



Cisco Unified Wireless IP Phone 7921G Administration Guide for Cisco Unified CallManager Release 4.1, 4.2, 5.0 and Later

Cisco Unified Wireless IP Phone 7921G

Americas Headquarters

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

Text Part Number: OL-10802-01

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

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

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

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

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

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

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

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

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

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

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

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

Cisco Unified Wireless IP Phone 7921G Administration Guide for Cisco Unified CallManager Release 4.1, 4.2, 5.0 and Later,
© 2000-2007 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xv

Overview 1-xv

Audience 1-xv

Objectives 1-xvi

Organization 1-xvi

Related Documentation 1-xvii

Obtaining Documentation 1-xviii

 Cisco.com 1-xviii

 Product Documentation DVD 1-xviii

 Ordering Documentation 1-xix

Documentation Feedback 1-xix

Cisco Product Security Overview 1-xix

 Reporting Security Problems in Cisco Products 1-xx

Product Alerts and Field Notices 1-xxi

Obtaining Technical Assistance 1-xxi

 Cisco Support Website 1-xxi

 Submitting a Service Request 1-xxii

 Definitions of Service Request Severity 1-xxiii

Obtaining Additional Publications and Information 1-xxiv

Document Conventions 1-xxv

CHAPTER 1

An Overview of the Cisco Unified Wireless IP Phone 7921G 1-1

Understanding the Cisco Unified Wireless IP Phone 7921G 1-1

- Features Supported on the Cisco Unified Wireless IP Phone 7921G **1-5**
 - Feature Overview **1-6**
 - Configuring Telephony Features **1-6**
 - Configuring Security for the Phone **1-7**
 - Configuring Network Access for the Phone **1-8**
 - Providing Users with Feature Information **1-8**
- Understanding Security Features for Cisco Unified IP Phones **1-9**
 - Overview of Supported Security Features **1-11**
 - Understanding Security Profiles **1-14**
 - Identifying Encrypted and Authenticated Phone Calls **1-15**
 - Security Restrictions **1-16**
- Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7921G **1-16**
 - Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager **1-17**
 - Checklist for Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager **1-17**
 - Installing the Cisco Unified Wireless IP Phone 7921G **1-22**
 - Checklist for Installing the Cisco Unified Wireless IP Phone 7921G **1-22**

CHAPTER 2

An Overview of the Voice Over IP Wireless Network 2-1

- Understanding the Wireless LAN **2-1**
 - The 802.11 Standards for Wireless LAN Communications **2-3**
 - Connecting to the Wireless Network **2-4**
 - Security for Voice Communications **2-6**
- Components of the VoIP Wireless Network **2-8**
 - Networking Protocols Used with Cisco Unified Wireless IP Phones **2-8**
 - Interacting with Cisco Unified Wireless Access Points **2-12**
 - Associating to an Access Point **2-13**
 - Roaming in a Wireless Network **2-14**

Voice Quality in a Wireless Network	2-16
Authentication Mechanisms in the Wireless Network	2-19
Authenticated Key Management	2-20
Encryption Methods	2-21
Choosing Authentication and Encryption Methods	2-21
Interacting with Cisco Unified CallManager	2-24
Phone Configuration Files and Profile Files	2-25
Interacting with the DHCP Server	2-25
Voice Over IP Wireless Network Configuration	2-27
Wireless Network Requirements for VoIP	2-27
Configuring the Wireless Network for Voice	2-28
Configuration Tip for Cisco Airespace Access Points	2-30
Site Survey Verification	2-31
Performing a Site Survey Verification	2-31
Using the Cisco Unified Wireless IP Phone 7921G Site Survey Utility	2-32

CHAPTER 3**Setting Up the Cisco Unified Wireless IP Phone 7921G 3-1**

Before You Begin	3-1
Network Requirements	3-1
Methods for Adding Phones to Cisco Unified CallManager	3-3
Adding Phones with Auto-Registration	3-4
Adding Phones with Auto-Registration and TAPS	3-4
Adding Phones with BAT	3-5
Adding Phones with Cisco Unified CallManager Administration	3-6
Safety Information	3-6
Battery Safety Notices	3-8
Installing the Cisco Unified Wireless IP Phone 7921G	3-10
Providing Power to the Phone	3-10
Installing or Removing the Phone Battery	3-11
Using the Power Supply to Charge the Phone	3-12

- Using the USB Cable to Charge the Phone 3-15
- Installing and Using the Desktop Charger 3-17
 - Using the Desktop Charger to Charge the Phone 3-19
 - Battery Charging Times Using the Desktop Charger 3-20
- Configuring Wireless LAN Settings for the Cisco Unified Wireless IP Phone 7921G 3-20
 - Cisco Unified Wireless IP Phone 7921G Web Pages 3-21
 - Network Profile Menu on the Cisco Unified Wireless IP Phone 7921G 3-21
 - Using a Headset 3-21
 - Audio Quality Subjective to the User 3-22
 - Connecting a Headset 3-22
 - Using External Devices with Your Cisco Unified IP Phone 3-22
- Powering On the Cisco Unified Wireless IP Phone 7921G 3-23
 - Active and Standby Phone Modes 3-25
 - Active mode 3-25
 - Standby mode 3-25
- Understanding the Phone Startup Process 3-26

CHAPTER 4

Using the Cisco Unified Wireless IP Phone 7921G Web Pages 4-1

- Using the USB Connection for Initial Phone Configuration 4-2
 - Setting Up Your PC to Configure the Cisco Unified Wireless IP Phone 7921G 4-2
 - Installing the USB Drivers 4-3
 - Configuring the USB LAN on the PC 4-4
 - Accessing the Phone Web Page 4-5
 - Using the USB Cable to Configure Phones 4-6
- Updating Phones Remotely 4-6
 - Setting Configuration Privileges for the Phone Web Page 4-7
 - Accessing the Configuration Web Page for a Phone 4-7

Summary Information Web Page	4-9
Configuring Network Profiles	4-10
Network Profile Settings	4-10
Configuring Wireless Settings in a Network Profile	4-15
Setting the Wireless LAN Security Mode	4-16
Configuring the Authentication Method	4-17
Setting the Wireless Security Credentials	4-18
Configuring the Username and Password	4-18
Configuring the Pre-shared Key	4-19
Setting Wireless Encryption	4-20
Configuring IP Network Settings	4-21
Enabling DHCP	4-22
Disabling DHCP	4-22
Configuring the Alternate TFTP Server	4-23
Configuring Advanced Settings	4-24
Configuring USB Settings	4-25
Configuring Trace Settings	4-27
Using System Settings	4-29
Viewing Trace Logs	4-30
Backup Settings for Phone Configuration	4-30
Using Network Profile Templates	4-31
Creating a Configuration Template	4-31
Importing a Configuration Template	4-34
Upgrading Phone Firmware	4-34
Changing the Admin Password	4-35

Configuring Settings on the Cisco Unified Wireless IP Phone 7921G 5-1

Accessing Network and Phone Settings	5-2
Configuring Network Profile Settings	5-3

- Accessing a Network Profile 5-3
- Changing the Profile Name 5-4
 - Guidelines for Editing Settings in the Network Profile 5-5
- Changing Network Configuration Settings 5-6
- Configuring DHCP Settings 5-8
 - Disabling DHCP 5-8
 - Configuring an Alternate TFTP Server 5-10
 - Changing the Cisco Discovery Protocol Settings 5-10
 - Erasing the Configuration 5-11
- Configuring Wireless Settings for the Network Profile 5-11
 - Accessing the WLAN Configuration Menu 5-12
 - Changing WLAN Configuration Settings 5-12
- Changing Phone Settings 5-15
- Configuring the Security Certificate on the Phone 5-17
- Changing the USB Configuration 5-19

CHAPTER 6

Configuring Features, Templates, Services, and Users 6-1

- Configuring Cisco Unified Wireless IP Phones in Cisco Unified CallManager 6-2
 - Telephony Features Available for the Phone 6-2
 - Specific Configuration Options for the Cisco Unified Wireless IP Phone 7921G 6-15
 - Configuring Softkey Templates 6-16
 - Softkey Templates for the Cisco Unified Wireless IP Phone 7921G 6-17
 - Changing Softkeys in a Template 6-17
 - Modifying Phone Button Templates 6-18
 - Setting Up Services 6-19
 - Configuring Corporate and Personal Directories 6-20
 - Configuring Corporate Directories 6-21
 - Configuring Personal Directory 6-21

- Adding Users to Cisco Unified CallManager 6-22
- Managing the User Options Web Pages 6-23
 - Giving Users Access to the User Options Web Pages 6-23
 - Specifying Options that Appear on the User Options Web Pages 6-24
- Creating Custom Phone Rings 6-25

CHAPTER 7**Viewing Security, Device, Model, and Status Information on the Phone 7-1**

- Viewing Security Information 7-2
 - Accessing the CTL File Screen 7-4
 - Trust List Screen 7-5
- Viewing Device Information 7-6
- Viewing Model Information 7-10
- Viewing the Phone Status Menu 7-12
 - Viewing the Status Messages 7-12
 - Viewing the Current Configuration 7-15
- Viewing Network Statistics 7-16
- Viewing Call Statistics 7-18
- Viewing Firmware Versions 7-22

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

- Accessing the Web Page for a Phone 8-2
- Summary Information 8-3
- Network Configuration Information 8-4
- Device Information 8-9
- Wireless LAN Statistics 8-11
- Network Statistics 8-13
- Stream Statistics 8-16

Troubleshooting the Cisco Unified Wireless IP Phone 7921G 9-1

Resolving Startup and Connectivity Problems 9-1

Symptom: The unified IP phone Does Not Complete the Normal Start Up Process 9-2

Symptom: The Wireless IP Phone Does Not Associate with a Cisco Aironet Access Point 9-3

Verifying Access Point Settings 9-3

Symptom: The unified IP phone Does Not Register with Cisco Unified CallManager 9-5

Registering the Phone with Cisco Unified CallManager 9-5

Checking Network Connectivity 9-6

Verifying TFTP Server Settings 9-6

Verifying IP Addressing 9-7

Verifying DNS Settings 9-8

Verifying Cisco Unified CallManager Settings 9-8

Cisco Unified CallManager and TFTP Services Are Not Running 9-9

Creating a New Configuration File 9-10

Resolving Voice Quality and Roaming Problems 9-11

Symptom: unified IP phone Resets Unexpectedly 9-11

Verifying Access Point Settings 9-11

Identifying Intermittent Network Outages 9-12

Verifying DHCP Settings 9-12

Verifying Voice VLAN Configuration 9-12

Verifying that the Phones Have Not Been Intentionally Reset 9-13

Eliminating DNS or Other Connectivity Errors 9-13

Symptom: The unified IP phone Has Audio Problems 9-14

No Audio During a Connected Call 9-14

One-Way Audio During a Connected Call 9-14

Symptom: The unified IP phone Does Not Roam Properly 9-15

Voice Quality Deteriorates While Roaming 9-16

Delays in Voice Conversation While Roaming	9-16
Phone Loses Connection with Cisco Unified CallManager While Roaming	9-16
Monitoring the Voice Quality of Calls	9-17
Using Voice Quality Metrics	9-18
Troubleshooting Tips	9-18
General Troubleshooting Information	9-20
Common Phone Status Messages	9-20
Troubleshooting Tips for the Cisco Unified Wireless IP Phone 7921G	9-22
Logging Information for Troubleshooting	9-24
Using a System Log Server	9-24
Using the Trace Logs on the unified IP phone	9-24
Erasing the Local Configuration	9-25

APPENDIX A
Providing Information to Users By Using a Website A-1

How the Cisco Unified Wireless IP Phone Operates	A-2
How to Care for and Clean the Phone	A-3
How Users Access the Help System on the Phone	A-4
How Users Get Copies of Cisco Unified IP Phone Manuals	A-5
How Users Configure Phone Features and Services	A-6
How Users Access Voice Messages	A-7

APPENDIX B
Supporting International Users B-1

Installing the Cisco Unified CallManager Locale Installer	B-1
---	-----

APPENDIX C
Physical and Operating Environment Specifications C-1

APPENDIX D
Checklist for Deploying the Cisco Unified Wireless IP Phone 7921G D-1

Configuring the Wireless Network	D-1
----------------------------------	-----

Configuration Tip for Cisco Aireospace Access Points **D-3**

Configuring QoS Policies **D-4**

 Access Point Configuration Settings **D-4**

 Controller Settings **D-5**

 Switch Configuration **D-5**

Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco
Unified CallManager **D-6**

Installing the Cisco Unified Wireless IP Phone 7921G **D-9**

INDEX



Preface

Overview

Cisco Unified Wireless IP Phone 7921G Administration Guide provides the information you need to understand, install, configure, and manage the Cisco Unified Wireless IP Phone 7921G on your network. This guide is intended to be used to administer phones running with Cisco Unified CallManager Release 4.1 or later and Cisco Unified CallManager Release 5.0 and later.

Audience

Network engineers, system administrators, or telecom engineers should review this guide to learn the steps required to properly set up the Cisco Unified Wireless IP Phone 7921G on the wireless network.

The tasks described are considered to be 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 Wireless IP Phone 7921G and Cisco Unified CallManager, these tasks require familiarity with Cisco Unified CallManager.

Objectives

This guide provides the required steps to get the Cisco Unified Wireless IP Phone 7921G up and running on a wireless Voice-over-IP (VoIP) network. Because of the complexity of an IP telephony network, this guide does not provide complete and detailed information for procedures that you need to perform on the Cisco Unified CallManager application or other network devices.

