   - Handset light strip
   - Hold button
   - Applications Menu button
2. The screen displays the Cisco Systems, Inc., logo screen.
3. These messages appear as the phone starts:
   - Configuring IP
   - Updating CTL
   - Verifying Load
   - Configuring CM List
   - Registering
4. The main LCD screen displays:
   - Current date and time
   - Directory number
   - 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

- Domain name
- DNS server IP address
- TFTP server IP address

Collect this information and see the instructions in Chapter 4, "Configuring Settings on the Cisco Unified IP Phone."

Configuring Security on the Cisco Unified IP Phone

The security features protect against several threats, including threats to the identity of the phone and to data. These features establish and maintain authenticated communication streams between the phone and the Cisco Unified 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 1-10. 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 install an LSC from the Security Configuration menu on the phone. This menu also lets you update or remove an LSC.

Before You Begin

Make sure that the appropriate Cisco Unified 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 C:\Program Files\Cisco\Certificates 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, press the **Applications Menu** button and choose **Settings > Model Information**.

See the *Cisco Unified CallManager Security Guide* for more information.

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

Procedure

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

Step 2 From the phone, press the **Applications Menu** button and 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 *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 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 pressing the **Applications Menu** button, then choosing **Settings > Model Information**, and ensuring that the LSC setting shows Installed.

Related Topic

- Understanding Security Features for Cisco Unified IP Phones, page 1-10

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 Phones 7906G and 7911G, 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

Configuration Menus on the Cisco Unified IP Phones 7906G and 7911G

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.

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 4-3 for instructions.

For information about the keys you can use to edit or change option settings, see the "Editing the Values of an Option Setting" 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 *Cisco Unified CallManager Administration Guide* for more information.

Related Topics

- Unlocking and Locking Options, page 4-3
- Editing the Values of an Option Setting, 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 these steps.

Note You can control whether a phone has access to the Settings menu or to options on this menu by using the Settings Access field in the Cisco Unified 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 *Cisco Unified CallManager Administration Guide*.

Procedure

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

Step 2 Choose **Settings > Network Configuration** or **Device Configuration**.

Step 3 Perform one of these actions to display the Network Configuration menu or the Device Configuration 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. To return to the Applications menu, press the **Applications Menu** button one or more times.

Related Topics

- Unlocking and Locking Options, page 4-3
- Editing the Values of an Option Setting, 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, as shown next.

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

After you have made your changes, you must lock the options.

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 the Values of an Option Setting, 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 the Values of an Option Setting

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 9-15.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Unlocking and Locking Options, page 4-3
- 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 and the or the "Device Configuration Menu" section on page 4-15.

Table 4-1 Network Configuration Menu Settings

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	Allow you to change the administrative VLAN used by the phone.	Admin. VLAN ID
		PC VLAN (applies to 7911G only)
Port settings	Allow you to set the speed and duplex of the network and access ports.	SW Port Configuration
		PC Port Configuration (applies to 7911G only)

Related Topics

- Displaying a Configuration Menu, page 4-2
- Unlocking and Locking Options, page 4-3
- Editing the Values of an Option Setting, 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 4-3. 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 the Values of an Option Setting" 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 on 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 *Cisco Unified CallManager Security Guide*. For information about unlocking the CTL file, see the "CTL File Screen" section on page 7-3.	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 *Cisco Unified CallManager Security Guide*. For information about unlocking the CTL file, see to the "CTL File Screen" section on page 7-3.	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). 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 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 (applies to 7911G only).	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 (applies to 7911G only)	Speed and duplex of the access port (labeled 10/100 PC). 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 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 (applies to 7911G only)	Allows the phone to work better with non-Cisco switches. Strips the 802.1P/Q tags from the packets going to a PC from the access port on the phone. The Admin. VLAN ID must be set before you can change this option.	1. Unlock network configuration options. 2. Make sure the Admin. VLAN ID option is set. 3. Scroll to the **PC VLAN** option, press the **Edit** softkey, and then enter a new PC VLAN setting. 4. Press the **Validate** softkey and then press the **Save** softkey.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Unlocking and Locking Options, page 4-3
- Editing the Values of an Option Setting, 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 submenus 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 4-18
- Locale Configuration Menu, page 4-19
- Media Configuration Menu, page 4-20
- Ethernet Configuration Menu, page 4-21
- Security Configuration Menu, page 4-21
- QoS Configuration Menu, page 4-23
- Network Configuration, page 4-24

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 states shown in Table 4-3.

Table 4-3 Cisco Unified CallManager Server States

State	Description
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 designations or icons shown in Table 4-4.

Table 4-4 Cisco Unified CallManager Server Designations

Designation	Description
SRST	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	Indicates that the phone was unable to register with a Cisco Unified CallManager listed in its configuration file and that it registered with the TFTP server instead.
 (Authentication icon)	Indicates that the connection to the Cisco Unified CallManager is authenticated. For more information about authentication, refer to *Cisco Unified CallManager Security Guide*.
 (Encryption icon)	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 4-5 describes the HTTP Configuration menu options.

Table 4-5 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 to modify.
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.	Use Cisco Unified CallManager Administration to modify.
Messages URL	URL of the server from which the phone obtains message services.	Use Cisco Unified CallManager Administration to modify.
Information URL	URL of the help text that appears on the phone.	Use Cisco Unified CallManager Administration to modify.
Authentication URL	URL that the phone uses to validate requests made to the phone web server.	Use Cisco Unified CallManager Administration to modify.
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.

Table 4-5 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 to modify.
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.

Locale Configuration Menu

The Locale Configuration menu displays information about the user locale and the network locale used by the phone. Table 4-6 describes the options on this menu.

Table 4-6 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 to modify.
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 4-6 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 to modify.
Network Locale Version	Version of the network locale loaded on the phone.	Display only—cannot configure.

UI Configuration Menu

The UI Configuration menu displays whether the group listen function is enabled. Use Cisco Unified CallManager Administration to modify.

Table 4-7 UI Configuration Menu Options

Option	Description	To Change
Group Listen, Enabled/Disabled	Indicates whether the group listen feature is enabled or disabled.	Use Cisco Unified CallManager Administration to modify.

Media Configuration Menu

The Media Configuration menu displays whether the speaker capability is enabled. Use Cisco Unified CallManager Administration to modify.

Table 4-8 Media Configuration Menu Options

Option	Description	To Change
Speaker Enabled	Indicates whether the speaker is enabled for monitoring calls on the phone.	Use Cisco Unified CallManager Administration to modify.

Ethernet Configuration Menu

The Ethernet Configuration menu displays whether the Span to PC Port option is enabled on the phone (Cisco Unified IP Phone 7911G only). Table 4-9 describes the option.

Table 4-9 Ethernet Configuration Menu Option

Option	Description	To Change
Span to PC Port (applies to 7911G only)	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 to modify.

Security Configuration Menu

The Security Configuration menu displays settings that relate to security for phone.

You can view additional security information and unlock the CTL file from the Security Configuration screen on a phone. For more information, see the "Security Configuration Menu" section on page 7-2.

Table 4-10 describes the Security Configuration menu options.

Table 4-10 Security Configuration Menu Options

Option	Description	To Change
PC Port Disabled (applies to 7911G only)	Indicates whether the access port on the phone is enabled (No) or disabled (Yes).	Use Cisco Unified CallManager Administration to modify.
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous 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 to modify.
Voice VLAN Enabled (applies to 7911G only)	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 to modify.
Web Access Enabled	Indicates whether web access is enabled (Yes) or disabled (No) for the phone.	Use Cisco Unified CallManager Administration to modify.

Table 4-10 Security Configuration Menu Options (continued)

Option	Description	To Change
Security Mode	Displays the security mode that is set for the phone.	Use Cisco Unified CallManager Administration to modify.
Logging Display	Used by Cisco Technical Assistance Center (TAC) for troubleshooting. The Cisco Unified IP Phone 7911G can be configured for Enabled/Disabled/PC Controlled The Cisco Unified IP Phone 7906G supports only Enabled/Disabled (no PC Controlled)	—

QoS Configuration Menu

The QoS Configuration menu displays information that relates to quality of service (QoS) for the phone. Table 4-11 describes the QoS Configuration menu options.