Organization

This guide is organized as follows:

Chapter	Description
Chapter 1, “An Overview of the Cisco Unified Wireless IP Phone 7921G”	Provides a conceptual overview and description of the Cisco Unified Wireless IP Phone 7921G and provides an overview of the tasks required prior to installation
Chapter 2, “An Overview of the Voice Over IP Wireless Network”	Describes how the IP Phone interacts with other key IP telephony and wireless network protocols and components
Chapter 3, “Setting Up the Cisco Unified Wireless IP Phone 7921G”	Describes how to properly and safely install and configure the Cisco Unified Wireless IP Phone 7921G on your network
Chapter 4, “Using the Cisco Unified Wireless IP Phone 7921G Web Pages”	Describes how to use the Cisco Unified Wireless IP Phone 7921G web pages for initial phone configuration and to update configuration files for the wireless IP phone
Chapter 5, “Configuring Settings on the Cisco Unified Wireless IP Phone 7921G”	Describes how to configure network profiles and phone settings, by using the Settings menu on the wireless IP phone
Chapter 6, “Configuring Features, Templates, Services, and Users”	Provides an overview of procedures for configuring telephony features and adding users to Cisco Unified CallManager

Chapter	Description
Chapter 7, “Viewing Security, Device, Model, and Status Information on the Phone”	Explains how to view phone security, device, and network information and network and call statistics from the wireless IP phone
Chapter 8, “Monitoring the Cisco Unified Wireless IP Phone Remotely”	Explains how to obtain status information about the phone using the phone web page
Chapter 9, “Troubleshooting the Cisco Unified Wireless IP Phone 7921G”	Provides tips for troubleshooting the wireless IP phone
Appendix A, “Providing Information to Users By Using a Website”	Provides suggestions for setting up a website for providing users with important information about their wireless IP phone
Appendix B, “Supporting International Users”	Provides information about setting up phones in non-English environments
Appendix C, “Physical and Operating Environment Specifications”	Provides technical specifications of the Cisco Unified Wireless IP Phone 7921G

Related Documentation

For more information about the Cisco Unified Wireless IP Phone 7921G , refer to the following publications, which are available at this location:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/wip7921/index.htm

- *Cisco Unified Wireless IP Phone 7921G Accessory Guide*
- *Cisco Unified Wireless IP Phone 7921G Phone Guide*
- *Regulatory Compliance and Safety Information for the Cisco Unified Wireless IP Phone 7920 Series and Peripheral Devices*

For more information about Cisco Unified CallManager, refer to the following publications, which are available at this location:

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

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

- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager System Guide*
- *Cisco Unified CallManager Troubleshooting Guide*
- *Cisco Unified IP Phone and Services Application Developers Guide*
- *Bulk Administration Tool User Guide*

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

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

Ordering Documentation

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

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

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

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

Documentation Feedback

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

Cisco Product Security Overview

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

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

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

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

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

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

- For nonemergencies — psirt@cisco.com

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

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



Tip

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

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

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

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

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

Product Alerts and Field Notices

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

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

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

To register as a Cisco.com user, go to this URL:

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

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support 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 Support Website

The Cisco Support 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/en/US/support/index.html>

Access to all tools on the Cisco Support 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**

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

**Tip**

Displaying and Searching on Cisco.com

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

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

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

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended

solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

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

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

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

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Internet Protocol Journal* is a quarterly journal published by Cisco 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, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:
<http://www.cisco.com/univercd/cc/td/doc/abtnicd/136957.htm>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

Document Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface .
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in <code>screen font</code> .
boldface screen font	Information you must enter is in boldface screen font.
<i>italic screen</i> font	Arguments for which you supply values are in <i>italic screen</i> font.

Convention	Description
^	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:



IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Waarschuwing

BELANGRIJKE VEILIGHEIDSINSTRUCTIES

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

BEWAAR DEZE INSTRUCTIES

Varoitus

TÄRKEITÄ TURVALLISUUSOHJEITA

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

SÄILYTÄ NÄMÄ OHJEET

Attention IMPORTANTES INFORMATIONS DE SÉCURITÉ

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

CONSERVEZ CES INFORMATIONS**Warnung WICHTIGE SICHERHEITSHINWEISE**

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

BEWAHREN SIE DIESE HINWEISE GUT AUF.**Avvertenza IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

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

CONSERVARE QUESTE ISTRUZIONI

Advarsel VIKTIGE SIKKERHETSINSTRUKSJONER

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

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

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

GUARDE ESTAS INSTRUÇÕES**¡Advertencia! INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

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

GUARDE ESTAS INSTRUCCIONES

Varning! VIKTIGA SÄKERHETSANVISNINGAR

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

SPARA DESSA ANVISNINGAR**Figyelem FONTOS BIZTONSÁGI ELOÍRÁSOK**

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

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!**Предупреждение ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

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

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告 重要的安全性说明

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

请保存这些安全性说明

警告 安全上の重要な注意事項

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

これらの注意事項を保管しておいてください。



CHAPTER 1

An Overview of the Cisco Unified Wireless IP Phone 7921G

The Cisco Unified Wireless IP Phone 7921G provides wireless voice communication over an Internet Protocol (IP) network. Like traditional analog telephones, you can place and receive phone calls and access features such as hold, transfer, and speed dial. In addition, because the phone connects to your wireless LAN, you can place and receive phone calls from anywhere in your wireless environment.

This chapter includes the following topics:

- [Understanding the Cisco Unified Wireless IP Phone 7921G, page 1-1](#)
- [Features Supported on the Cisco Unified Wireless IP Phone 7921G, page 1-5](#)
- [Understanding Security Features for Cisco Unified IP Phones, page 1-9](#)
- [Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7921G, page 1-16](#)

Understanding the Cisco Unified Wireless IP Phone 7921G









The Cisco Unified Wireless IP Phone 7921G is an 802.11 dual band wireless device that provides comprehensive voice communications in conjunction with Cisco Unified CallManager and Cisco Aironet 802.11b/g and Cisco Aironet 802.11a Access Points (APs) in a private business communications network. This phone model supports G.711a, G.711u, G.729a and G.729ab audio compression









coder-decoders (codecs). You must configure and manage a wireless IP phone like other IP phones and wireless devices on your network. The wireless IP phone supports multiple lines and most of the IP phone features of other Cisco Unified IP Phones.




Figure 1-1 shows the Cisco Unified Wireless IP Phone 7921G. The table that follows describes the functions of the keys on the phone.

Figure 1-1 Cisco Unified Wireless IP Phone 7921G Buttons and Keys



1	Indicator light (LED)	<p>Provides these indications:</p> <ul style="list-style-type: none"> • Solid red—Phone is connected to AC power source and battery is charging. • Solid green—Phone is connected to AC power source and battery is fully charged. • Fast blinking red—Incoming call. (Phone can be charging or fully charged.) • Slow blinking red—Voice message. (When connected to AC power source, red light displays longer than when phone is using only the battery.) • Slow blinking green—Phone is using only battery power. Phone is registered with the wireless network and is within service coverage area.
2	Headset port 	Port for plugging in a headset or ear bud.
3	Speaker button 	Toggles the speaker mode on or off for the phone.
4	Right softkey button 	Activates the Options menu for access to the list of softkeys. Sometimes displays a softkey label.
5	Navigation button 	<p>Accesses these menus and lists from the main screen:</p> <p>Directory </p> <p>Line View </p> <p>Settings </p> <p>Services </p> <p>Allows you to scroll up and down menus to highlight options and to move left and right through phone numbers and text entries.</p>

6	Select button 	Activates the Help menu from the main screen. Allows you to select a menu item, a softkey, a call, or an action.
7	Power/End button (red) 	Turns the phone on or off, silences a ringing call, or ends a connected call. When using menus, acts as a shortcut to return to the main screen.
8	Pound (#) key 	Toggles between locking and unlocking the keypad. Allows you to enter these special characters when you are entering text: # ? () [] { }
9	Zero (0) key 	Enters “0” when dialing a number. Allows you to enter a space or these special characters when you are entering text: , . ‘ “ _ ~ ’
10	Asterisk (*) key 	Toggles between Ring and Vibrate mode. Allows you to enter these special characters when you are entering text: * + - / = \ : ;
11	Keypad	Allows you to dial numbers, enter letters, and choose menu items by number. Press and hold key 1 to access your voice messaging system.
12	One (1) key 	Enters “1” when dialing a number. Allows you to access the voice messaging system. Allows you to enter these special characters when you are entering text: ! @ < > \$ % ^ &
13	Answer/Send button (green) 	Allows you to answer a ringing call or, after dialing a number, to place the call.
14	Left softkey button 	Activates the softkey option displayed on the screen.

15	Mute button 	Toggles the mute feature on or off.
16	Volume button 	When the phone is idle, controls the ring volume, vibrate option, or turns off the ring. During a call, controls the volume for the handset, headset, and speaker mode.
17	Applications button 	Configurable button that is used with XML applications, such as Push to Talk or Directory services. See “Setting Up Services” section on page 6-19 .

For more information about phone features and how they operate, refer to the [Cisco Unified Wireless IP Phone 7921G Guide](#).

Related Topics

- [Features Supported on the Cisco Unified Wireless IP Phone 7921G, page 1-5](#)
- [Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7921G, page 1-16](#)

Features Supported on the Cisco Unified Wireless IP Phone 7921G

The Cisco Unified Wireless IP Phone 7921G functions much like traditional IP phones allowing you to place and receive telephone calls while connected to the wireless LAN. In addition to traditional phone features, the Cisco Unified Wireless IP Phone includes features that enable you to administer and monitor the phone as a network device.



Caution

This product is not a medical device and may use an unlicensed frequency band that is susceptible to interference from other devices or equipment.

This section provides information about these topics:

- [Feature Overview, page 1-6](#)
- [Configuring Telephony Features, page 1-6](#)
- [Configuring Security for the Phone, page 1-7](#)
- [Configuring Network Access for the Phone, page 1-8](#)
- [Providing Users with Feature Information, page 1-8](#)

Feature Overview

The Cisco Unified Wireless IP Phone 7921G provides traditional telephony functionality, such as call forwarding and transferring, call pickup, redialing, speed dialing, conference calling, and voice messaging system access, as well as these features:

- Wireless access to your phone number and the corporate directory.
- Access to network data, XML applications, and web-based services.
- Online customizing of phone features and services from your User Options web pages.
- An online help system that displays information on the phone screen.

Related Topics

- [Configuring Network Profiles, page 4-10](#)
- [Configuring Features, Templates, Services, and Users, page 6-1](#)

Configuring Telephony Features

You can use the Cisco Unified CallManager Administration application to set up phone registration criteria and calling search spaces, and to modify softkey templates, among other tasks. For more information, see [Chapter 6, “Configuring Features, Templates, Services, and Users.”](#)

In some places, this manual provides partial instructions for procedures that involve Cisco Unified CallManager Administration. These instructions are intended to point you to the appropriate page in the Cisco Unified CallManager application and to provide some initial guidance.

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

Help > For this screen from the main menu bar.

You can access the complete Cisco Unified CallManager documentation for your version at this location:

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

Related Topics

- [Methods for Adding Phones to Cisco Unified CallManager, page 3-3](#)
- [Configuring Features, Templates, Services, and Users, page 6-1](#)

Configuring Security for the Phone

Implementing security in the wireless network (WLAN) protects against data tampering threats and identity theft of phones. To alleviate these threats, the Cisco wireless LAN provides many options for user authentication with servers and for encrypting communications streams between phones and network devices.

For information about supported security options for the Cisco Unified Wireless IP Phone 7921G, see the [“Authentication Mechanisms in the Wireless Network” section on page 2-19](#).

For information about security features supported by Cisco Unified CallManager and Cisco Unified IP Phones, see the [“Understanding Security Features for Cisco Unified IP Phones” section on page 1-9](#).

Related Topics

- [Security for Voice Communications, page 2-6](#)
- [Choosing Authentication and Encryption Methods, page 2-21](#)
- [Understanding Security Features for Cisco Unified IP Phones, page 1-9](#)

Configuring Network Access for the Phone

Like other network devices, you must configure IP phones to access Cisco Unified CallManager and the rest of the IP network using the wireless LAN. There are two methods for configuring network settings such as DHCP, TFTP, and for wireless settings for the phone.

- Cisco Unified Wireless IP Phone 7921G web pages
- Network Profiles menu on the Cisco Unified Wireless IP Phone 7921G

You can access the configuration web pages by using a browser from your PC. For more information, see [Chapter 4, “Using the Cisco Unified Wireless IP Phone 7921G Web Pages.”](#)

You can also configure network settings on the phone itself. For more information about configuring features from the phone, see [Chapter 5, “Configuring Settings on the Cisco Unified Wireless IP Phone 7921G.”](#)

Because the Cisco Unified Wireless IP Phone is a network device, you can obtain detailed status information about it. This information can assist you in troubleshooting problems that users might encounter when using their IP phones. See [Chapter 8, “Monitoring the Cisco Unified Wireless IP Phone Remotely,”](#) for tips on using this information.

Related Topics

- [Using the Cisco Unified Wireless IP Phone 7921G Web Pages, page 4-1](#)
- [Configuring Settings on the Cisco Unified Wireless IP Phone 7921G, page 5-1](#)
- [Monitoring the Cisco Unified Wireless IP Phone Remotely, page 8-1](#)

Providing Users with Feature Information

If you are a system administrator, you are the primary source of information for Cisco Unified Wireless 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 Wireless IP Phone 7921G documentation. Make sure to visit the Cisco Unified IP Phone web site:

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

From this site, you can view additional phone documentation. For complete ordering information, see the [“Obtaining Documentation” section on page xviii](#).

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

For a summary of the key information that you can provide to phone users, see [Appendix A, “Providing Information to Users By Using a Website.”](#)

**Note**

The radio frequency (RF) for the Cisco Unified Wireless IP Phone 7921G is configured for a specific regulatory domain. If users attempt to use this phone outside of the regulatory domain, the phone will not function properly and they might violate local regulations.

Related Topic

[Providing Information to Users By Using a Website, page A-1](#)

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, and also prevents data, call signaling, and media stream tampering.

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

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

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

Topic	Reference
Detailed explanation of security, including set up, configuration, and troubleshooting information for Cisco Unified CallManager and Cisco Unified IP Phones	Refer to <i>Cisco Unified CallManager Security Guide</i>
Security features supported on the Cisco Unified IP Phone	See the “ Overview of Supported Security Features ” section on page 1-11
Restrictions regarding security features	See the “ Security Restrictions ” section on page 1-16
Viewing a security profile name when running Cisco Unified CallManager 5.0 or later	See the “ Understanding Security Profiles ” section on page 1-14
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 “ Networking Protocols Used with Cisco Unified Wireless IP Phones ” section on page 2-8 See the “ Phone Configuration Files and Profile Files ” section on page 2-25
Security and the phone startup process	See the “ Understanding the Phone Startup Process ” section on page 3-26
Security and phone configuration files	See the “ Phone Configuration Files and Profile Files ” section on page 2-25
Changing the TFTP Server 1 or TFTP Server 2 option on the phone when security is implemented	See the “ Configuring Network Profiles ” section on page 4-10
Items on the Security Configuration menu on the phone	See the “ Viewing Security Information ” section on page 7-2
Unlocking the CTL file	See the “ Accessing the CTL File Screen ” section on page 7-4
Disabling access to a phone’s web pages	See the “ Specific Configuration Options for the Cisco Unified Wireless IP Phone 7921G ” section on page 6-15

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

Topic	Reference
Troubleshooting	See the “General Troubleshooting Information” section on page 9-20 Refer to <i>Cisco Unified CallManager Security Guide</i> , Troubleshooting chapter
Resetting or restoring the phone	See the “Erasing the Local Configuration” section on page 9-25

Overview of Supported Security Features

[Table 1-2](#) provides an overview of the security features that the Cisco Unified Wireless IP Phone 7921G 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, choose **Settings > Security Configuration**. For more information, see the [“Viewing Security Information”](#) 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 “Configuring the Cisco CTL Client” chapter in the *Cisco Unified CallManager Security Guide*.

Table 1-2 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 LSC (locally significant certificate) from the Security Configuration menu on the phone. See the “Configuring the Security Certificate on the Phone” section on page 5-17 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 unless they can be authenticated by the Cisco Unified CallManager.
File authentication	Validates digitally-signed files that the phone downloads. The phone validates the signature to make sure that file tampering did not occur after the file creation. Files that fail authentication are not written to Flash memory on the phone. The phone rejects such files without further processing.
Signaling Authentication	Uses the TLS protocol to validate that no tampering has occurred to signaling packets during transmission.
Manufacturing installed certificate	Each Cisco Unified IP Phone contains a unique manufacturing installed certificate (MIC), which is used for device authentication. The MIC is a permanent unique proof of identity for the phone, and allows Cisco Unified CallManager to authenticate the phone.

Table 1-2 Overview of Security Features (continued)

Feature	Description
Secure SRST reference	After you configure a SRST reference for security and then reset the dependent devices in Cisco Unified CallManager Administration, the TFTP server adds the SRST certificate to the phone cnf.xml file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router.
Media encryption	Uses SRTP to ensure that the media streams between supported devices proves secure and that only the intended device receives and reads the data. Includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport.
Signaling encryption	Ensures that all SCCP signaling messages that are sent between the device and the Cisco Unified CallManager server are encrypted.
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure that are too processing-intensive for the phone, and it interacts with the phone for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the phone, or it can be configured to generate certificates locally.
Security profiles	Defines whether the phone is non-secure, authenticated, or encrypted. See the “Understanding Security Profiles” section on page 1-14 for more information.
Encrypted configuration files	Lets you ensure the privacy of phone configuration files.

Table 1-2 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	<p>Additional security options, which you control from Cisco Unified CallManager Administration:</p> <ul style="list-style-type: none"> • Disabling Gratuitous ARP (GARP) • Disabling access to the Setting menus • Disabling access to web pages for a phone <p>Note You can view current settings for the GARP Enabled, and Web Access options by looking at the phone's Device Information menu. For more information, see the “Viewing Security Information” section on page 7-2.</p>

Related Topics

- [Understanding Security Profiles, page 1-14](#)
- [Identifying Encrypted and Authenticated Phone Calls, page 1-15](#)
- [Viewing Device Information, page 7-6](#)
- [Security Restrictions, page 1-16](#)

Understanding Security Profiles

A security profile, which defines whether the phone is non-secure, authenticated, or encrypted, is associated with every Cisco Unified IP Phone that is supported in Cisco Unified CallManager 5.0 and later. For information about configuring the security profile and applying the profile to the phone, refer to *Cisco Unified CallManager Security Guide, Release 5.0*.

**Note**

For Cisco Unified IP Phones using Cisco Unified CallManager 4.1 and later, security is configured on each phone. For more information about configuring security, refer to *Cisco Unified CallManager Security Guide, Release 4.1 (2)* or a later release document.


To view the security mode that is set for the phone, from the phone screen, choose **Settings > Device Information > Security > Security Mode**. For more information, see the “[Viewing Security Information](#)” section on page 7-2.


Related Topics

- [Identifying Encrypted and Authenticated Phone Calls](#), page 1-15
- [Viewing Device Information](#), page 7-6
- [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 screen on the phone.

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

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



Note

If the call is routed through non-IP call legs, such as the PSTN, the call might be non-secure even though it is encrypted within the IP network and has a lock icon associated with it.

Related Topics

- [Understanding Security Features for Cisco Unified IP Phones](#), page 1-9
- [Understanding Security Profiles](#), page 1-14
- [Security Restrictions](#), page 1-16

Security Restrictions

When using a phone that is not configured for encryption, the user cannot barge into an encrypted call. When barge fails in this case, a reorder tone (fast busy tone) plays on the barge initiator's phone.

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

If the phone is configured for encryption, the user 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 non-secure. The authentication icon continues to display on the authenticated phones in the call, even if the initiator's phone does not support security.

Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7921G

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

To add wireless IP phones to the IP network, system administrators also must perform a site survey to determine where to place and install access points (APs) for wireless voice coverage. For detailed information about a voice over WLAN deployment, refer to the *Cisco Enterprise Mobility 3.0 Design Guide*.

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

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

- [Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager, page 1-17](#)
- [Installing the Cisco Unified Wireless IP Phone 7921G, page 1-22](#)

Configuring the Cisco Unified Wireless IP Phone 7921G 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 [“Methods for Adding Phones to Cisco Unified CallManager” section on page 3-3](#).

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*.

Related Topic

[Checklist for Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager, page 1-17](#)

Checklist for Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager

[Table 1-3](#) provides an overview and checklist of configuration tasks for the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager Administration. The list presents a suggested order to guide you through the phone configuration process. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, refer to the sources in the list.

Table 1-3 Checklist for Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager

Task	Purpose	For More Information
<p>1. Gather the following information about the phone:</p> <ul style="list-style-type: none"> • MAC address • Name or user ID of phone user • Device pool • Calling search space and location information (if used) • Security (authentication mode and encryption) • Number of lines, associated directory numbers (DNs), and partitions to assign to the phone • User to associate with the phone • Phone usage information 	<p>Provides list of configuration requirements for setting up phones.</p> <p>Identifies preliminary configuration that you need to perform before configuring individual phones, such as button and softkey templates.</p> <p>Applies to softkey template, phone features, IP Phone services, or phone applications.</p>	<p>Refer to the <i>Cisco Unified CallManager System Guide</i>, Cisco Unified IP Phone chapter.</p> <p>See the “Telephony Features Available for the Phone” section on page 6-2.</p>
<p>2. Customize phone button templates (if required).</p>	<p>Changes the number of lines, speed-dial, Service URLs or adds a Privacy feature to Line View list to meet user needs.</p> <p>Changes softkey positions in Options menu</p>	<p>Refer to <i>Cisco Unified CallManager Administration Guide</i>, “Phone Button Template Configuration” chapter.</p> <p>See the “Modifying Phone Button Templates” section on page 6-18.</p>

Table 1-3 Checklist for Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager (continued)

Task	Purpose	For More Information
<p>3. Customize softkey templates (optional).</p>	<p>Adds, deletes, or changes order of softkey features that display in the Options menu to meet feature usage needs.</p>	<p>Refer to the <i>Cisco Unified CallManager Administration Guide</i>, Softkey Template Configuration chapter.</p> <p>See the “Configuring Softkey Templates” section on page 6-16.</p>
<p>4. Add and configure the phone by completing these fields in the Phone Configuration window:</p> <ul style="list-style-type: none"> • MAC address • Description (user name or ID) • Device Pool • Common Phone Profile • Calling Search Space • Location* • Built In Bridge and Privacy* • Phone Button Template • Softkey template (if customized) • Presence Group* • Device Security Profile* • Certificate Operation • Authentication Mode • Key Size (Bits) • Product Specific Configuration 	<p>Adds the device with its default settings to the Cisco Unified CallManager database.</p> <p>*These fields are required in Cisco Unified CallManager 5.0 and later.</p>	<p>Refer to the <i>Cisco Unified CallManager Administration Guide</i>, Cisco Unified IP Phone Configuration chapter.</p> <p>For information about Product Specific Configuration fields, click the “I or ?” Help button in the Phone Configuration window.</p>

Table 1-3 Checklist for Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager (continued)

Task	Purpose	For More Information
<p>5. Add and configure directory numbers (lines) on the phone by completing these required fields in the Directory Number Configuration window.</p> <ul style="list-style-type: none"> • Directory number(s) • Partition • Directory number settings: Voice Mail (if used) Presence Group* • Call Forwarding and Pickup (if used) • Line Settings • Multiple Calls and Call Waiting 	<p>Adds primary and secondary directory numbers and features associated with directory numbers to the phone.</p> <p>*This field is required in Cisco Unified CallManager 5.0 and later.</p>	<p>Refer to the <i>Cisco Unified CallManager 4.x Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter: “Adding a Directory Number” section “Creating a Cisco Unity Voice Mailbox” section.</p> <p>Refer to the <i>Cisco Unified CallManager 5.x Administration Guide</i>, “Configuring Directory Numbers” chapter:</p> <p>See the “Telephony Features Available for the Phone” section on page 6-2.</p>
<p>6. Configure speed-dial numbers (optional).</p>	<p>Adds speed-dial numbers.</p> <p>Note Users can change speed-dial settings on their phones by using Cisco Unified IP Phone User Options.</p>	<p>Refer to the <i>Cisco Unified CallManager Administration Guide</i>, Cisco Unified IP Phone Configuration chapter, “Configuring Speed-Dial Buttons” section.</p>
<p>7. Configure Cisco Unified IP Phone services and assign services (optional).</p>	<p>Provides IP Phone services.</p> <p>Note Users can add or change services on their phones by using the Cisco Unified IP Phone User Options.</p>	<p>Refer to the <i>Cisco Unified CallManager Administration Guide</i>, Cisco Unified IP Phone Services Configuration chapter.</p> <p>See the “Setting Up Services” section on page 6-19.</p>

Table 1-3 Checklist for Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager (continued)

Task	Purpose	For More Information
<p>8. Add user information by configuring required fields: (optional).</p> <ul style="list-style-type: none"> • Name (last) • User ID • Password (for use with User Options web pages) • PIN (for use with Extension Mobility and Personal Directory) • Presence Group* 	<p>Adds user information to the global directory for Cisco Unified CallManager.</p> <p>Note To search for a user in the Corporate Directory, add user information to Cisco Unified CallManager.</p> <p>*This field is required in Cisco Unified CallManager 5.0 and later.</p>	<p>Refer to the <i>Cisco Unified CallManager Administration Guide</i>, Adding a New User chapter.</p> <p>See the “Adding Users to Cisco Unified CallManager” section on page 6-22.</p>
<p>9. Associate a user with a phone (optional).</p>	<p>Provides users with control over their phone such as forwarding calls or adding speed-dial numbers or services.</p> <p>Note Some phones, such as those in conference rooms, do not have an associated user.</p>	<p>Refer to the <i>Cisco Unified CallManager Administration Guide</i>, Adding a New User chapter, “Associating Devices to a User” section.</p>

Related Topics

- [Installing the Cisco Unified Wireless IP Phone 7921G, page 1-22](#)
- [Checklist for Installing the Cisco Unified Wireless IP Phone 7921G, page 1-22](#)
- [Configuring Features, Templates, Services, and Users, page 6-1](#)

Installing the Cisco Unified Wireless IP Phone 7921G

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 Wireless IP Phone Installation Guide that ships in the box with each phone provides directions for assembling the phone and accessories and charging the battery.

Prior to using the phone to connect to the wireless LAN, you need to configure a network profile for the phone. You can use the Cisco Unified Wireless IP Phone 7921G web pages to set up the network profile and other phone settings, or you can configure the network profile using phone menus.

If you use auto-registration with Cisco Unified CallManager, you need to update the specific configuration information for the phone such as associating the phone with a user, changing the softkey template, or directory number.

**Note**

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

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

Related Topic

[Checklist for Installing the Cisco Unified Wireless IP Phone 7921G, page 1-22](#)

Checklist for Installing the Cisco Unified Wireless IP Phone 7921G

Table 1-4 provides an overview and checklist of installation tasks for the Cisco Unified Wireless IP Phone 7921G. The list presents a suggested order to guide you through the phone installation. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, refer to the sources in the list.

Table 1-4 Checklist for Installing the Cisco Unified Wireless IP Phone 7921G

Task	Purpose	For More Information
1. Assemble the phone components and charge the battery.	Charges the phone for use.	See Providing Power to the Phone , page 3-10.
2. Configure the network profile by using the USB cable and the Cisco Unified Wireless IP Phone 7921G web pages.	Sets up IP network and WLAN configuration for the phone.	See Using the Cisco Unified Wireless IP Phone 7921G Web Pages , page 4-1.
3. Configure other phone settings by using the Settings menu on the phone.	Sets up phone settings such as sounds, display, and keypad settings.	See Configuring Settings on the Cisco Unified Wireless IP Phone 7921G , page 5-1.
4. Power on the phone and monitor the phone startup process.	Verifies that phone is configured properly.	See Understanding the Phone Startup Process , page 3-26. See Resolving Startup and Connectivity Problems , page 9-1.
5. Make calls with the wireless IP phone.	Verifies that the phone and features work correctly.	Refer to the <i>Cisco Unified Wireless IP Phone 7921G Guide</i> . See Resolving Voice Quality and Roaming Problems , page 9-11.
6. 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 wireless IP phone.	See Appendix A, "Providing Information to Users By Using a Website."