Table 4-11 QoS Configuration Menu Options

Option	Description	To Change
DSCP For Services	DSCP IP classification for phone-based services.	Use Cisco Unified CallManager Administration to modify.
DSCP For Configuration	DSCP IP classification for any phone configuration transfer.	Use Cisco Unified CallManager Administration to modify.
DSCP For Call Control	DSCP IP classification for call control signaling.	Use Cisco Unified CallManager Administration to modify.

Related Topics

- Displaying a Configuration Menu, page 4-2
- Network Configuration Menu, page 4-7

Network Configuration

The Network Configuration menu contains the Load Server option. The Load Server option is used to optimize installation time for phone firmware upgrades. 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 upgrades on the phones. When the Load Server option is set, the phone contacts the designated server for the firmware upgrade.

Note Even if a Load Server is configured, the phone continues to use TFTP Server 1 or TFTP Server 2 for obtaining configuration files.

To configure the Load Server option, use the Cisco Unified CallManager Administration Phone Configuration page, Product Specific Configuration section.

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 communications 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."

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 Phone, page 5-2
- Configuring Corporate and Personal Directories, page 5-13
- Modifying Phone Button Templates, page 5-14
- Configuring Softkey Templates, page 5-14
- Setting Up Services, page 5-15
- Adding Users to Cisco Unified CallManager, page 5-16
- Specifying Options that Appear on the User Options Web Pages, page 5-17

Telephony Features Available for the 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 Configuration Reference column lists Cisco Unified CallManager documentation that contains configuration procedures and related information.

For more information about using most of these features on the phone, refer to the *Cisco Unified IP Phones 7906G and 7911G Guide*.

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 the *Cisco Unified CallManager Administration Guide*.

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

Feature	Description	Configuration Reference
Abbreviated dialing	A user can configure up to 99 speed-dial entries. Speed-dial entries that are not assigned to the speed-dial buttons on the phone are used for abbreviated dialing. When a user starts dialing digits, the **AbbrDial** softkey appears, and the user can access any speed-dial entry by entering the appropriate index.	For more information, refer to the: • *Cisco Unified CallManager Administration Guide,* Cisco Unified IP Phone Configuration chapter • *Cisco Unified CallManager System Guide,* Cisco Unified IP Phones chapter
Auto answer	Causes the speakerphone to go off hook automatically when an incoming call is received. The user can monitor the call using the speaker but must pick up the handset to speak to the caller.	For more information, refer to the *Cisco Unified CallManager Administration Guide,* Configuring Directory Numbers chapter.

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

Feature	Description	Configuration Reference
Barge	Allows a user to join an in-progress call on a shared line. 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 the: • *Cisco Unified CallManager Administration Guide,* Cisco Unified IP Phone Configuration chapter • *Cisco Unified CallManager System Guide,* Cisco Unified IP Phones chapter • *Cisco Unified CallManager Features and Services Guide,* Barge and Privacy chapter
Block external to external transfer	Prevents users from transferring an external call to another external number.	For more information, refer to the *Cisco Unified CallManager Features and Services Guide*, External Call Transfer Restrictions 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 the: • *Cisco Unified CallManager Administration Guide*, Cisco Unified IP Phone Configuration chapter • *Cisco Unified CallManager System Guide,* Understanding Route Plans chapter • *Cisco Unified CallManager Features and Services Guide,* Call Display Restrictions chapter

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

Feature	Description	Configuration Reference
Call forward	Forwards all calls to the designated directory number.	For more information, refer to the: • *Cisco Unified CallManager Administration Guide,* Configuring Directory Numbers chapter • *Cisco Unified CallManager System Guide,* Cisco Unified IP Phones chapter • *Cisco Unified CallManager Features and Services Guide,* Multilevel Precedence and Preemption chapter
Call park	Places the call on hold so that anyone connected to the Cisco Unified CallManager system can retrieve the call.	For more information, refer to the: • *Cisco Unified CallManager Administration Guide,* Feature Configuration chapter • *Cisco Unified CallManager System Guide,* Cisco Unified IP Phones chapter • *Cisco Unified CallManager Features and Services Guide*, 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 the: • *Cisco Unified CallManager Administration Guide,* Pickup Group Configuration chapter • *Cisco Unified CallManager System Guide*, Call Pickup chapter

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

Feature	Description	Configuration Reference
Call waiting	Receives a second incoming call on the same line without disconnecting the first call.	For more information, refer to the: • *Cisco Unified CallManager Administration Guide*, Cisco Unified IP Phone Configuration chapter • *Cisco Unified CallManager System Guide*, Cisco Unified IP Phones chapter • *Cisco Unified CallManager Features and Services Guide*, Multilevel Precedence and Preemption chapter
Caller ID	Displays the telephone number and name of the caller.	For more information, refer to the: • *Cisco Unified CallManager Administration Guide,* Configuring Cisco Unified IP Phones chapter • *Cisco Unified CallManager System Guide,* Understanding Route Plans chapter • *Cisco Unified CallManager Features and Services Guide*, Call Display Restrictions chapter
Cisco Call Back	Allows a user to receive call back notification on a Cisco Unified IP Phone when a called party's line becomes available.	For more information, refer to the: • *Cisco Unified CallManager System Guide,* Cisco Unified IP Phones chapter • *Cisco Unified CallManager Features and Services Guide*, Cisco Call Back chapter

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

Feature	Description	Configuration Reference
Client matter codes (CMC)	Enables a user to specify that a call relates to a specific client matter.	For more information, refer to the: • *Cisco Unified CallManager Administration Guide,* Client Matter Codes chapter • *Cisco Unified CallManager Features and Services Guide,* Client Matter Codes and Forced Authorization Codes chapter
Conference	Initiates an ad hoc conference and then conferences in other participants one at a time.	For more information, refer to the: *Cisco Unified CallManager System Guide*, Cisco Unified IP Phones chapter.
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 the: • *Cisco Unified CallManager Administration Guide,* Cisco Unified IP Phone Configuration chapter • *Cisco Unified CallManager System Guide*, Cisco Unified IP Phones chapter
Direct transfer	Joins two established calls (calls that are on hold or in connected state) into one call and drops the feature initiator from the call. Does not initiate a consultation call and does not put the active call on hold.	For more information, refer to the *Cisco Unified CallManager System Guide*, Cisco Unified IP Phones chapter.

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

Feature	Description	Configuration Reference
Extension Mobility	Enables users to sign into their directory number from any Cisco Unified IP Phone.	For more information, refer to the: • *Cisco Unified CallManager Features and Services Guide,* Cisco Unified CallManager Extension Mobility chapter • *Cisco Unified CallManager System Guide*, Cisco Unified CallManager Extension Mobility and Phone Login Features chapter
Forced authorization codes (FAC)	Controls the types of calls that certain users can place.	For more information, refer to the: • *Cisco Unified CallManager System Guide*, Forced Authorization Codes (FAC) chapter • *Cisco Unified CallManager Features and Services Guide,* Client Matter Codes and Forced Authorization Codes chapter
Group call pickup	Allows users to pick up incoming calls within their own group or in other groups.	For more information, refer to the: • *Cisco Unified CallManager Administration Guide,* Pickup Group Configuration chapter • *Cisco Unified CallManager System Guide,* Call Pickup chapter
Hold	Places an active call on hold.	Requires no configuration, unless you want to use music on hold; see "Music-on-Hold" in this table for information.

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

Feature	Description	Configuration Reference
Immediate Divert	Immediately diverts a call to a voice messaging system. When a call is diverted, the line becomes available to make or receive new calls.	For more information, refer to the: • *Cisco Unified CallManager System Guide,* Cisco Unified IP Phones chapter • *Cisco Unified CallManager Features and Services Guide*, Immediate Divert chapter
Join	Allows a user to initiate an ad hoc conference by using the **Join** softkey. Join does not create a consultation call and does not put the active call on hold. Join can include more than two calls, which results in a call with more than three parties.	For more information, refer to the *Cisco Unified CallManager System Guide,* Cisco Unified IP Phones chapter
Malicious caller identification (MCID)	Allows you to report a call of a malicious nature by requesting that Cisco Unified CallManager identify and register the source of an incoming call in the network.	For more information refer to the: • *Cisco Unified CallManager System Guide,* Cisco Unified IP Phones chapter • *Cisco Unified CallManager Features and Services Guide,* Malicious Call Identification chapter
Meet-Me conference	Enables other callers to join in a conference.	For more information refer to the *Cisco Unified CallManager Administration Guide*, Meet-Me Number/Pattern Configuration chapter

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

Feature	Description	Configuration Reference
Message waiting	Indicates that one or more voice messages are waiting for a user.	For more information refer to the: • *Cisco Unified CallManager Administration Guide,* Message Waiting Configuration chapter • *Cisco Unified CallManager System Guide*, Voice Mail Connectivity to Cisco Unified CallManager chapter
Multilevel Precedence and Preemption (MLPP)	Allows properly validated users to place priority calls. If necessary, users can preempt lower-priority phone calls. Also allows the use of the call-forward alternate party (CFAP) feature for forwarding a precedence call.	For more information refer to the *Cisco Unified CallManager Features and Services Guide,* Multilevel Precedence and Preemption chapter.
Music-on-hold	Plays music while callers are on hold.	For more information refer to the: • *Cisco Unified CallManager Administration Guide*, Music On Hold Audio Source Configuration and Music On Hold Server Configuration chapters • *Cisco Unified CallManager System Guide*, Music on Hold chapter • *Cisco Unified CallManager Features and Services Guide*, Music On Hold chapter.

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

Feature	Description	Configuration Reference
Privacy	Enables or disables whether users with phones that share the same line can view call status and can barge a call.	For more information: • See the "Modifying Phone Button Templates" section on page 5-14 • Refer to the *Cisco Unified CallManager System Guide,* Cisco Unified IP Phones 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 the: • *Cisco Unified CallManager System Guide,* Cisco Unified IP Phones chapter • *Cisco Unified CallManager Features and Services Guide,* Quality Report Tool chapter
Redial	Redials the last number dialed on the Cisco Unified IP Phone.	Requires no configuration.
Ring setting	Identifies ring type used for a line when a phone has another active call	For more information refer to the: • *Cisco Unified CallManager Administration Guide*, Configuring Directory Numbers chapter • *Cisco Unified CallManager Features and Services Guide,* Custom Phone Rings chapter

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

Feature	Description	Configuration Reference
Services	Allows you to use the Cisco Unified IP Phone Services Configuration menu in Cisco Unified CallManager Administration to define and maintain the list of phone services to which users can subscribe.	For more information refer to the: • *Cisco Unified CallManager Administration Guide,* Cisco Unified IP Phone Configuration chapter • *Cisco Unified CallManager System Guide,* Cisco Unified IP Phone Services chapter
Speed-dial	Dials a specified number that has been previously stored.	For more information refer to the: • *Cisco Unified CallManager Administration Guide,* Cisco Unified IP Phone Configuration chapter • *Cisco Unified CallManager System Guide,* Cisco Unified IP Phones chapter
Time-of-Day Routing	Restricts access to specified telephony features by time period.	For more information refer to the: • *Cisco Unified CallManager Administration Guide,* Time Period Configuration chapter • *Cisco Unified CallManager System Guide,* Time-of-Day Routing chapter
Transfer	Transfers an active call to another directory number.	Requires no configuration.

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

Feature	Description	Configuration Reference
Voice messaging system	Enables callers to leave voice messages if calls are unanswered.	For more information refer to the: • *Cisco Unified CallManager Administration Guide,* Cisco Voice-Mail Port Configuration chapter • *Cisco Unified CallManager System Guide*, Voice Mail Connectivity to Cisco Unified CallManager chapter
Video mode (7911 only)	Allows a user to select the video display mode for viewing a video conference, depending on the modes configured in the system.	For more information: • See the "Configuring Softkey Templates" section on page 5-14. • *Cisco Unified CallManager Administration Guide*, "Conference Bridge Configuration" chapter. • *Cisco Unified CallManager System Guide*, "Understanding Video Telephony" chapter.
Video support (7911 only)	Enable video support on the phone.	For more information refer to: • *Cisco Unified CallManager Administration Guide*, "Conference Bridge Configuration" chapter. • *Cisco Unified CallManager System Guide,* "Understanding Video Telephony" chapter. • *Cisco VT Advantage Administration Guide*, "Overview of Cisco VT Advantage" chapter.

Configuring Corporate and Personal Directories

The **Directories** menu on the Cisco Unified IP Phones 7906G and 7911G 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 5-13 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 5-13 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 a user's right to access the system. Authorization identifies the telephony resources that a user is permitted to use, such as a specific telephone extension.

After the LDAP directory configuration completes, users can use the Corporate Directory service on your Cisco Unified IP Phone 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 Synchronizer utility

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

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

Modifying Phone Button Templates

Phone button templates let you assign features to phone buttons. On the Cisco Unified IP Phones 7906G and 7911G, only the Privacy feature (Private softkey) can be configured on the template.

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 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 *Cisco Unified CallManager Administration Guide* and *Cisco Unified CallManager System Guide* for more information.

Configuring Softkey Templates

Using Cisco Unified CallManager Administration, you can manage softkeys associated with applications that are supported by the Cisco Unified IP Phones 7906G and 7911G. Cisco Unified CallManager supports two types of softkey templates: standard and nonstandard. Standard softkey templates include Standard User and Standard Feature. 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 *Cisco Unified CallManager Administration Guide*, *Cisco Unified CallManager System Guide* for more information.

Setting Up Services

The **Services** button on the Cisco Unified IP Phone gives users access to Cisco Unified IP Phone Services. These services comprise XML applications that enable the display of interactive content with text and graphics on the phone. Examples of services include local movie times, stock quotes, and weather reports.

Before a user can access any service,

- You must use Cisco Unified CallManager Administration to configure available services.
- The user must subscribe to services using the Cisco Unified IP Phone 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 **Feature > Cisco Unified IP Phone Services** from Cisco Unified CallManager Administration. Refer to *Cisco Unified CallManager Administration Guide* and *Cisco Unified CallManager System Guide* for more information.

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

Adding Users to Cisco Unified CallManager

Adding users to Cisco Unified CallManager allows you to display and maintain information about users such as their directory information and passwords.

Users added to Cisco Unified CallManager can perform these actions:

- 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 > Add a New User** from Cisco Unified CallManager Administration.

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

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

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

Specifying Options that Appear on 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 *Customizing Your Cisco Unified IP Phone on the Web*.)

All options on the User Options web pages appear by default. However, you can disable options by making appropriate enterprise parameter settings using Cisco Unified CallManager Administration.

The settings you make affect all User Options web pages at your site.

Customizing the Cisco Unified IP Phone

This chapter describes how you can customize phone ring sounds and background images at your site. Ring sounds play when the phone receives a call. Background images appear on the phone screen.

This chapter includes these topics:

- Creating Custom Phone Rings, page 6-1
- Creating Custom Background Images, page 6-4

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.

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

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

RingList.xml File Format Requirements

The RingList.xml file defines an XML object that contains a list of phone ring types. This file can include up to 50 ring types. Each ring type contains a pointer to the PCM file that is used for that ring type and the text that will appear on the Ring Type menu on a Cisco Unified IP Phone for that ring. The C:\Program Files\Cisco\TFTPPath directory of 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 these requirements for proper playback on Cisco Unified IP Phones:

- Raw PCM (no header)
- 8000 samples per second
- 8 bits per sample
- µLaw 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 Phones 7906G and 7911G, 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 Place the new PCM files that you created in the C:\Program Files\Cisco\TFTPPath directory on the Cisco TFTP server for each Cisco Unified CallManager in your cluster.

Step 3 Use an 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 pressing the **Applications Menu** button and choosing **Settings > User Preferences > Background Images** on the phone.

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

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

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

List.xml File Format Requirements

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

C:\Program Files\Cisco\TFTPPath\Desktops\95x34x1

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

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>
- <!--
 Please Add Images to the end of the list
-->
<ImageItem Image="TFTP:Desktops/95x34x1/TN-Mountain.png"
URL="TFTP:Desktops/95x34x1/Mountain.png" />
<ImageItem Image="TFTP:Desktops/95x34x1/TN-Ocean.png"
URL="TFTP:Desktops/95x34x1/Ocean.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—95 pixels (width) X 34 pixels (height).
- Thumbnail image—23 pixels (width) X 8 pixels (height).
- Color palette—For best results, set to monochrome (1-bit) when you create a PNG file.