Related Topics

- [Understanding the Cisco Unified Wireless IP Phone 7921G](#), page 1-1
- [Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager](#), page 1-17
- [Troubleshooting the Cisco Unified Wireless IP Phone 7921G](#), page 9-1



CHAPTER 2

An Overview of the Voice Over IP Wireless Network

With the introduction of wireless communication, wireless IP phones can provide voice communication within the corporate wireless local area network (WLAN). The Cisco Unified Wireless IP Phone 7921G depends upon and interacts with wireless access points and key Cisco IP telephony components, including Cisco Unified CallManager, to provide wireless voice communication.

This chapter provides you with an overview of the interaction between the Cisco Unified Wireless IP Phone 7921G and other key components of the Voice-over-IP (VoIP) network in the WLAN environment.

- [Understanding the Wireless LAN, page 2-1](#)
- [Components of the VoIP Wireless Network, page 2-8](#)
- [Voice Over IP Wireless Network Configuration, page 2-27](#)
- [Understanding the Phone Startup Process, page 3-26](#)
- [Site Survey Verification, page 2-31](#)

Understanding the Wireless LAN

This section includes the following topics about the wireless LAN:

- [The 802.11 Standards for Wireless LAN Communications, page 2-3](#)
- [Connecting to the Wireless Network, page 2-4](#)
- [Security for Voice Communications, page 2-6](#)

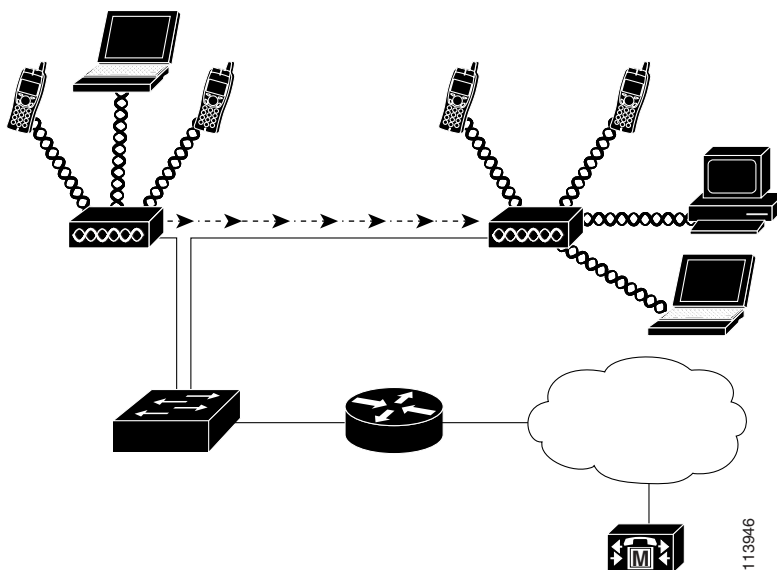
In a traditional LAN, phones and computers use cables to transmit messages and data packets over a wire conductor. Wireless LANs use radio waves to carry the messages and data packets.

WLANs require access point devices that receive and transmit radio signals. Cisco Aironet Access Points, such as the 1200, 1100, and 350 series models, support voice on a WLAN. [Figure 2-1](#) shows a typical WLAN topology that incorporates wireless data for laptop computers and wireless IP telephony (WIPT) for wireless IP phones.

When a wireless device powers on, it immediately searches for and becomes associated with an access point. As users move from one location to another within the corporate WLAN environment, the wireless device roams out of range of one access point and into the range of another. The access point uses the wired network to transmit data and voice packets to the switches and routers. Voice signaling packets are sent to the Cisco Unified CallManager server for call processing and routing.

For more information about the Cisco wireless products, refer to http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_package.html

Figure 2-1 *Wireless LAN with Wireless IP Phones*



113946

The 802.11 Standards for Wireless LAN Communications

Wireless LANs must follow the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards that define the protocols that govern all Ethernet-based wireless traffic. The Cisco Unified Wireless IP Phone 7921G supports these standards:

- The 802.11b standard was the first standard in wireless LAN communications, which is commonly called Wi-Fi. The 802.11b standard specifies the radio frequency (RF) of 2.4 GHz for both transmitting and receiving data.
- The 802.11g standard uses the same unlicensed 2.4 GHz band as 802.11b, but extends the data rates to provide greater performance by using Orthogonal Frequency Division Multiplexing (OFDM) technology.
- The 802.11a standard uses the 5 GHz band that provides more channels and improved data rates by using OFDM technology.

Radio Frequency Ranges

Wireless LAN communications uses these two radio frequency ranges:

- 2.4 GHz radio frequency range—This open RF range does not require licensing. To reduce interference within this band, WLANs transmit on non-overlapping channels, which are typically limited to three channels, although Japan uses four channels. Many devices operate in this bandwidth including cordless phones and microwave ovens; consequently, wireless communication is susceptible to interference or noise. Interference does not destroy the signal, but can impede the transmission speed and reduce an 11 Mbps signal all the way down to a 1 Mbps signal. In addition, RF interference can reduce the voice quality over the wireless network.
- 5 GHz radio frequency range—This band has been divided into several sections called Unlicensed National Information Infrastructure (UNII) bands which have four channels each. The channels were spaced at 20 MHz thereby providing non-overlapping channels. As a result, 802.11a provides more channels.

Wireless Modulation Technologies

Wireless communications uses these two methods for carrying data and signals:

- Direct-Sequence Spread Spectrum (DSSS) technology—To help prevent interference, DSSS technology was developed to spread the signal out over the frequency range or bandwidth. DSSS technology multiplexes chunks of data over several frequencies so that multiple devices can communicate without interference. Each device has a special code that it uses to identify its data packets and to ignore all others. The Cisco wireless 802.11b/g products use DSSS technology to support multiple devices on the WLAN.
- Orthogonal Frequency Division Multiplexing (OFDM) technology—OFDM is a physical layer encoding technology for transmitting signals through the RF. This method breaks one high-speed data carrier into several lower-speed carriers that transmit in parallel across the particular RF spectrum. OFDM, when used with various modulation types such as 802.11g and 802.11a, is capable of supporting data rates as high as 54 Mbps.

Table 2-1 provides a comparison of the Wi-Fi standards and their features.

Table 2-1 Comparing Wi-Fi Standards Features

Item	802.11b	802.11g	802.11a
Data Rates	1, 2, 5.5, 11 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps
Non-overlapping Channels	3 (Japan uses 4)	3 (Japan uses 4)	Up to 23
Wireless Modulation	DSSS	DSSS, OFDM	OFDM

Connecting to the Wireless Network

The critical components in the wireless network are the access points that provide the wireless links or “hot spots” to the network. Cisco requires that the access points supporting voice communications must run Cisco IOS Version 12.3(8)JA or later. Cisco IOS provides features for managing voice traffic. For more information about access points, see the [“Voice Over IP Wireless Network Configuration” section on page 2-27](#).

Each access point has a hard-wired connection to an Ethernet switch, such as a Cisco Catalyst 3750, that is configured on the LAN. The switch provides access to gateways and the Cisco Unified CallManager server to support wireless IP telephony (WIPT).

Access points transmit and receive RF signals over channels within the 2.4 GHz or 5.1 to 5.8 GHz frequency band. Regulatory domains determine the number of channels that wireless communications can use within the frequency band.

Table 2-2 lists the frequency ranges and operating channels for three regulatory domains. The Cisco Unified Wireless IP Phone 7921G has a fourth domain type (product number is CP-7921G-W) for all other regions in the world. Wireless LANs in the rest of the world will use 802.11d to inform the phone which channels and data rates to use.

An access point broadcasts on a specific channel within the available channel range. To provide a stable wireless environment and reduce channel interference, you must specify non-overlapping channels for each access point. The recommended channels for 802.11b/g in North America are channels 1, 6, and 11.

**Note**

In a non controller-based wireless network, it is recommended that you statically configure channels for each access point. If your wireless network uses a controller, you can use the Auto-RF feature with minimal voice disruption.

Table 2-2 Regulatory Domain Frequency Band and Channel Usage

Regulatory Domain	Frequency Band Range	Operating Channels
Federal Communications Commission (FCC) Product number is CP-7921G-A	2.412-2.462 GHz	11 channels
	5.15-5.25 GHz (UNII-1)	12 channels
	5.25-5.35 GHz (UNII-2)	
	5.725-5.825 (UNII-3)	
	5.470 - 5.725 (DFS)	11 channels
5.47-5.725 GHz (pending approval)		
ETSI (Europe) Product number is CP-7921G-E	2.412-2.472 GHz	13 channels (1-13)
	5.15-5.725 GHz	19 channels

Table 2-2 Regulatory Domain Frequency Band and Channel Usage

Regulatory Domain	Frequency Band Range	Operating Channels
Japan	2.412-2.472 GHz	13 channels (ODFM)
Product number is CP-7921G-P	2.412-2.484 GHz	14 channels (CCK)
	5.15-5.35 GHz	8 channels
World	Uses 802.11d to identify band ranges	Uses 802.11d to identify channels
Product number is CP-7921G-W		

The access point has a transmission range or coverage area that depends on its type of antenna and transmission power. The access point coverage range is from 500 to 1000 feet with effective isotropic radiated power (EIRP) output that scales at 1, 5, 20, and 50 mW. To provide effective coverage, access points need a range overlap of approximately 20 percent to allow uninterrupted connections as phone users roam from one access point to another.

Wireless networks use a service set identifier (SSID). The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. The SSID provides a way to group a set of user devices that can associate with a set of access points.

For more information about wireless network components and design, refer to *Cisco Enterprise Distributed Wireless Solution Reference Network Design* at http://www.cisco.com/application/pdf/en/us/guest/netso/ns178/c649/ccmigration_09186a00800d67eb.pdf.

Security for Voice Communications

Because all WLAN devices that are within range can receive all other wireless LAN traffic, securing voice communications is critical. To ensure that voice traffic is not manipulated or intercepted by intruders, the Cisco Unified Wireless IP Phone 7921G and Cisco Aironet Access Points are supported in the overall Cisco SAFE Security architecture.

To secure voice communications, wireless networks use authentication and encryption methods. Wired Equivalent Privacy (WEP) is the method that was first introduced for wireless security, but this method is easily compromised. To address the security problems and weaknesses of WEP, the Wi-Fi Alliance defined Wireless Protected Access (WPA.)

Wi-Fi Protected Access is a standards-based, interoperable security enhancement that increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages Temporal Key Integrity Protocol (TKIP) for data protection and 802.1x for authenticated key management.

Through stronger encryption algorithms, stronger authentication, and rapid key updates, WPA has significantly improved security compared to WEP. Wireless clients, such as wireless IP phones, can authenticate at either the access point or with the network by using a centralized remote authentication dial-in user service (RADIUS) server.

The Cisco Wireless IP telephony solution provides wireless network security that prevents unauthorized logins and compromised communications by using these features:

- Encryption and authentication with Wired Equivalent Privacy (WEP)
- Wireless Protected Access (WPA and WPA2)
- Extensible Authentication Protocol (EAP)
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)

For additional information about Cisco Wireless LAN Security, refer to http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.html

Related Topics

- [Networking Protocols Used with Cisco Unified Wireless IP Phones, page 2-8](#)
- [Authentication Mechanisms in the Wireless Network, page 2-19](#)

Components of the VoIP Wireless Network

The wireless IP phone must interact with several network components in the wireless local area network (WLAN) to successfully place and receive calls.

The following topics provide an overview of the network components:

- [Networking Protocols Used with Cisco Unified Wireless IP Phones, page 2-8](#)
- [Interacting with Cisco Unified Wireless Access Points, page 2-12](#)
- [Roaming in a Wireless Network, page 2-14](#)
- [Voice Quality in a Wireless Network, page 2-16](#)
- [Authentication Mechanisms in the Wireless Network, page 2-19](#)
- [Interacting with Cisco Unified CallManager, page 2-24](#)
- [Interacting with the DHCP Server, page 2-25](#)

Networking Protocols Used with Cisco Unified Wireless IP Phones

Cisco Unified IP Phones support several industry-standard and Cisco networking protocols for voice communication. [Table 2-3](#) provides an overview of the networking protocols that the Cisco Unified Wireless IP Phone 7921G supports.

Table 2-3 Supported Networking Protocols on the Cisco Unified Wireless IP Phone 7921G

Networking Protocol	Purpose	Usage Notes
Advanced Encryption Standard (AES)	Encryption standard that uses Cipher Blocking Chain (CBC) mode to IP security (IPSec).	Cisco Unified Wireless IP Phone 7921G can use AES to secure and preserve the integrity of wireless voice communications.
Cisco Centralized Key Management (CCKM)	Key generation protocol used for fast authentication in wireless networks.	Cisco Unified Wireless IP Phone 7921G can use CCKM for fast, secure roaming between access points.