Configuring a Custom Background Image

To configure 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 Place the new PNG files that you created in the following folder on the TFTP server for each Cisco Unified CallManager in the cluster:

C:\Program Files\Cisco\TFTPPath\Desktops\95x34x1

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 6-4 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 your 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.

Viewing Security Information, 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 Phones 7906G and 7911G to view model information, status messages, network statistics, and firmware information for the phone:

- Security Configuration screen—Displays information about security on the phone.
- Model Information screen—Displays hardware and software information about the phone.
- Status menu—Provides access to screens that display the status messages, network statistics, and firmware versions.

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 Phones 7906G and 7911G, see Chapter 9, "Troubleshooting and Maintenance."

This chapter includes these topics:

- Security Configuration Menu, page 7-2
- Model Information Screen, page 7-6
- Status Menu, page 7-7

Security Configuration Menu

The Security Configuration menu displays information about security settings on the phone and provides access to the certificate trust list (CTL) file screen and the trust list screen.

To display the Security Configuration menu, follow these steps:

Procedure

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

Step 2 Select **Settings > Security Configuration**.

The Security Configuration menu provides these options:

- Web Access Enabled—Displays whether web access is enabled (Yes) or disabled (No) for the phone. You configure web access in Cisco Unified CallManager Administration.
- Security Mode—Displays the security mode that is set for the phone. You configure the security mode in Cisco Unified CallManager Administration.
- 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).
- 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).

- 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 *Cisco Unified CallManager Security Guide*.)

  If a CTL file is installed on the phone, also provides access to the CTL File screen. For more information, see the "CTL File Screen" section on page 7-3.
- Trust List—If a CTL file is installed on the phone, provides access to the Trust List screen. For more information, see the "Trust List Screen" section on page 7-5.
- CAPF Server—Displays the IP address and the port of the CAPF that the phone uses.
- Logging Display—Used only by Cisco Technical Assistance Center (TAC) for troubleshooting.

Note To exit any menu or screen, press the **Exit** softkey.

CTL File Screen

The CTL File screen displays information about the certificate trust list (CTL) file that is installed in the phone and provides access to the CTL File screen. 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 *Cisco Unified CallManager Security Guide*.

To display the CTL File screen, follow these steps:

Procedure

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

Step 2 Select **Settings > Security Configuration**.

Step 3 Select **CTL File.**

Table 7-1 provides a list of the CTL File items and a description of each.

Table 7-1 CTL File Information

Item	Description
CTL File	Displays the MD5 hash of the certificate trust list (CTL) file that is installed in the phone. 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.
CAPF Server	IP address of the CAPF server used by the phone. Also displays a certificate icon if a certificate is installed for this server.
CallManager / TFPT 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.

To add or change the primary CallManager / TFTP server (TFTP Server 1) or secondary (TFTP Server 2) in the CTL File, you must unlock the CTL file before you can save changes. You must use the Network Configuration menu to make changes to the TFTP Server 1 option or to the TFTP Server 2 option. (For information about changing these options, see the "Network Configuration Menu" section on page 4-7.)

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

Procedure

Step 1 Press ****#** to unlock options on the CTL File menu.

If you decide not to continue, press ****#** again to lock options on this menu.

Step 2 Highlight the CTL 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 screen displays information about all of the servers that the phone trusts. If a CTL file is installed on the phone, you can view the trust list.

To access the Trust List screen, follow these steps:

Procedure

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

Step 2 Select **Settings > Security Configuration**.

Step 3 Select **Trust List**.

Table 7-2 provides a list of the Trust List items and a description of each.

Table 7-2 Trust List Information

Item	Description
CAPF Server	IP address of the CAPF used by the phone. Also displays a certificate icon if a certificate is installed for this server.
CallManager / TFPT 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.
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.

Model Information Screen

The Model Information screen displays specific information about the IP phone. To display the Model Information screen, follow these steps:

Procedure

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

Step 2 Select **Settings > Model Information**.

Table 7-3 provides a list of Model Information items and a description of each.

Table 7-3 Model Information

Item	Description
Model Number	Model number of the phone
MAC Address	MAC address of the phone
Load File	Identifier of the factory-installed load running on the phone
Boot Load ID	Identifier of the factory-installed load running on the phone
Serial Number	Serial number of the phone
CTL	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 *Cisco Unified CallManager Security Guide*.)
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).
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)
Call Control Protocol	Displays the call control protocol for the phone, Skinny Client Control Protocol (SCCP).

Status Menu

The Status menu provides information about the phone and its operation that includes messages, statistics, and information about firmware versions on the phone and any expansion modules.

To access the Status menu, follow these steps:

Procedure

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

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

The Status menu includes the following 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 7-8.
- Network Statistics—Displays the Network Statistics screen, which shows Ethernet traffic statistics. For more information, see the "Network Statistics Screen" section on page 7-16.
- 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 7-19.

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 7-4 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 **Applications Menu** button.

Step 2 Select **Settings**.

Step 3 **Status**.

Step 4 Select **Status Messages**.

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

Table 7-4 provides a list of the Status Messages with their description and explanation.

Table 7-4 Status Messages on the Cisco Unified IP Phones 7906G and 7911G

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.
Error Verifying Config Info	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 `CFG File Not Found` 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 2-14 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.

Table 7-4 Status Messages on the Cisco Unified IP Phones 7906G and 7911G (continued)

Message	Description	Possible Explanation and Action
Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firmware and place it in the TFTPPath directory. You should only copy files into this directory when the TFTP server software is shut down, otherwise the files may be corrupted.
CTL 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 *Cisco Unified CallManager Security Guide*.
CTL update failed	The phone could not update its certificate trust list (CTL) file.	Problem with the CTL file on the TFTP server. For more information, refer to *Cisco Unified CallManager Security Guide*.
DHCP timeout	DHCP server did not respond.	• Network is busy—The errors should resolve themselves when the network load reduces. • No network connectivity between the DHCP server and the phone—Verify the network connections. • DHCP server is down—Check configuration of DHCP server. • Errors persist—Consider assigning a static IP address. See the "Network Configuration Menu" section on page 4-7 for details on assigning a static IP address.

Table 7-4 Status Messages on the Cisco Unified IP Phones 7906G and 7911G (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.
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: – g3-tones.xml • Located in subdirectory with same name as user locale: – glyphs.xml – SCCP-dictionary.xml – kate.xml

Table 7-4 Status Messages on the Cisco Unified IP Phones 7906G and 7911G (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.
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 section for details.
Load ID incorrect	Load ID of the software file is of the wrong type.	Check the load ID assigned to the phone (from Cisco Unified CallManager, choose **Device > Phone**). Verify that the load ID is entered correctly.
Load rejected HC	The application that was downloaded is not compatible with the phone's hardware.	Occurs if you were attempting to install a version of software on this phone that did not support hardware changes on this newer phone. Check the load ID assigned to the phone (from Cisco Unified CallManager, choose **Device > Phone**). Re-enter the load displayed on the phone. See the "Firmware Versions Screen" section on page 7-19 to verify the phone setting.

Table 7-4 Status Messages on the Cisco Unified IP Phones 7906G and 7911G (continued)

Message	Description	Possible Explanation and Action
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.
No CTL installed	A 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 *Cisco Unified CallManager Security Guide*.
Programming Error	The phone failed during programming.	Attempt to resolve this error by power cycling the phone. If the problem persists, contact Cisco technical support for additional assistance.

Table 7-4 Status Messages on the Cisco Unified IP Phones 7906G and 7911G (continued)

Message	Description	Possible Explanation and Action
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.
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.

Table 7-4 Status Messages on the Cisco Unified IP Phones 7906G and 7911G (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.

Network Statistics Screen

The Network Statistics screen displays information about the phone and network performance.

To display the Network Statistics screen, follow these steps:

Procedure

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

Step 2 Select **Settings**.

Step 3 Select **Status**.

Step 4 Select **Network Statistics**.

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

Table 7-5 provides a list of Network Statistics items and a description of each.

Table 7-5 Network Statistics Screen

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 7-5 Network Statistics Screen (continued)

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 connected to Cisco Unified CallManager
Port 1	Link state and connection of the Network port
Port 2 (applies to 7911G only)	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)

Firmware Versions Screen

The Firmware Versions screen displays information about the firmware version running on the phone.

To display the Firmware Version screen, follow these steps:

Procedure

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

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

Step 3 Select **Firmware Versions**.

Table 7-6 provides a list of Firmware Version items and a description of each.

Table 7-6 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 DSP load file running on the phone.

Monitoring the Cisco Unified IP Phone Remotely

To allow system administrators to remotely monitor the operation of a phone, each Cisco Unified IP Phone has a web page from which you can view a variety of information about the phone. You can use the following to assist you with troubleshooting a phone:

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

You can also obtain much of this information directly from a phone. For more information, see Chapter 7, "Viewing Security Information, Model Information, Status, and Statistics on the Cisco Unified IP Phone."

For more information about troubleshooting the Cisco Unified IP Phones 7906G and 7911G, see Chapter 9, "Troubleshooting and Maintenance."

This chapter includes these topics:

- Accessing the Web Page for a Phone, page 8-2
- Disabling Web Page Access, page 8-3
- Device Information, page 8-4
- Network Configuration, page 8-7
- Network Statistics, page 8-12

- Device Logs, page 8-15
- Streaming Statistics, page 8-16

Accessing the Web Page for a Phone

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

Note If you cannot access the web page, it may be disabled. See the "Disabling 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 at the top of the Phone Configuration web page.
- On the 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 Cisco Unified IP Phone includes these hyperlinks:

- **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 8-7.

- **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 8-12.
  - **Access**—Displays information about network traffic to and from the PC port on the phone. For more information, see the "Network Statistics" section on page 8-12.
  - **Network**—Displays information about network traffic to and from the network port on the phone. For more information, see the "Network Statistics" section on page 8-12.
- **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 8-15.
  - **Core Dumps**—Includes hyperlinks to individual dump files.
  - **Status Messages**—Displays up to the 10 most recent status messages that the phone has generated since it was last powered up. For more information, see the "Device Logs" section on page 8-15.
  - **Debug Display**—Displays messages that might be useful to the Cisco TAC if you require assistance with troubleshooting. For more information, see the "Device Logs" section on page 8-15.
- **Streaming Statistics**—Includes the **Stream 1**, **Stream 2**, and **Stream 3** hyperlinks, which display a variety of streaming statistics. For more information, see the "Streaming Statistics" section on page 8-16.

Disabling 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 phone's 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 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, refer to the preceding steps about disabling access. Follow these same steps, but choose **Enabled** in Step 4.

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	Host name that the DHCP server assigned to the phone
Phone DN	Directory number assigned to the phone

Table 8-1 Device Information Area Items (continued)

Item	Description
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
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

Table 8-1 Device Information Area Items (continued)

Item	Description
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: – Cisco Unified IP Phone 7970G, Global – Cisco Unified IP Phone 7971G-GE, Global, Gig Ethernet – Cisco Unified IP Phone 7961 – Cisco Unified IP Phone 7961G-GE, Global, Gig Ethernet – Cisco Unified IP Phone 7941 – Cisco Unified IP Phone 7941G-GE, Global, Gig Ethernet – Cisco Unified IP Phone 7911G – Cisco Unified IP Phone 7931G • Device Model—specifies the phone model • Device Version Identifier—represents the hardware version of the phone • Device 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

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.

Table 8-2 Network Configuration Area Items (continued)

Item	Description
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.
IP Address	Internet Protocol (IP) address of the phone.
Subnet Mask	Subnet mask used by the phone.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone.
Default Router 1–5	Default router used by the phone (Default Router 1) and optional backup routers (Default Router 2–5.
DNS Server 1–5	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) used by the phone.
Operational VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member.
Admin. VLAN ID	Auxiliary VLAN in which the phone is a member.

Table 8-2 Network Configuration Area Items (continued)

Item	Description
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 option may also include the Survivable Remote Site Telephony (SRST) designation, which indicates 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.
Messages URL	URL of the server from which the phone obtains message services.

Table 8-2 Network Configuration Area Items (continued)

Item	Description
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 • No Link—No connection to the switch port

Table 8-2 Network Configuration Area Items (continued)

Item	Description
PC Port Configuration (applies to 7911G only)	Speed and duplex of the switch port, where: • A—Auto Negotiate • 10H—10-BaseT/half duplex • 10F—10-BaseT/full duplex • 100H—100-BaseT/half duplex • 100F—100-BaseT/full duplex • No Link—No connection to the PC port
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.
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 (applies to 7911G only)	Indicates whether the PC port on the phone is enabled or disabled.
Speaker Enabled	Indicates whether the speakerphone is enabled on the phone.
Group Listen	Enables both the handset and speaker to be active at the same time, so that one user can talk into the handset while other users listen over the speaker.
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.

Table 8-2 Network Configuration Area Items (continued)

Item	Description
Voice VLAN Enabled (applies to 7911G only)	Indicates whether the phone allows a device attached to the PC port to access the Voice VLAN.
Auto Line Select Enabled	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 (applies to 7911G only)	Indicates whether the phone will forward packets transmitted and received on the network port to the access port.
PC VLAN (applies to 7911G only)	VLAN used to identify and remove 802.1P/Q tags from packets sent to the PC

Network Statistics

These network statistics areas on a phone's web page provide information about network traffic on the phone:

- Ethernet Information area—Displays information about Ethernet traffic. Table 8-3 describes the items in this area.
- Access area—Displays information about network traffic to and from the PC port on the phone. Table 8-4 describes the items in this area.
- Network area—Displays information about network traffic to and from the network port on the phone. Table 8-4 describes the items in this area.

To display a network statistics area, access the web page for the phone as described in the "Accessing the Web Page for a Phone" section on page 8-2, and then click the **Ethernet Information**, the **Access**, and or the **Network** hyperlink.

Table 8-3 Ethernet Information Area 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 Area Items

Item	Description
Rx totalPkt	Total number of packets received by the phone
Rx crcErr	Total number of packets received with CRC failed
Rx alignErr	Total number of packets received between 64 and 1522 bytes in length that have a bad 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

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

Item	Description
Rx shortErr	Total number of FCS error packets or Align error packets received that are less than 64 bytes in size
Rx shortGood	Total number of good packets received that are less than 64 bytes size
Rx longGood	Total number of good packets received that are greater than 1522 bytes in size
Rx longErr	Total number of FCS error packets or Align error packets received that are greater than 1522 bytes in size
Rx size64	Total number of packets received, including bad packets, that are between 0 and 64 bytes in size
Rx size65to127	Total number of packets received, including bad packets, that are between 65 and 127 bytes in size
Rx size128to255	Total number of packets received, including bad packets, that are between 128 and 255 bytes in size
Rx size256to511	Total number of packets received, including bad packets, that are between 256 and 511 bytes in size
Rx size512to1023	Total number of packets received, including bad packets, that are between 512 and 1023 bytes in size
Rx size1024to1518	Total number of packets received, including bad packets, that are between 1024 and 1518 bytes in size
Rx tokenDrop	Total number of packets dropped due to lack of resources (for example, FIFO overflow)
Tx excessDefer	Total number of packets delayed from transmitting due to medium being busy
Tx lateCollision	Number of times that collisions occurred later than 512 bit times after the start of packet transmission
Tx totalGoodPkt	Total number of good packets (multicast, broadcast, and unicast) received by the phone
Tx Collisions	Total number of collisions that occurred while a packet was being transmitted

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

Item	Description
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 Device Logs area on a phone's web page provides information you can use to help monitor and troubleshoot the phone.

- 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.
- Status Messages area—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 7-4 on page 7-10 describes the status messages that can appear.

  To display the Status Messages, 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 **Status Messages** hyperlink.
- Debug Display area—Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting.

Streaming Statistics

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

Table 8-5 describes the items in the Streaming Statistics areas.