Table 2-3 Supported Networking Protocols on the Cisco Unified Wireless IP Phone 7921G

Networking Protocol	Purpose	Usage Notes
Cisco Discovery Protocol (CDP)	<p>Device-discovery protocol that runs on all Cisco-manufactured equipment.</p> <p>Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.</p>	Cisco Unified IP Phones use CDP to communicate information such as auxiliary VLAN ID, per-port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Extensible Authentication Protocol (EAP)	Password-based mutual authentication scheme between the client (phone) and a RADIUS server.	Cisco Unified Wireless IP Phone 7921G can use EAP for authentication with the wireless network.
Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)	Protected Access Credential (PAC) authentication scheme between the client (phone) and an EAP-FAST RADIUS server.	Cisco Unified Wireless IP Phone 7921G can use EAP-FAST for authentication with the wireless network.
Dynamic Host Configuration Protocol (DHCP)	<p>Dynamically allocates and assigns an IP address to network devices.</p> <p>DHCP enables an IP phone to connect to the network and become operational without the administrator assigning an IP address or configuring additional network parameters.</p>	<p>DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and an TFTP server on each phone locally.</p> <p>Use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, refer to <i>Cisco Unified CallManager System Guide</i>.</p>

Table 2-3 Supported Networking Protocols on the Cisco Unified Wireless IP Phone 7921G

Networking Protocol	Purpose	Usage Notes
Internet Protocol (IP)	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, subnet, and gateway identifications are automatically assigned if you are using the Cisco Unified IP Phone with DHCP. If you are not using DHCP, you must manually assign these properties to each phone locally.
Light Extensible Authentication Protocol (LEAP)	Cisco proprietary password-based mutual authentication scheme between the client (phone) and a RADIUS server.	Cisco Unified Wireless IP Phone 7921G can use LEAP for authentication with the wireless network.
Power Save Poll (PS-Poll)	Allows the phone to be in power save mode yet receive queued packets from AP.	Cisco Unified Wireless IP Phone 7921G can use PS-Poll to preserve battery life.
Real-Time Control Protocol (RTCP)	Used with the RTP protocol to provide control over the transporting of real-time data, such as interactive voice and video, over data networks.	Cisco Unified IP Phones use the RTCP protocol to allow monitoring of the data delivery and minimal control and identification functionality.
Real-Time Transport (RTP)	Standard 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.
Skinny Client Control Protocol (SCCP)	Uses Cisco-proprietary messages to communicate between IP devices and Cisco Unified CallManager.	Cisco Unified IP Phones use SCCP protocol for VoIP call signaling and enhanced features such as Message Waiting Indication (MWI).
Temporal Key Integrity Protocol (TKIP) with message integrity check (MIC)	Encryption and data integrity protocol that encrypts data sent over the wireless LAN.	Cisco Unified Wireless IP Phone 7921G can use TKIP/MIC algorithms to secure and preserve the integrity of voice communications.

Table 2-3 Supported Networking Protocols on the Cisco Unified Wireless IP Phone 7921G

Networking Protocol	Purpose	Usage Notes
Transmission Control Protocol (TCP)	Connection-oriented transport protocol.	Cisco Unified IP Phones use TCP to connect to Cisco Unified CallManager and to access XML services.
Trivial File Transfer Protocol (TFTP)	Method for transferring files over the network. On the Cisco Unified IP Phone, TFTP enables you to obtain a configuration file specific to the phone type.	You must have a TFTP server in your network that the DHCP server automatically identifies. If more than one TFTP server is running in your network, you must manually assign a TFTP server to each phone.
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.
Unscheduled Asynchronous Power Save Delivery (U-APSD)	Allows the phone to be in power save mode yet receive queued packets from AP.	When the Cisco Unified Wireless IP Phone 7921G can use U-APSD, battery life is substantially improved.
User Datagram Protocol (UDP)	Connectionless messaging protocol for delivery of data packets.	Cisco Unified IP Phones receive and process UDP messages. RTP voice traffic runs over UDP.
Wi-Fi (802.11)	An open standard that defines wireless methods of transmitting Ethernet traffic and is commonly called Wi-Fi. This standard defines radio frequencies (RF) and data speed for wireless LAN communications.	Cisco Unified Wireless IP Phone 7921G supports the Wi-Fi standards. See Table 2-1 for more information.

Table 2-3 Supported Networking Protocols on the Cisco Unified Wireless IP Phone 7921G

Networking Protocol	Purpose	Usage Notes
Wired Equivalent Privacy (WEP)	Wireless security protocol for encrypting data that uses an encryption key stored on the phone and access point.	Cisco Unified Wireless IP Phone 7921G can use either static WEP or dynamic WEP keys for encryption, depending on the network security configuration.
Wireless Protected Access (WPA)	Provides stronger authentication, encryption key management and alternative encryption and message integrity methods.	Cisco Unified Wireless IP Phone 7921G supports WPA, WPA2, and WPA Pre-shared key authentication, including encryption using TKIP and MIC (message integrity check).

Related Topics

- [Understanding the Phone Startup Process, page 3-26](#)
- [Components of the VoIP Wireless Network, page 2-8](#)
- [Configuring DHCP Settings, page 5-8](#)

Interacting with Cisco Unified Wireless Access Points

Wireless voice devices use the same access points as wireless data devices. However, voice traffic over a WLAN requires different equipment configurations and layouts than a WLAN that is used exclusively for data traffic. Data transmission can tolerate a higher level of RF noise, packet loss, and channel contention than voice transmission. Packet loss during voice transmission can cause choppy or broken audio and make the phone call inaudible.

Wireless voice users are mobile and often roam across a campus or between floors in a building while they are connected to a call. In contrast, data users remain in one place or occasionally move to another location. The ability to roam while maintaining voice session continuity is one of the advantages of wireless voice; therefore, RF coverage needs to include areas not usually covered for data, such as stairwells, elevators, quiet corners outside conference rooms, and passage ways.

To assure good voice quality and optimal RF signal coverage, you must perform a site survey that determines settings suitable to wireless voice. The survey results provide information for the design and layout of the WLAN for voice, such as access point placement, power levels, and channel assignments.

After deploying and using wireless voice, you should continue to perform post installation site surveys. When you add a group of new users or install more equipment or stack large amounts of inventory, you are changing the wireless environment. You must verify that the access point coverage is still adequate for optimal voice communications. See the [“Site Survey Verification” section on page 2-31](#) for more information.

Associating to an Access Point

At startup, the Cisco Unified Wireless IP Phone 7921G uses its radio to scan for access points with Service Set Identifiers (SSIDs) and encryption types that it recognizes. The phone builds and maintains a list of eligible access point targets and uses the following variables to determine the best access point with which to associate.

- Received Signal Strength Indicator (RSSI)—The phone uses this value to determine the signal strength of available access points within the RF coverage area. The phone attempts to associate with the access point with the highest RSSI value.
- QoS Basic Service Set (QBSS)—The access point uses this beacon information element (IE) to send the channel utilization of the access point to the unified IP phone. The phone uses the QBSS value to determine whether the access point can effectively handle more traffic.



Note QBSS is not supported when using Wi-Fi 802.11a.

- Traffic Specification (TSpec)—The TSpec value is used to calculate call limits and WLAN load balancing. The TSpec value of each voice stream allows the system to allocate bandwidth to voice devices on a first-come, first-served basis. For more information, see [“Voice Quality in a Wireless Network” section on page 2-16](#).

The unified IP phone associates with the access point with the highest RSSI and lowest channel utilization values (QBSS) that have matching SSID and encryption types. To insure that voice traffic will be handled properly, you must configure the correct QoS in the access point. For configuration information, see [“Wireless Network Requirements for VoIP” section on page 2-27](#).

Related Topics

- [Roaming in a Wireless Network, page 2-14](#)
- [Security for Voice Communications, page 2-6](#)
- [Voice Over IP Wireless Network Configuration, page 2-27](#)

Roaming in a Wireless Network

Wireless IP phones provide communication mobility to users within the enterprise WLAN environment. Unlike cellular phones that have broad coverage, the coverage area for the unified IP phone is smaller; therefore, phone users frequently roam from one access point to another. To understand some of the limitations of roaming with wireless IP phones, these examples provide information about the WLAN environment.

- Pre-call Roaming—A wireless IP phone user powers on the phone in the office, and the phone associates with the nearby access point. The user leaves the building, moves to another building, and then places a call. The phone associates with a different access point in order to place the call from the new location. If the associated access point is within the same Layer 2 VLAN, the IP address remains the same for the phone. But, if the roaming phone crosses a Layer 3 boundary with DHCP enabled, the phone recognizes that it is no longer in the same subnet. The phone requests a new IP address before it can connect to the network and place the call.



Note If a user leaves the WLAN coverage area and then comes back into the *same* WLAN area, the phone must reconnect to the network. By pressing a key on the phone, the user activates the phone and increases the scanning rate to speed up reconnecting to the network.

- **Mid-call Roaming**—A wireless IP phone user is actively engaged in a call and moves from one building to another. The roaming event occurs when the phone moves into the range of a different access point, and then the phone authenticates and associates with the new access point. The previous access point hands the call over to the new access point while maintaining continuous audio connection without user intervention. As long as the access points are in the same Layer 2 subnet, the unified IP phone keeps the same IP address and the call continues. As a unified IP phone roams between access points, it must re-authenticate with each new access point. See the [“Authentication Mechanisms in the Wireless Network”](#) section on page 2-19 for information about authentication.

If the unified IP phone user moves from an access point that covers IP Subnet A to an access point that covers IP Subnet B, the phone no longer has an IP address or gateway that is valid within the new subnet and the call can disconnect.

- **Layer 3 Roaming**—With the release of the Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM), the Cisco Unified Wireless IP Phone 7921G now supports Layer 3 roaming for autonomous mode access points. For details about the Cisco WLSM, refer to the product documentation available at:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/wls_m_1_1/index.htm

Layer 3 roaming with lightweight mode access points is accomplished by controllers that use dynamic interface tunneling. Clients that roam across controllers and VLANs can keep their IP address when using the same SSID.

- **Fast and Secure Roaming**—Cisco Centralized Key Management (CCKM) enables authenticated client devices to roam securely from one access point to another without any perceptible delay during reassociation. With the support of CCKM protocol, the wireless IP phone is able to negotiate the handoff from one access point to another more easily. During the roaming process, the phone must scan for the nearby access points, determine which

access point can provide the best service, and then reassociate with the new access point. When implementing stronger authentication methods, such as WPA and EAP, the number of information exchanges increases and causes more delay during roaming. To avoid additional delays, use CCKM to manage authentication.

CCKM, a centralized key management protocol, provides a cache of session credentials on the wireless domain server (WDS). As the phone roams from one access point to the next, CCKM compresses the number of message exchanges during roaming by providing a master key stored on the WDS for the access point to use. The reassociation exchange is reduced to two messages, thereby reducing the roaming time.

For details about CCKM, refer to the “Cisco Fast Secure Roaming Application Note” at:

http://www.cisco.com/en/US/products/hw/wireless/ps4570/prod_technical_reference09186a00801c5223.html

**Note**

In dual band WLANs, it is possible to roam between 2.4 GHz bands (802.11b/g) and 5 GHz bands (802.11a). The phone moves out of range of one AP using one band and into the range of another that has the same SSID but is using a different band. This can cause gaps in voice communications. To avoid these communication gaps, try to use only one band for voice communications.

Related Topics

- [Voice Quality in a Wireless Network, page 2-16](#)
- [Interacting with Cisco Unified Wireless Access Points, page 2-12](#)
- [Voice Over IP Wireless Network Configuration, page 2-27](#)

Voice Quality in a Wireless Network

Voice traffic on the Wireless LAN, like data traffic, is susceptible to delay, jitter, and packet loss. These issues do not impact the data end user, but have serious implications for a voice call. To ensure that voice traffic receives timely and reliable treatment with low delay and low jitter, you must use Quality of Service (QoS), and use separate virtual LANs (VLANs) for voice and data. By isolating the voice traffic onto a separate VLAN, you can use QoS to provide priority

treatment for voice packets when traveling across the network. Also, use a separate VLAN for data traffic, not the default native VLAN which is typically used for all network devices.

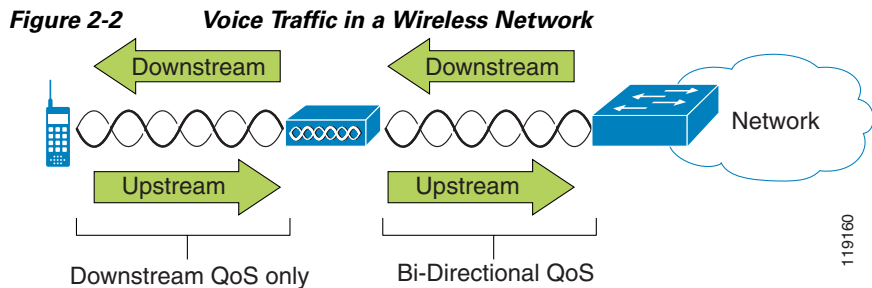
You need the following VLANs on the network switches and the access points that support voice connections on the WLAN.

- Voice VLAN—Voice traffic to and from the wireless IP phone
- Data VLAN—Data traffic to and from the wireless PC
- Native VLAN—Data traffic to and from other wireless devices

Assign separate SSIDs to the voice and to the data VLANs. If you configure a separate management VLAN in the WLAN, do not associate an SSID with the management VLAN.

By separating the phones onto a voice VLAN and marking voice packets with higher CoS, you can ensure that voice traffic gets priority treatment over data traffic resulting in lower packet delay and fewer lost packets.

Unlike wired networks with dedicated bandwidths, wireless LANs have to consider traffic direction when implementing QoS. Traffic is classified as upstream or downstream from the point of view of the access point as shown in [Figure 2-2](#).



Beginning with Cisco IOS release 12.2(11)JA, Cisco Aironet APs support the contention-based channel access mechanism called Enhanced Distributed Coordination Function (EDCF). The EDCF-type of QoS has up to eight queues for downstream (toward the 802.11b/g clients) QoS. You can allocate the queues based on these options:

- QoS or Differentiated Services Code Point (DSCP) settings for the packets
- Layer 2 or Layer 3 access lists

- VLANs for specific traffic
- Dynamic registration of devices

Although you can have up to eight queues on the access point, you should use only two queues for voice traffic to ensure the best possible voice QoS. Place voice (RTP) and signaling (SCCP) traffic in the highest priority queue, and place data traffic in a best-effort queue. Although 802.11b/g EDCF does not guarantee that voice traffic is protected from data traffic, you should get the best statistical results by using this queuing model.