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 Streaming Statistics Area Items

Item	Description
Domain	Domain of the phone
Remote Address	IP address of the destination of the stream
Local Address	IP address of the phone
Sender Joins	Number of times the phone has started transmitting a stream
Receiver Joins	Number of times the phone has started receiving a stream
Byes	Number of times the phone has stopped transmitting a stream
Start Time	Internal time stamp indicating when Cisco Unified CallManager requested that the phone start transmitting packets
Row Status	Whether the phone is streaming
Host Name	Host name of the phone
Sender Packets	Total number of packets sent by the phone
Sender Octets	Total number of octets sent by the phone
Sender Tool	Type of audio encoding used for the stream
Sender Reports	Number of times this streaming statistics report has been accessed from the web page (resets when the phone resets)

Table 8-5 Streaming Statistics Area Items (continued)

Item	Description
Sender Report Time	Internal time stamp indicating when this streaming statistics report was generated
Sender Start Time	Time that the stream started
Rcvr Lost Packets	Total number of packets lost
Rcvr Jitter	Maximum jitter of stream
Receiver Tool	Type of audio encoding used for the stream
Rcvr Reports	Number of times this streaming statistics report has been accessed from the web page (resets when the phone resets)
Rcvr Report Time	Internal time stamp indicating when this streaming statistics report was generated
Rcvr Packets	Total number of packets received by the phone
Rcvr Octets	Total number of octets received by the phone
Rcvr Start Time	Internal time stamp indicating when Cisco Unified CallManager requested that the phone start receiving packets

Troubleshooting and Maintenance

This chapter provides information that can assist you in troubleshooting problems with your Cisco Unified IP Phone 7906G or 7911G or with your Cisco Unified Communications 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

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 9-12
- Resetting or Restoring the Cisco Unified IP Phone, page 9-15
- Using the Quality Report Tool, page 9-17
- Where to Go for More Troubleshooting Information, page 9-18
- Cleaning the Cisco Unified IP Phone, page 9-18

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 3-16. 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: 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 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 9-16.

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
- Registering the Phone with Cisco Unified CallManager, page 9-4
- Checking Network Connectivity, page 9-4
- Verifying TFTP Server Settings, page 9-5
- Verifying IP Addressing and Routing, page 9-5
- Verifying DNS Settings, page 9-6
- Verifying Cisco Unified CallManager Settings, page 9-6

- Cisco Unified CallManager and TFTP Services Are Not Running, page 9-6
- Creating a New Configuration File, page 9-7

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 7-8 for instructions about accessing status messages and for a list of potential errors, their explanations, and their solutions.

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 2-11 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 > 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 of a Cisco Unified IP Phone" section on page 2-15.

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.

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 **Applications Menu** button on the phone and then selecting **Settings > Network Configuration > TFTP Server 1**.

If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option. See the "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. Refer to *Configuring Windows 2000 DHCP Server for Cisco Unified CallManager*, available at this URL:
http://www.cisco.com/warp/customer/788/AVVID/win2000_dhcp.html

You can also enable the phone to use an alternate TFTP server. Such a setting is particularly useful if the phone was recently moved from one location to another. See the "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 **Applications Menu** button, then select **Settings > 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 *Troubleshooting Switch Port Problems*, 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 *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks*, 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 **Applications Menu** button and selecting **Settings > Network Configuration > DNS Server 1**. You should also verify that there is a CNAME entry in the DNS server for the TFTP server and for the Cisco Unified CallManager system.

You must also ensure that DNS is configured to do reverse look-ups. Windows2000 is configured by default only to perform forward look-ups.

Verifying Cisco Unified CallManager Settings

On the Cisco Unified IP Phone, press the **Applications Menu** button and select **Settings > Network Configuration > CallManager 1–5**. 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 "Registering the Phone with Cisco Unified CallManager" 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 **Application > Cisco Unified CallManager Serviceability**.

Step 2 Choose **Tools > Control Center**.

Step 3 From the Servers column, choose the primary Cisco Unified CallManager server.

The page displays the service names for the server that you chose, the status of the services, and a service control panel to stop or start a service.

Step 4 If a service has stopped, 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 2-11 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.

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 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 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 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.

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 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 same switch as 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.

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 **Applications Menu** button on the phone and choosing **Settings > Status > Network Statistics**. If the phone was recently reset one of these messages appears:

- Reset-Reset—Phone closed due to receiving a Reset/Reset from Cisco Unified 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:

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 9-15 for details.

Step 2 Modify DHCP and IP settings.

- **a.** Disable DHCP. See the "Network Configuration Menu" section on page 4-7 for instructions.
- **b.** 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.
- **c.** Assign 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. Refer to *Configuring The IP Hosts File on a Windows 2000 CallManager Server*, available at this URL:
http://www.cisco.com/warp/customer/788/AVVID/cm_hosts_file.html

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** 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 of a Cisco Unified IP Phone" section on page 2-15.

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, 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.	Invalid 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.

General Troubleshooting Tips

This section provides troubleshooting information for some common issues that might occur on the Cisco Unified IP Phone.

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.
Prolonged broadcast storms cause IP phones to re-register.	Prolonged broadcast storms (lasting several minutes) on the voice VLAN cause the IP phones to re-register with another Cisco Unified CallManager server.
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.

Table 9-2 Cisco Unified IP Phone Troubleshooting (continued)

Summary	Explanation
Changing the telephone configuration.	By default, the network configuration options are locked to prevent users from making changes that could impact their network connectivity. You must unlock the network configuration options before you can configure them. See the "Unlocking and Locking Options" section on page 4-3 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.
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.

Resetting or Restoring the Cisco Unified IP Phone

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

- Performing a Basic Reset, page 9-15
- Performing a Factory Reset, page 9-16

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 9-3 describes the ways to perform a basic reset. You can reset a phone with any of these operations any time after the phone has started up. Choose the operation that is appropriate for your situation.

Table 9-3 Basic Reset Methods

Operation	Performing	Explanation
Reset phone	From any screen (but not when the phone is idle), press **#**.	Resets any user and network configuration changes that you have made but that the phone has not written to its Flash memory to previously-saved settings, then restarts the phone.

Table 9-3 Basic Reset Methods (continued)

Operation	Performing	Explanation
Erase softkey	From the Settings menu, unlock phone options (see the "Unlocking and Locking Options" section on page 4-3). 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 4-3). The press the **Erase** softkey.	Resets network configuration settings to their default values and resets the phone. (This method causes DHCP reconfigure the IP address of the phone.)
	From the Security Configuration menu, unlock phone options (see the "Unlocking and Locking Options" section on page 4-3). 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
- 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 term11.default.loads file)

Note This phone must be on a DHCP-enabled network before you can perform these steps.

To perform a factory reset of a phone, follow these 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 **Applications Menu** button flashes on and off, press and hold **#**.

Continue to hold # until the message LED on the handset flashes on and off in sequence in red.

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 message LED on the handset flashes faster in 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 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* and *Cisco Unified CallManager Serviceability System Guide*.

Where to Go for More Troubleshooting Information

If you have additional questions about troubleshooting the Cisco Unified IP Phones, these Cisco.com web sites can provide you with more tips.

- 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 a soft, dry cloth to wipe the phone screen. Do not apply liquids or powders directly on the phone. As with all non-weather-proof electronics, liquids and powders can damage the components and cause failures.

Providing Information to Users

If you are a system administrator, you are likely the primary source of information for Cisco Unified IP Phone users in your network or company. It is important to provide current and thorough information to end users.

Cisco recommends that you create a web page on your internal support site that provides end users with important information about their Cisco Unified IP Phones.

Consider including the following types of information on this site:

- How Users Obtain Support for the Cisco Unified IP Phone, page A-1
- How Users Get Copies of Cisco Unified IP Phone Manuals, page A-2
- How Users Subscribe to Services and Configure Phone Features, page A-2
- How Users Access a Voice Messaging System, page A-3
- How Users Configure Personal Directory Entries, page A-4

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.

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. The *Cisco Unified IP Phone 7911G Guide* include detailed user instructions for key phone features.

There are several Cisco Unified IP Phone models available, so to assist users in finding the appropriate documentation on the Cisco website, Cisco recommends that you provide links to the current documentation. If you do not want to or cannot send users to the Cisco website, Cisco suggests that you download the PDF files and provide them to end users on your website.