Note The Cisco Unified Wireless IP Phone 7921G marks the SCCP signaling packets with a DSCP value of 24 and RTP packets with DSCP value of 46.

To improve reliability of voice transmissions in a nondeterministic environment, the Cisco Unified Wireless IP Phone 7921G supports the IEEE 802.11e industry standard and is Wi-Fi Multimedia (WMM) capable. WMM enables differentiated services for voice, video, best effort data and other traffic. However, in order for these differentiated services to provide sufficient QoS for voice packets, only a certain amount of voice bandwidth can be serviced or admitted on a channel at one time. If the network can handle “N” voice calls with reserved bandwidth, when the amount of voice traffic is increased beyond this limit, (to N+1 calls), the quality of all calls suffers.

To help address the problems of VoIP stability and roaming, an initial Call Admission Control (CAC) scheme is required. With CAC, QoS is maintained in a network overload scenario by ensuring that the number of active voice calls does not exceed the configured limits on the access point. The Cisco Unified Wireless IP Phone 7921G can integrate layer 2 TSpec admission control with layer 3 Cisco Unified CallManager admission control (RSVP). During times of network congestion, calling or called parties receive a fast busy indication. The system maintains a small bandwidth reserve so wireless phone clients can roam into a neighboring access point (AP), even when the AP is at “full capacity”. After reaching the voice bandwidth limit, the next call is load-balanced to a neighboring AP without affecting the quality of the existing calls on the channel.

Implementing Quality of Service in the connected Ethernet switch is highly desirable to maintain good voice quality. The COS and DSCP values that the Cisco Unified Wireless IP Phone 7921G sets do not need to be modified. To configure QoS correctly on the access point, see the [“Configuring the Wireless Network for Voice” section on page 2-28](#).

Related Topics

- [Authentication Mechanisms in the Wireless Network, page 2-19](#)
- [Interacting with Cisco Unified CallManager, page 2-24](#)
- [Voice Over IP Wireless Network Configuration, page 2-27](#)

Authentication Mechanisms in the Wireless Network

Before a wireless device can communicate on the network, it must authenticate with the access point or the network by using an authentication method. The wireless IP phone can use these authentication methods in the WLAN:

- **Open Authentication**—Any wireless device can request authentication in an open system. The access point that receives the request may grant authentication to any requestor or only to requestors on a list of users. Communication between the wireless device and access point could be non-encrypted or devices can use WEP keys to provide security. Devices that are using WEP only attempt to authenticate with an access point that is using WEP.
- **Shared Key Authentication**—The access point sends an unencrypted challenge text string to any device attempting to communicate with the access point. The device that is requesting authentication uses a pre-configured WEP key to encrypt the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. A device can authenticate only if its WEP key matches the WEP key on the access points.

Shared key authentication can be less secure than open authentication with WEP because someone can monitor the challenges. An intruder can calculate the WEP key by comparing the unencrypted and encrypted challenge text strings.

- **WPA Pre-Shared Key (PSK) Authentication**—The access point and the phone are configured with the same authentication key. The pre-shared key is used to create unique pair-wise keys that are exchanged between each phone and the access point. You can configure the pre-shared key as a hexadecimal or ASCII character string. Because the pre-shared key is stored on the phone, it might be compromised if the phone is lost or stolen.

- **EAP-FAST Authentication**—This client server security architecture encrypts EAP transactions within a Transport Level Security (TLS) tunnel between the access point and the Remote Authentication Dial-in User Service (RADIUS) server such as the Cisco Access Control Server (ACS).

The TLS tunnel uses Protected Access Credentials (PACs) for authentication between the client (phone) and the RADIUS server. The server sends an Authority ID (AID) to the client (phone), which in turn selects the appropriate PAC. The client (phone) returns a PAC-Opaque to the RADIUS server. The server decrypts the PAC with its master-key. Both end points now have the PAC key and a TLS tunnel is created. EAP-FAST supports automatic PAC provisioning, but you must enable it on the RADIUS server.



Note In the Cisco ACS, by default, the PAC expires in one week. If the phone has an expired PAC, authentication with the RADIUS server takes longer while the phone gets a new PAC.
To avoid these PAC provisioning delays, set the PAC expiration period to 90 days or longer on the ACS or RADIUS server.

Authenticated Key Management

The following authentication schemes use the RADIUS server to manage authentication keys:

- **Wi-Fi Protected Access (WPA)**—Uses information on a RADIUS server to derive unique pair-wise keys for authentication. Because these keys are generated at the centralized RADIUS server, WPA provides more security than WPA pre-shared keys that are stored on the access point and phone.
- **Cisco Centralized Key Management (CCKM)**—Uses information on a RADIUS server and a wireless domain server (WDS) to manage and authenticate keys. The WDS creates a cache of security credentials for CCKM-enabled client devices for fast and secure reauthentication.

With WPA and CCKM, encryption keys are not entered on the phone, but are automatically derived between the access point and phone. But the EAP username and password that are used for authentication must be entered on each phone.

Encryption Methods

To ensure that voice traffic is secure, the Cisco Unified Wireless IP Phone 7921G supports Wired Equivalent Privacy (WEP), Temporal Key Integrity Protocol (TKIP), and Advanced Encryption Standards (AES) for encryption. When using either of these mechanisms for encryption, both the signaling (SCCP) packets and voice (RTP) packets are encrypted between the access point and the unified IP phone.

- **WEP**—When using WEP in the wireless network, authentication happens at the access point by using open or shared-key authentication. The WEP key that is setup on the phone must match the WEP key that is configured at the access point for successful connections. The Cisco Unified Wireless IP Phone 7921G supports WEP keys that use 40-bit encryption or a 128-bit encryption and remain static on the phone and access point.

EAP and CCKM authentication can use WEP keys for encryption. The RADIUS server manages the WEP key and passes a unique key to the access point after authentication for encrypting all voice packets; consequently, these WEP keys can change with each authentication.

- **TKIP**—WPA and CCKM use TKIP encryption that has several improvements over WEP. TKIP provides per-packet key ciphering and longer initialization vectors (IVs) that strengthen encryption. In addition, a message integrity check (MIC) ensures that encrypted packets are not being altered. TKIP removes the predictability of WEP that helps intruders decipher the WEP key.
- **AES**—An encryption method used for WPA2 authentication. This national standard for encryption uses a symmetrical algorithm that has the same key for encryption and decryption. AES uses Cipher Blocking Chain (CBC) encryption of 128 bits in size, supporting key sizes of 128, 192 and 256 bits, as a minimum.



Note The Cisco Unified Wireless IP Phone 7921G does not support Cisco Key Integrity Protocol (CKIP) with CMIC.

Choosing Authentication and Encryption Methods

Authentication and encryption schemes are setup within the wireless LAN. VLANs are configured in the network and on the access points and specify different combinations of authentication and encryption. An SSID is associated

with a VLAN and its particular authentication and encryption scheme. In order for wireless client devices to authenticate successfully, you must configure the same SSIDs with their authentication and encryption schemes on the access points and on the unified IP phone.

Some authentication schemes require specific types of encryption. With Open authentication, you have the option to use static WEP for encryption for added security. But if you are using Shared Key authentication, you must set static WEP for encryption, and you must configure a WEP key on the phone.

When using Authenticated Key Management (AKM) for the Cisco Unified Wireless IP Phone 7921G, several choices for both authentication and encryption can be set up on the access points with different SSIDs. When the unified IP phone attempts to authenticate, it chooses the access point that advertises the authentication and encryption scheme that the phone can support. Auto (AKM) mode can authenticate by using WPA, WPA2, WPA Pre-shared key, or CCKM.

**Note**

- When using WPA Pre-shared key or WPA2 Pre-shared key, the pre-shared key must be statically set on the phone. These keys must match the keys configured on the access point.
- When using Auto (AKM), encryption options are automatically configured for WPA, WPA2, WPA Pre-shared key, WPA2 Pre-shared key, or CCKM.

For more information about configuring authentication and encryption schemes on access points, refer to the *Cisco Aironet Configuration Guide* for your model and release at this URL:

http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_installation_and_configuration_guides_list.html

Table 2-4 provides a list of authentication and encryption schemes configured on the Cisco Aironet Access Points supported by the Cisco Unified Wireless IP Phone 7921G. The table shows the network configuration option for the phone that corresponds to the access point configuration.

Table 2-4 Authentication and Encryption Schemes

Cisco Access Point Configuration			Cisco Unified Wireless IP Phone 7921G
Authentication	Key Management	Common Encryption	Authentication
Open	None	None	Open (optional)
Open (Static WEP)	None	WEP	Open+WEP
Shared key (Static WEP)	None	Static WEP	Shared Key+WEP
LEAP Open and Network EAP—can use both	Optional CCKM	WEP	LEAP
EAP-FAST Open and Network EAP—can use both	Optional CCKM	WEP	EAP-FAST
EAP-FAST with WPA Open and Network EAP—can use both	WPA/ Optional CCKM	TKIP	EAP-FAST
EAP-FAST with WPA2 Open and Network EAP—can use both	WPA	AES	EAP-FAST
WPA Open and Network EAP—can use both Optional CCKM	WPA/ Optional CCKM	TKIP	Auto (AKM) with WPA
WPA-PSK Open and Network EAP—can use both Optional CCKM	WPA	TKIP	Auto (AKM) with WPA-PSK

Table 2-4 Authentication and Encryption Schemes (continued)

Cisco Access Point Configuration			Cisco Unified Wireless IP Phone 7921G
Authentication	Key Management	Common Encryption	Authentication
WPA2 Open and Network EAP—can use both	WPA	AES	Auto (AKM) with WPA2
WPA2-PSK Open and Network EAP—can use both	WPA	AES	Auto (AKM) with WPA2-PSK

Related Topics

- [Interacting with Cisco Unified CallManager, page 2-24](#)
- [Components of the VoIP Wireless Network, page 2-8](#)
- [Voice Over IP Wireless Network Configuration, page 2-27](#)

Interacting with Cisco Unified CallManager

Cisco Unified CallManager is the call control component in the network that handles and routes calls for the wireless IP phones. Cisco Unified CallManager manages the components of the IP telephony system—the phones, access gateways, and the resources—for such features as call conferencing and route planning. When deploying Cisco Unified Wireless IP Phone 7921G, you must use Cisco Unified CallManager Release 4.1, 4.2, 5.0 or later and SCCP protocol.

Before Cisco Unified CallManager can recognize a phone, it must register with Cisco Unified CallManager and be configured in the database. For information about setting up phones in Cisco Unified CallManager, see the “[Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager](#)” section on page 1-17.

You can find more information about configuring Cisco Unified CallManager to work with the IP phones and IP devices in the *Cisco Unified CallManager Administration Guide* and *Cisco Unified CallManager System Guide*.

Related Topics

- [Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager, page 1-17](#)
- [Phone Configuration Files and Profile Files, page 2-25](#)

Phone Configuration Files and Profile Files

Configuration files for a phone define parameters for connecting to Cisco Unified CallManager and are stored on the TFTP server. In general, any time you make a change in Cisco Unified CallManager Administration that requires resetting the phone, the phone configuration file changes automatically.

Configuration files also contain information about the correct image load for the phone. If this image load differs from the one currently loaded on a phone, the phone contacts the TFTP server to request the new image file.

The phone first requests the configuration file `SEPxxxxxxxxxxxx.cnf.xml`, where each `xx` is the two-digit lowercase hexadecimal representation of each integer in the phone's MAC address. If the phone cannot find this file, it requests the configuration file `XMLDefault.cnf.xml`.

After the phone obtains the `*.cnf.xml` files, it requests a phone-specific profile file. If a phone cannot find this profile file, it requests the appropriate common profile file.

After the phone finds one of the profile files, or if it cannot find a profile file, it continues with its startup process.

Related Topic

[Understanding the Phone Startup Process, page 3-26](#)

Interacting with the DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage and automate the assignment of Internet Protocol (IP) addresses in a network. When an IP device is added to the network, it must have a unique IP address. Without DHCP, the IP address must be entered manually at each device. DHCP allocates IP addresses dynamically and reuses IP addresses when devices no longer need them.

If DHCP is enabled in the network, the Cisco Unified Wireless IP Phone 7921G uses the DHCP scope settings in the DHCP server to perform the phone provisioning bootstrap process. You must configure the settings of the DHCP server in the Cisco Unified CallManager network.

The DHCP scope settings include the following:

- TFTP servers
- DNS server IP address (optional unless using host names)
- Pool and range of the subnet mask, IP address, and gateway

The priority of the DHCP settings for the TFTP server is unique to the Cisco Unified Wireless IP Phone 7921G, as shown in [Table 2-5](#).

Table 2-5 *DHCP Settings Priority*

Priority	DHCP Settings
1st	DHCP option 150
2nd	DHCP option 66
3rd	SIADDR
4th	ciscoCM1

If DHCP is disabled, the Cisco Unified Wireless IP Phone 7921G uses the following network settings in [Table 2-6](#) to perform the phone provisioning bootstrap process. You must configure these static parameters for each Cisco Unified Wireless IP Phone 7921G.

Table 2-6 *Static IP Addresses When DHCP is Disabled*

Static Setting	Description
IP Address	IP address, the unique identifier assigned by the system administrator for the phone.
Subnet Mask	Used to partition the IP address into a network identifier and host identifier so TCP/IP can distinguish between them.
Default Router 1	Identifies the gateway that provides connectivity to the IP network beyond the subnet to which the phone belongs.

Table 2-6 *Static IP Addresses When DHCP is Disabled (continued)*

Static Setting	Description
DNS Server 1 DNS Server 2	If the system is configured to use host names for servers instead of IP addresses, identifies the primary and secondary DNS server to resolve host names.
TFTP Server 1 TFTP Server 2	Identifies the TFTP servers that the phone uses to obtain configuration files.

Voice Over IP Wireless Network Configuration

This section provides configuration guidelines for deploying wireless IP phones in the WLAN and includes these topics:

- [Wireless Network Requirements for VoIP, page 2-27](#)
- [Configuring the Wireless Network for Voice, page 2-28](#)

Wireless Network Requirements for VoIP

When configuring voice over the wireless LAN, use access points that run Cisco IOS Version 12.3(8)JA or later. Controllers should be running version 4.0 and higher with IOS Version 12.3(8)JX or later.

The Cisco Unified Wireless IP Phone 7921G supports Cisco Aironet Access Points (APs) that can run Cisco IOS in autonomous mode and APs that run in lightweight mode with lightweight access point protocol (LWAPP) and use a wireless LAN controller. [Table 2-7](#) lists the supported AP models and their operation mode in the WLAN.



Note

Voice over the wireless LAN (VoWLAN) does not currently support MESH technology such as Cisco Aironet 1500 Series Lightweight Outdoor Mesh Access Points.

Table 2-7 Supported Access Points and Modes

Access Point Models	Autonomous Mode	Lightweight Mode
Cisco Aironet 350 Series AP	Yes	No
Cisco Aironet 1100 Series AP	Yes	Yes
Cisco Aironet 1130 Series AP	Yes	Yes
Cisco Aironet 1200 Series AP	Yes	Yes
Cisco Aironet 1240 Series AP	Yes	Yes
Cisco Aironet 1300 Series AP	Yes	Yes
Cisco 1000 Series Lightweight AP	No	Yes

**Note**

Be aware that Wi-Fi compliant access points that are manufactured by third-party vendors can function with the Cisco Unified Wireless IP Phone 7921G, but might not support key features such as Dynamic Transmit Power Control (DTPC), ARP-caching, LEAP/EAP-FAST, QBSS, U-APSD, 802.11d and 802.11h.

Configuring the Wireless Network for Voice

This section identifies key access point (AP) configuration options that are required for optimal voice performance. This is not a complete list of configuration steps or options for deploying access points such as the Cisco Aironet Access Points. For more information about configuring your access point, refer to the appropriate [Cisco Aironet Access Point Installation and Configuration Guide](#) for your model or the documentation for your access point.

**Note**

When deploying the Cisco Unified Wireless IP Phone 7921G with World regulatory domain (CP-7921G-W-K9), you must enable the access points for world mode (802.11d). The world model phone gets the channels and power information from the access point.

Table 2-8 explains and provides references for many of the configuration tasks for the Cisco Aironet Access Point, controller, and Ethernet switch when setting up VoIP on the WLAN.

Table 2-8 Checklist for Wireless Network Configuration

Tasks	Explanation	Reference
1. Check that the Cisco IOS version is the recommended version	<ul style="list-style-type: none"> Under System Software, check for Cisco IOS version 12.3(8)JA or later. For the controller, use Version 4.0 and Cisco IOS version 12.3(8)JX or later. 	Interacting with Cisco Unified Wireless Access Points, page 2-12
2. Configure a VLAN for voice	To isolate voice traffic and enable QoS, you need a separate voice VLAN on the access point and network switch.	Voice Quality in a Wireless Network, page 2-16
3. Configure Service Set Identifier (SSID) for each VLAN	Identifier for a set of wireless devices to communicate with each other. Several access points can have the same SSID to support a group of wireless phones.	Interacting with Cisco Unified Wireless Access Points, page 2-12 Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA
4. Configure QoS settings for VLANs	<p>Create a QoS policy for the voice VLAN and assign a higher CoS to voice traffic.</p> <p>Enable the QoS element for wireless IP phones to provide channel utilization (QBSS) information to phones.</p>	Voice Quality in a Wireless Network, page 2-16 Configuring the Wireless Network for Voice, page 2-28 Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA
5. Enable ARP caching	Enable this option to ensure two-way audio. The access point has ARP caching disabled by default.	Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA

Table 2-8 Checklist for Wireless Network Configuration (continued)

Tasks	Explanation	Reference
6. Configure radio (802.11) settings	<p>Data Rate—Set for 11 Mbps or to the rate for the frequency band that you are using.</p> <p>Client Transmit Power—After a site survey, determine the appropriate power requirements and set a specific Client Transmit Power setting. The Cisco Unified Wireless IP Phone 7921G uses the same setting as the access point.</p> <p>Note If autonomous AP power is set for Max, the access point does not advertise Client Transmit Power (DTPC) setting.</p>	<p><i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA</i></p>
7. Configure security for the voice VLANs	<p>Use one of these authentication and encryption options for the SSID that corresponds to the voice VLAN:</p> <ul style="list-style-type: none"> • Open • Shared Key • EAP • Auto (AKM) 	<p><i>Choosing Authentication and Encryption Methods, page 2-21</i></p> <p><i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA</i></p>

Configuration Tip for Cisco Airespace Access Points

If you are using EAP-FAST with Cisco Airespace technology, you must increase the EAP request (802.1x) timeout to at least 20 seconds to ensure that the phone gets the PAC credentials successfully.

To change the request timeout on the controller, follow these steps:

Procedure

-
- | | |
|---------------|---|
| Step 1 | Use SSH or Telnet to access the Aireospace controller or controllers. |
| Step 2 | Enter <code>config advanced eap request-timeout 20</code> |
| Step 3 | Enter <code>save config</code> |
| Step 4 | Enter <code>y</code> to confirm. |
-

Site Survey Verification

After the initial deployment of wireless phones in the WLAN, it is a good practice to perform site surveys at regular intervals to verify that the APs are providing adequate coverage and that wireless phones can roam from one AP to another with no audio problems.

You should use the wireless IP phone and the Aironet Client Utility (ACU) to verify that the signal range and transmission power provide adequate coverage for roaming phones.

Use the following topics for information about performing the site survey:

- [Performing a Site Survey Verification, page 2-31](#)
- [Using the Cisco Unified Wireless IP Phone 7921G Site Survey Utility, page 2-32](#)

Performing a Site Survey Verification

Perform these tasks to verify wireless voice network operation. Check that the wireless IP phones:

1. Associate with all APs in the WLAN.
2. Authenticate with all APs in the WLAN.
3. Register with Cisco Unified CallManager.

4. Can make stationary phone calls with good quality audio.
5. Can make roaming phone calls with good quality audio and no disconnections.
6. Can place multiple calls, especially in areas designated for high density use.

After phones are installed, request that users report any problems when using their wireless IP phones.

When you perform a site survey verification and encounter problems, see the [Chapter 9, “Troubleshooting the Cisco Unified Wireless IP Phone 7921G”](#) for assistance with finding the cause of the problem.

Related Topic

[Using the Cisco Unified Wireless IP Phone 7921G Site Survey Utility, page 2-32](#)

Using the Cisco Unified Wireless IP Phone 7921G Site Survey Utility

The Cisco Unified Wireless IP Phone 7921G includes a site survey utility within the **Settings > Status** menu that provides information about the access points currently within range of the phone.

To use the Site Survey utility, follow these steps:

Procedure

-
- Step 1** Configure the Cisco Unified Wireless IP Phone 7921G with the same SSID and encryption/authentication settings as the APs.
 - Step 2** Power on the phone so that it associates with the WLAN.
 - Step 3** Choose **Settings > Status > Site Survey**.

The phone displays a list of access points within range that have the same SSID and security settings as the phone.

The display provides the following information about the APs:

SSID: abcd

Channel	BSSID	RSSI	Channel Utilization
01	19:50	-38	50
06	cf:d0	-51	38
11	7b:b0	-42	61

Step 4 To see more information about an AP, scroll to the desired line and press **Details**.

The following information appears for the specific AP:

```

SSID: abcd
Channel: 06
BSSID: 00:13:1a:16:cf:d0
RSSI: -51
CU: 38

```

Step 5 To verify the ability to roam between APs, walk through all areas where phones are used and take readings. Approach areas from different directions to assure successful roaming conditions.

Step 6 Adjust AP and antenna placement and AP power settings to provide approximately 20 percent coverage overlap.

In addition to the Site Survey utility in the Cisco Unified Wireless IP Phone 7921G, you can also use the Cisco Aironet Client Utility Site Survey Utility from a laptop PC. Refer to the section on “Performing a Site Survey” in the *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide* for your system.

Related Topic

[Performing a Site Survey Verification, page 2-31](#)



CHAPTER **3**

Setting Up the Cisco Unified Wireless IP Phone 7921G

This chapter includes the following topics, which help you install and configure the Cisco Unified Wireless IP Phone 7921G on an IP telephony network:

- [Before You Begin, page 3-1](#)
- [Installing the Cisco Unified Wireless IP Phone 7921G, page 3-10](#)
- [Understanding the Phone Startup Process, page 3-26](#)

Before You Begin

Before installing a Cisco Unified Wireless IP Phone 7921G, review the requirements in these sections:

- [Network Requirements, page 3-1](#)
- [Methods for Adding Phones to Cisco Unified CallManager, page 3-3](#)
- [Safety Information, page 3-6](#)

Network Requirements

For the Cisco Unified Wireless IP Phone 7921G to successfully operate as a Cisco Unified IP Phone endpoint, your network must support these requirements:

Voice-over-Wireless Network (VoWLAN)

- Cisco Aironet Access Points configured to support Voice over WLAN (VoWLAN)
- Controllers and switches configured to support VoWLAN
- Security implemented for authenticating wireless voice devices and users

**Note**

You must verify that your wireless network is configured properly for voice service. For more information, see the [“Performing a Site Survey Verification” section on page 2-31](#)

Voice-over-IP (VoIP) Network

- Cisco routers and gateways configured for Voice over IP (VoIP)
- One of these call control products installed and configured:
 - Cisco Unified CallManager Release 4.1, 4.2 or 5.0 and later
 - Cisco Unified CallManager Express 4.1 or later
- IP network configured to support DHCP or manual assignment of IP address, gateway, and subnet mask

Related Topics

- [Features Supported on the Cisco Unified Wireless IP Phone 7921G, page 1-5](#)
- [Understanding the Wireless LAN, page 2-1](#)
- [Methods for Adding Phones to Cisco Unified CallManager, page 3-3](#)
- [Installing the Cisco Unified Wireless IP Phone 7921G, page 3-10](#)
- [Powering On the Cisco Unified Wireless IP Phone 7921G, page 3-23](#)

Methods for Adding Phones to Cisco Unified CallManager

Before installing the wireless IP phone, you must choose a method for adding phones to the Cisco Unified CallManager database. Some methods require entering the media access control (MAC) address of the phone. [Table 3-1](#) provides an overview of these methods.

Table 3-1 *Methods for Adding Phones to the Cisco Unified CallManager Database*

Method	Requires MAC Address?	Notes
Using auto-registration	No	Results in automatic assignment of directory numbers
Using auto-registration with the Tool for Auto-Registered Phones Support (TAPS)	No	Requires auto-registration and BAT; updates information in the Cisco Unified IP Phone and in Cisco Unified CallManager Administration
Using Bulk Administration Tool (BAT)	Yes	Allows for simultaneous registration of multiple phones
Using the Cisco Unified CallManager Administration only	Yes	Requires phones to be added individually

The following sections describe these methods:

- [Adding Phones with Auto-Registration, page 3-4](#)
- [Adding Phones with Auto-Registration and TAPS, page 3-4](#)
- [Adding Phones with BAT, page 3-5](#)
- [Adding Phones with Cisco Unified CallManager Administration, page 3-6](#)

Adding Phones with Auto-Registration

You can use auto-registration to quickly enter phones into the Cisco Unified CallManager database without first gathering MAC addresses from the phones.

When auto-registration is enabled, Cisco Unified CallManager automatically assigns the next available sequential directory number to new phones as they register with Cisco Unified CallManager during the initial phone startup process.

After registering phones with Cisco Unified CallManager, you can modify settings, such as the directory numbers and device pools, by using Cisco Unified CallManager Administration.

Auto-registration is disabled by default in Cisco Unified CallManager. You must enable and properly configure auto-registration 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*.

Related Topics

- [Adding Phones with Auto-Registration and TAPS, page 3-4](#)
- [Adding Phones with BAT, page 3-5](#)
- [Adding Phones with Cisco Unified CallManager Administration, page 3-6](#)

Adding Phones with Auto-Registration and TAPS

You can add a group of phones quickly by using auto-registration and TAPS. First, use the Bulk Administration Tool (BAT) to add phones to the Cisco Unified CallManager database with dummy MAC addresses. Then use TAPS to update MAC addresses and download pre-defined configurations for the phones.

To implement TAPS, you or the end-users dial a TAPS directory number and follow voice prompts. When the process is complete, the phone has downloaded its directory number and other settings. The correct MAC address for the phone is updated in Cisco Unified CallManager Administration.

You must enable auto-registration in Cisco Unified CallManager Administration for TAPS to function.

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

Related Topics

- [Adding Phones with Auto-Registration, page 3-4](#)
- [Adding Phones with Cisco Unified CallManager Administration, page 3-6](#)
- [Adding Phones with BAT, page 3-5](#)

Adding Phones with BAT

To add a group of phones to the Cisco Unified CallManager database, you can use BAT. This plug-in application for Cisco Unified CallManager enables you to perform batch operations, including registration, on multiple phones.

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

Determining the MAC Address of a Cisco Unified IP Phone

When adding phones to the Cisco Unified CallManager database using Cisco Unified CallManager Administration or using BAT, you must enter the media access control (MAC) address of the phone. [Table 3-2](#) describes how to determine the MAC address of the wireless IP phone.

Table 3-2 *Determining the MAC Address of the Phone*

Method	For More Information
Choose Settings > Model Information > MAC Address and look at the MAC Address field.	See “Viewing Model Information” section on page 7-10
Remove the battery and look on the back of the phone.	See the “Installing or Removing the Phone Battery” section on page 3-11

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

**Note**

When using BAT to add Cisco Unified Wireless IP Phones, use the default setting for the phone load. The phone load name includes symbols (-, _, .) and BAT does not permit symbols in an entry.