For a list of available documentation, go to the Cisco Unified IP Phone website at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/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 and default password 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 5-16).

- A brief description of what a web-based, graphical user interface application is, and how to access it with a web browser.
- An overview of the tasks that users can accomplish using the web page.

You can also refer users to *Customizing Your Cisco Unified IP Phone on the Web*, which is available at this URL:

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

How Users Access a Voice Messaging System

Cisco Unified CallManager lets you integrate with many different voice mail 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 mail messaging system account.

  Make sure that you have used Cisco Unified CallManager to configure the **Messages** menu or the **Msgs** softkey.

- 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-2 for details.

- Cisco Unified IP Phone Address Book Synchronizer.

  Make sure to provide users with the installer for this application. To obtain the installer, choose **Application > Install Plugins** from Cisco Unified CallManager and click **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 using Cisco Unified IP Phones in a locale other than English, you should install the Cisco Unified Communications 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. For more information, refer to *Using the Cisco Unified Communications Locale Installer* at this URL:

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

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 Phones 7906G and 7911G.

- 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.

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	6.5 in. (20.3 cm)
Width	7 in. (17.67 cm)
Depth	6 in. (15.2 cm)
Weight	1.9 lb (0.9 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 100m (330 feet) 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).
- RJ-45 jack for the access port 10/100BaseT connection (labeled 10/100 PC).
- 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-

Table C-2 Network Port Connector Pinouts (continued)

Pin Number	Function
3	RD+
4	+48 Volts return[1]
5	+48 Volts return[1]
6	RD-
7	+48 Volts source[1]
8	+48 Volts source[1]

1. When used to receive power from an inline power card in the Cisco Catalyst switch.

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

.cnf.xml configuration file 2-7

Numerics

10/100/1000 PC port 3-5
10/100 PC port 3-5
  See also access port
10/100 SW port 3-5
  See also network port

A

abbreviated dialing 5-2
AC adapter, connecting 3-10
access, to phone settings 3-18, 4-2
access port
  10/100/1000 PC 3-5
  10/100 PC 3-5
  configuring 4-14
  connecting 3-10
  disabled 4-22
  forwarding packets to 4-21
access to phone settings 4-2
Access web page 8-3, 8-12
adding
  Cisco Unified IP Phones manually 2-14
  Cisco Unified IP Phones using auto-registration 2-12
  Cisco Unified IP Phones using auto-registration with TAPS 2-13
  Cisco Unified IP Phones using BAT 2-15
  users to Cisco Unified CallManager 5-16
Admin. VLAN ID 4-11
Alternate TFTP 4-12
audience, for this document xiii
authenticated call 1-16
authentication 1-10, 3-17
Authentication URL 4-18
auto answer 5-2
auto-registration
  using 2-12
  using with TAPS 2-13
auxiliary VLAN 2-3

B

background image
  configuring 6-6
  creating 6-4

custom 6-4
List.xml file 6-4
PNG file 6-4, 6-6
background images
requirements 6-6
barge 1-16, 5-3
BAT (Bulk Administration Tool) 2-15
block external to external transfer 5-3
BootP 1-5
BOOTP Server 4-7
Bootstrap Protocol (BootP) 1-5

C

call
authenticated 1-16
Call Control Protocol 7-7
call display restrictions 5-3
caller ID 5-5
call forward 5-4
call-forward alternate party (CFAP) 5-9
call forward display, configuring 5-6
CallManager 1-5 4-15
CallManager Configuration menu 4-15
call park 5-4
call pickup 5-4
call waiting 5-5
CAPF (Certificate Authority Proxy Function) 3-17
cell phone interference 1-1
certificate trust list file
See CTL file
Cisco Call Back 5-5
Cisco Discovery Protocol
See CDP
Cisco Unified CallManager
adding phone to database of 2-11
interactions with 2-2
required for Cisco Unified IP Phones 3-3
verifying settings 9-6
Cisco Unified CallManager Administration
adding phones using 2-14
adding telephony features using 5-2
Cisco Unified IP Phone
adding manually to Cisco Unified CallManager 2-14
adding to Cisco Unified CallManager 2-11
cleaning 9-18
configuration requirements 1-17
configuring user services 5-15
features 1-2
figure 1-2
installation overview 1-17
installation procedure 3-9
installation requirements 1-17
modifying phone button templates 5-14
mounting to wall 3-15
power sources 2-4
registering 2-11

registering with Cisco Unified CallManager 2-12, 2-13, 2-15
resetting 9-15
supported networking protocols 1-4
technical specifications C-1
troubleshooting 9-1
using LDAP directories 5-13
web page 8-1
Cisco Unified IP Phone 7912G
figure 3-13
cleaning the Cisco Unified IP Phone 9-18
Clear softkey 7-9, 7-17
client matter codes 5-6
conference 5-6
configurable call forward display 5-6
configuration file
.cnf.xml 2-7
creating 9-7
overview 2-6
XmlDefault.cnf.xml 2-7
configuring
from a Cisco Unified IP Phone 4-3
LDAP directories 5-13
overview 1-17
personal directories 5-13
phone button templates 5-14
softkey templates 5-14
startup network settings 3-16
user features 5-16
connecting
handset 3-10
to AC adapter 3-10
to a computer 3-10
to the network 3-10
Console Logs web page 8-3
Core Dumps web page 8-3
CTL file
deleting from phone 9-16
requesting 2-9
unlocking 7-4
custom phone rings
about 6-1
creating 6-1, 6-3, 6-6
PCM file requirements 6-3

D

daisy chaining 9-13
data VLAN 2-4
Debug Display web page 8-3, 8-15
Default Router 1-5 4-10
device authentication 1-13
Device Configuration menu
displaying 4-2
editing values 4-4
overview 4-2
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 URL 4-18
directory numbers, assigning manually 2-14
direct transfer 5-6
DNS server
troubleshooting 9-11
verifying settings 9-6
DNS Server 1-5 4-11
documentation
additional xv
Domain Name 4-8
Domain Name System (DNS) 4-8
Domain Name System (DNS) server 4-11
DSCP For Call Control 4-23
DSCP For Configuration 4-23
DSCP For Services 4-23
Dynamic Host Configuration Protocol
See DHCP

E

editing, configuration values 4-4
encryption 1-10
media 1-14
Erase softkey 9-16
error messages, used for troubleshooting 9-4
Ethernet Configuration menu
about 4-21
options
Span to PC Port 4-21
Ethernet Information web page 8-3, 8-12
extension mobility 5-7

F

features
configuring on phone, overview 1-9
configuring with Cisco Unified CallManager, overview 1-9
informing users about 1-10
figure
Cisco Unified IP Phone features 1-2
file authentication 1-13
file format
List.xml 6-4
RingList.xml 6-2
firmware
verifying version 7-19
Firmware Versions screen 7-19
footstand, installing 3-11, 3-12
forced authorization codes 5-7

G

GARP Enabled 4-22
group call pickup 5-7
Group Listen 4-20
Group Listen mode 3-6

H

handset
  light strip 1-4
handset, connecting 3-10
headset port 3-10
hold 5-7
Host Name 4-7
HTTP
  description 1-5
HTTP Configuration menu
  about 4-18
  options
    Authentication URL 4-18
    Directories URL 4-18
    Idle URL 4-19
    Idle URL Time 4-19
    Information URL 4-18
    Messages URL 4-18
    Proxy Server URL 4-18
    Services URL 4-18

I

icon
  lock 1-16
  padlock 1-16
  shield 1-16
idle display
  timeout 4-19
  XML service 4-19
Idle URL 4-19
Idle URL Time 4-19
image authentication 1-13
immediate divert 5-8
Information URL 4-18
installing
  Cisco Unified CallManager configuration 3-3
  network requirements 3-2
  preparing 2-11
  procedure 3-9
  requirements, overview 1-17
  safety warnings 3-3
interference, cell phone 1-1
Internet Protocol (IP) 1-6
IP address
  assigning 4-8
  troubleshooting 9-5

J

join 5-8

L

LDAP directories, using with Cisco Unified IP Phone 5-13
List.xml file 6-4
Locale Configuration menu
about 4-19
options
Network Locale 4-20
Network Locale Version 4-20
User Locale 4-19
User Locale Char Set 4-19
User Locale Version 4-19
Locale Installer B-1
localization
Installing the Cisco Unified Communications Locale Installer B-1
Locally Significant Certificate (LSC) 3-17
lock icon 1-16
LSC (locally significant certificate) 7-7

M

MAC address 4-7
malicious caller identification (MCID) 5-8
manufacturing installed certificate (MIC) 1-14
Media Configuration menu
about 4-20
options
Speaker Enabled 4-20
media encryption 1-14
meet-me conference 5-8
messages (status) 7-8
Messages URL 4-18
message waiting 5-9
MIC 1-14, 7-7
Model Information screen 7-1
Monitor mode 3-6
multilevel precedence and preemption (MLPP) 5-9
music-on-hold 5-9

N

native VLAN 2-4
Network Configuration menu
about 4-7
displaying 4-2
editing values 4-4
locking options 4-3
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
PC VLAN 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 4-3
Network Configuration web page 8-2, 8-7
network connectivity, verifying 9-4
networking protocol
BootP 1-5
CDP 1-5
DHCP 1-5
HTTP 1-5
IP 1-6
RTP 1-6
SCCP 1-6
SRTP 1-6
TCP 1-6
TFTP 1-7
TLS 1-6
UDP 1-7
networking protocols, supported 1-4
Network Locale
description 4-20
version 4-20
network outages, identifying 9-9
network port
10/100 SW 3-5
configuring 4-13
connecting to 3-10
network requirements, for installing 3-2
network settings, startup configuration 3-16
network statistics 7-16, 8-12
Network Statistics screen 7-16
Network web page 8-3, 8-12

O

Operational VLAN ID 4-11

P

padlock icon 1-16, 4-4
PC, connecting to the phone 3-5
PCM file requirements, for custom ring types 6-3
PC Port Configuration 4-14
PC Port Disabled 4-22

PC VLAN 4-14
personal directories 5-13
phone button templates, modifying 5-14
phones
  configuration checklist (table) 1-18
phone settings access 4-2
physical connection, verifying 9-9
plugging in Cisco Unified IP Phone 3-9
PNG file 6-4, 6-6
PoE
power
  providing to the Cisco Unified IP Phone 2-4
Power over Ethernet
  See PoE
power source
  description 2-4
  external power 2-4, 2-5
  PoE 2-4, 2-5
privacy 5-10
Proxy Server URL 4-18

Q

QoS Configuration menu
  about 4-23
  options
    DSCP For Call Control 4-23
    DSCP For Configuration 4-23
    DSCP For Services 4-23
QRT softkey 5-10, 9-17
Quality Reporting Tool (QRT) 5-10, 9-17

R

Real-Time Transport Protocol
  See RTP
redial 5-10
reset, factory 9-16
resetting
  basic 9-15
  Cisco Unified IP phone 9-15
  continuously 9-8
  intentionally 9-10
  methods 9-15
RingList.xml file format 6-2
ring setting 5-10

S

safety warnings 3-3
SCCP
  description 1-6
Secure Real-Time Transport Protocol
  See RTP
security
  CAPF (Certificate Authority Proxy Function) 3-17
  configuring on phone 3-17

- device authentication 1-13
- file authentication 1-13
- image authentication 1-13
- Locally Significant Certificate (LSC) 3-17
- media encryption 1-14
- signaling authentication 1-13

Security Configuration menu
- about 4-21
- options
  - GARP Enabled 4-22
  - Logging Display 4-23
  - PC Port Disabled 4-22
  - Security Mode 4-23
  - Voice VLAN Enabled 4-22
  - Web Access Enabled 4-22

Security Configuration screen 7-1
Security Mode 4-23
services
- configuring for users 5-15
- description 5-11
- subscribing to 5-15

Services URL 4-18
Settings menu access 3-18, 4-2
shield icon 1-16
signaling authentication 1-13
softkey templates, configuring 5-14
Span to PC Port 4-21
speaker
- about 3-6
- disabling 3-6

Speaker Enabled 4-20
speed dial 5-11
speed dialing 5-2
startup problems 9-2
startup process
- accessing TFTP server 2-9
- configuring VLAN 2-8
- contacting Cisco Unified CallManager 2-10
- loading stored phone image 2-8
- obtaining IP address 2-8
- obtaining power 2-8
- requesting configuration file 2-10
- requesting CTL file 2-9
- understanding 2-7
- verifying 3-16

statistics
- network 7-16, 8-12

Status menu 7-1, 7-8
status messages 7-2, 7-3
Status Messages screen 7-8
Status Messages web page 8-3, 8-15
Stream 1 web page 8-3, 8-16
Stream 2 web page 8-3, 8-16
Stream 3 web page 8-3, 8-16
Subnet Mask 4-8
SW Port Configuration 4-13

T

TAPS (Tool for Auto-Registered Phones Support) 2-13

TCP 1-6

technical specifications, for Cisco Unified IP Phone C-1

telephony features

- abbreviated dialing 5-2
- auto answer 5-2
- barge 1-16, 5-3
- block external to external transfer 5-3
- call display restrictions 5-3
- caller ID 5-5
- call forward 5-4
- call park 5-4
- call pickup 5-4
- call waiting 5-5
- Cisco Call Back 5-5
- client matter codes 5-6
- conference 5-6
- configurable call forward display 5-6
- direct transfer 5-6
- extension mobility 5-7
- forced authorization codes 5-7
- group call pickup 5-7
- hold 5-7
- immediate divert 5-8
- join 5-8
- malicious caller identification (MCID) 5-8
- meet-me conference 5-8
- multilevel precedence and preemption (MLPP) 5-9
- music-on-hold 5-9
- privacy 5-10
- redial 5-10
- ring setting 5-10
- services 5-11
- speed dial 5-11
- Time-of-Day Routing 5-11
- transfer 5-11
- voice messaging system 5-12

TFTP

- description 1-7
- troubleshooting 9-5

TFTP Server 1 4-9

TFTP Server 2 4-10

time, displayed on phone 3-2

Time-of-Day Routing 5-11

TLS 2-6

touchscreen

- See also LCD screen

transfer 5-11

Transmission Control Protocol

- See TCP

Transport Layer Security

- See TLS

Trivial File Transfer Protocol

- See TFTP

troubleshooting

Cisco Unified CallManager settings 9-6
Cisco Unified IP Phone 9-1
DHCP 9-9
DNS 9-11
DNS settings 9-6
IP addressing and routing 9-5
network connectivity 9-4
network outages 9-9
phones resetting 9-10
physical connection 9-9
services on Cisco Unified CallManager 9-6
TFTP settings 9-5
VLAN configuration 9-10
Trust List screen 7-5

U

UDI 8-6
UI Configuration menu
about 4-20
options
Group Listen 4-20
Unlock softkey 7-4
User Datagram Protocol
See UDP
User Locale
character set 4-19
description 4-19
version 4-19
users
adding to Cisco Unified CallManager 5-16
configuring personal directories A-4
documentation for A-2
providing required information to A-1
providing support to A-1
subscribing to services A-2

V

verifying
firmware version 7-19
startup process 3-16
video
mode 5-12
support 5-12
VLAN
auxiliary, for voice traffic 2-3
configuring 4-11
configuring for voice networks 2-3
native, for data traffic 2-4
verifying 9-10
voice messaging system 5-12
voice messaging system, accessing A-3
voice VLAN 2-3
Voice VLAN Enabled 4-22

W

wall mounting 3-15
Web Access Enabled 4-22
web page
  about 8-1
  Access 8-3, 8-12
  accessing 8-2
  Console Logs 8-3
  Core Dumps 8-3
  Debug Display 8-3, 8-15
  Device Information 8-2, 8-4
  disabling access to 8-3
  Ethernet Information 8-3, 8-12
  Network 8-3, 8-12
  Network Configuration 8-7
  Network Configuration web page 8-2
  preventing access to 8-3
  Status Messages 8-3, 8-15
  Stream 1 8-3, 8-16
  Stream 2 8-3, 8-16
  Stream 3 8-3, 8-16

X

XmlDefault.cnf.xml 2-7

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

OL-10008-01