Related Topics

- [Adding Phones with Auto-Registration, page 3-4](#)
- [Adding Phones with Auto-Registration and TAPS, page 3-4](#)
- [Adding Phones with Cisco Unified CallManager Administration, page 3-6](#)

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 must obtain the MAC address for each phone. See the “[Methods for Adding Phones to Cisco Unified CallManager](#)” section on page 3-3 for instructions.

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

For additional 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 3-4](#)
- [Adding Phones with Auto-Registration and TAPS, page 3-4](#)
- [Adding Phones with BAT, page 3-5](#)

Safety Information

Review the following warnings before installing the Cisco Unified IP Phone. To see translations of these warnings, refer to the [Regulatory Compliance and Safety Information for the Cisco Unified Wireless IP Phone 7921G and Peripheral Devices](#) document that accompanied this device.



Warning

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



Warning

Read the installation instructions before connecting the system to the power source. Statement 1004



Warning

This equipment will not be able to access emergency services during a power outage because of reliance on utility power for normal operation. Alternative arrangements should be made for access to emergency services. Access to emergency services can be affected by any call-barring function of this equipment.



Warning

Do not use the Cisco Unified Wireless IP Phone 7921G in hazardous environments such as areas where high levels of explosive gas may be present. Check with the site safety engineer before using any type of wireless device in such an environment.



Warning

The plug-socket combination for the battery charger must be accessible at all times, because it serves as the main disconnecting device. Statement 1019



Warning

The battery charger requires short-circuit (overcurrent) protection to be provided as part of the building installation. Install only in accordance with national and local wiring regulations. Statement 1045



Warning

The power supply must be placed indoors. Statement 331

**Warning**

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

**Warning**

Telephone receivers produce a magnetic field that can attract small magnetic objects such as pins and staples. To avoid the possibility of injury, do not place the handset where such objects may be picked up.

Battery Safety Notices

These battery safety notices apply to the batteries that are approved by the Cisco Unified Wireless IP Phone 7921G manufacturer.

**Warning**

There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions. Statement 1015

**Warning**

Do not dispose of the battery pack in fire or water. The battery may explode if placed in a fire.

**Caution**

The battery pack is intended for use only with this device.

**Caution**

Do not disassemble, crush, puncture, or incinerate the battery pack.

**Caution**

To avoid risk of fire, burns, or damage to your battery pack, do not allow a metal object to touch the battery contacts.

**Caution**

Handle a damaged or leaking battery with extreme care. If you come in contact with the electrolyte, wash the exposed area with soap and water. If the electrolyte has come in contact the eye, flush the eye with water for 15 minutes and seek medical attention.

**Caution**

Do not charge the battery pack if the ambient temperature exceeds 104 degrees Fahrenheit (40 degrees Celsius).

**Caution**

Do not expose the battery pack to high storage temperatures (above 140 degrees Fahrenheit, 60 degrees Celsius).

**Caution**

When discarding a battery pack, contact your local waste disposal provider regarding local restrictions on the disposal or recycling of batteries.

**Caution**

Use only a battery that has a Cisco part number:

Standard battery—CP-BATT-7921G-STD

Extended battery—CP-BATT-7921G-EXT

**Caution**

Use only a power supply for your geographical region with one of the following Cisco part numbers:

Australia—CP-PWR-7921G-AU

Central Europe—CP-PWR-7921G-CE

China—CP-PWR-7921G-CN

Japan—CP-PWR-7921G-JP

North America—CP-PWR-7921G-NA

United Kingdom—CP-PWR-7921G-UK

**Note**

The battery and power supply are not included with your phone. To order the battery and power supply, see your local dealer.

Related Topics

- [Network Requirements, page 3-1](#)
- [Providing Power to the Phone, page 3-10](#)

Installing the Cisco Unified Wireless IP Phone 7921G

After setting up the wireless network to support voice communications and configuring the wireless IP phones in Cisco Unified CallManager, you are ready to install the phones. This section includes the following installation information:

- [Providing Power to the Phone, page 3-10](#)
- [Configuring Wireless LAN Settings for the Cisco Unified Wireless IP Phone 7921G, page 3-20](#)
- [Using a Headset, page 3-21](#)

Providing Power to the Phone

The Cisco Unified Wireless IP Phone 7921G uses a battery for power. [Table 3-3](#) lists the types of batteries available for the wireless IP phone and the maximum talk and standby times.

Table 3-3 *Batteries Available for the Cisco Unified Wireless IP Phone 7921G*

Type	Technology	Talk Time	Standby Time
Standard	Lithium ion	Up to 10 hr	Up to 80 hr
Extended	Lithium ion	Up to 12 hr	Up to 100 hr

Table 3-4 shows the charging time for the two types of batteries. You can stop charging the battery when the battery is fully charged, and leave the batteries in the charger with no ill effects. Lithium ion batteries can be partially charged without shortening the battery life. Batteries should handle up to 4000 recharges.

Table 3-4 Battery Charging Time Information

Battery Type	Power Supply Connected to Phone	Phone Connected to PC with USB Cable	Power Supply with Desktop Charger
Standard	2 hours	5 hours	2 hours
Extended	3 hours	7 hours	3 hours

The following sections provide information about the battery and charging the phone:

- [Installing or Removing the Phone Battery, page 3-11](#)
- [Using the Power Supply to Charge the Phone, page 3-12](#)
- [Using the USB Cable to Charge the Phone, page 3-15](#)
- [Installing and Using the Desktop Charger, page 3-17](#)

Installing or Removing the Phone Battery

To install the battery in the Cisco Unified Wireless IP Phone use [Figure 3-1](#), and follow these steps:

Procedure

-
- Step 1** To install the battery, insert the battery catches (as shown in [Figure 3-1](#)) in the corresponding slots at the bottom of the Cisco Unified Wireless IP Phone 7921G. Make sure that the metal contacts on the battery and the phone are facing each other.
- Step 2** Press the battery to the body of the phone until it locks into place.
- Step 3** To remove the battery, press up on the locking catch, then lift and remove the battery.
-

Figure 3-1 Cisco Unified Wireless IP Phone 7921G Battery Installation

1	Locking catch	3	Metal contacts
2	Battery catches		

**Note**

The media access control (MAC) address for each Cisco Unified Wireless IP Phone 7921G appears on a printed label on the back of the phone underneath the battery.

Using the Power Supply to Charge the Phone

To charge the battery in your phone quickly, you can use the power supply. You must assemble the appropriate AC adapter plug and then connect the power supply.

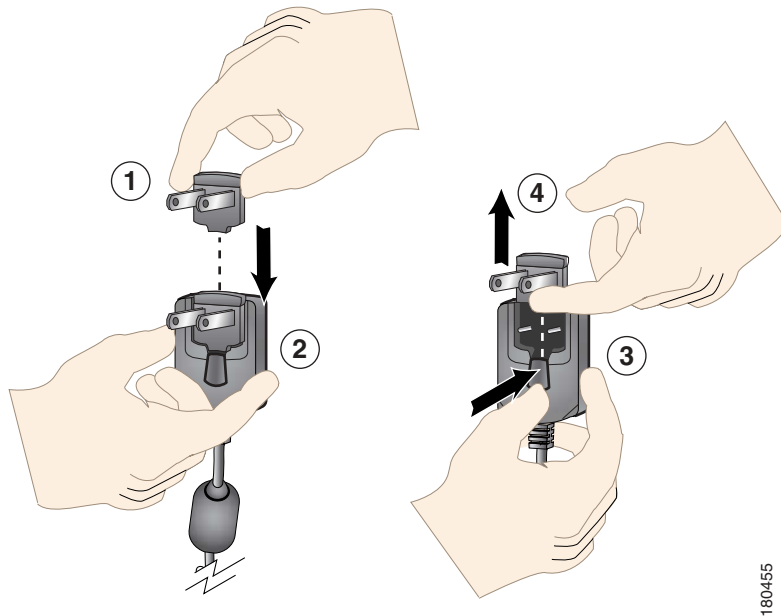
Assembling or Removing the AC Plug Adapter

To assemble or remove the AC plug adapter for the power supply, use [Figure 3-2](#), and follow these steps:

Procedure

-
- Step 1** Insert AC plug adapter (as shown in [Figure 3-2](#)) in slot on the power supply.
 - Step 2** Push AC plug adapter securely into place.
 - Step 3** To remove AC plug adapter, press on locking button.
 - Step 4** Pull AC plug adapter out of slot on power supply.
-

Figure 3-2 Assembling and Removing the AC Plug Adapter



180455

1	AC plug adapter	3	Battery release button
2	Power supply	4	AC plug adapter removal

Charging the Phone Using the Power Supply

After assembling the power supply, you are ready to charge your Cisco Unified Wireless IP Phone 7921G. You can use the phone while the battery is being charged. For charging times, see [Table 3-5](#).

To charge the Lithium ion battery using the power supply, follow these steps:

Procedure

- Step 1** Connect the cable from the power supply to the outlet in the phone as shown in [Figure 3-3](#).
 - Step 2** Connect the power supply to an AC outlet.
 - Step 3** Monitor the indicator light. While the battery is charging the light is red, and turns green when the battery is fully charged.
 - Step 4** When the battery is charged, you can disconnect the power supply from the phone, and unplug the power cord from the AC outlet.
-

Figure 3-3 Charging the Phone Using the Power Supply



1	AC plug adapter
2	AC power supply
3	Phone connector on AC power supply cable
4	Indicator light (LED)

Using the USB Cable to Charge the Phone

You can charge the phone by using a USB cable connected to a USB port on your PC. Charging times are longer when you use the USB cable. See [Table 3-4](#) for charging times.

Figure 3-4 Charging the Phone Using a USB Cable Connected to a PC



180350

1	Phone connection—Insert into slot at bottom of phone.
2	USB connector—Insert into USB port on PC.
3	Indicator LED—Indicates the charging status.

**Note**

When you plug the phone into the USB port, the Found New Hardware Wizard appears. Use the following steps to avoid this pop-up window every time you use the USB cable with your phone.

To turn off the Found New Hardware Wizard when using the USB cable to charge the phone, follow these steps:

Procedure

- Step 1** Plug the USB cable into the Cisco Unified Wireless IP Phone 7921G.
- Step 2** Plug the USB connector into the USB port on your PC.
The Found New Hardware Wizard dialog opens.
- Step 3** To turn off the wizard, for Update New Software, click **No, not this time**.
- Step 4** Next, click the button next to **Install the Software automatically (Recommended)**.
- Step 5** After a time delay, the Cannot Install This Hardware dialog box appears. Click **Don't prompt me again to install this software**.
- Step 6** Click **Finish** to close the dialog box.
The phone briefly displays “USB Connected” on the status line.
While the battery is charging, the indicator light is red.
- Step 7** When the battery is fully charged, the indicator light turns green. You can disconnect the USB cable from the phone, and unplug the cable from the PC.
-

Installing and Using the Desktop Charger

The desktop charger can charge both the phone battery installed in the phone and a spare battery at the same time. You can place the phone in the desktop charger to use the speakerphone capability while charging the phone and battery. For information about using the desktop charger speakerphone, refer to the “Using a Handset, Headset, and Speakerphone” in the *Cisco Unified Wireless IP Phone 7921G Guide*.

To identify the desktop charger components and how to set up the desktop charger, use [Figure 3-5](#).

Figure 3-5 Desktop Charger Assembly and Components



1	Power connector—Plugs into the back of the charger	6	Speaker—For speakerphone mode
2	AC power supply—Plugs into wall outlet	7	Microphone—Single-direction, internal microphone for speakerphone mode
3	Upper compartment—For charging the phone	8	Lock hole—For inserting a cable lock
4	Battery LED indicator—Red light indicates battery is charging; green light indicates battery is fully charged	9	USB connector—For B-type USB connector on cable that connects the phone to a computer
5	Power LED indicator—Green light indicates desktop charger has power	10	Lower slot—For charging the battery

Using the Desktop Charger to Charge the Phone

To use the desktop charger to charge the phone and spare battery, follow these steps:

Procedure

-
- Step 1** Plug the AC adapter into an AC outlet, and insert the connector into the back of the desktop charger.
- Step 2** Insert the Cisco Unified Wireless IP Phone 7921G into the upper compartment of the charger.
- Step 3** Insert the spare battery into the lower compartment.



Note You can insert and charge both the phone and the spare battery at the same time or you can charge them separately.

- Step 4** Check the LED indicator on the phone for charging status. The battery LED on the desktop charger provides charging status for the spare battery.

[Table 3-5](#) gives the battery charging time information.

Battery Charging Times Using the Desktop Charger

The LED indicator on the phone turns green and the phone beeps when the phone battery is charged. The battery LED indicator on the desktop charger turns green when the spare battery is charged. Batteries will stop charging after they are fully charged. You can leave the phone or battery in the charger for extended periods of time with no problems.

[Table 3-5](#) lists the approximate battery charging times when using the desktop charger.

Table 3-5 *Battery Charging Times and Configurations for the Desktop Charger*

Battery Charging Configuration	Approximate Charging Times
Spare battery alone	2 hours
Phone with battery	2 hours
Phone with battery and spare battery	2-3 hours

Related Topics

- [Powering On the Cisco Unified Wireless IP Phone 7921G, page 3-23](#)
- [Installing or Removing the Phone Battery, page 3-11](#)
- [Using the Power Supply to Charge the Phone, page 3-12](#)

Configuring Wireless LAN Settings for the Cisco Unified Wireless IP Phone 7921G

Before the phone can connect to the WLAN, you must configure the network profile for the phone with the WLAN settings. You can use two methods for setting up the network profiles:

- [Cisco Unified Wireless IP Phone 7921G Web Pages, page 3-21](#)
- [Network Profile Menu on the Cisco Unified Wireless IP Phone 7921G, page 3-21](#)

Cisco Unified Wireless IP Phone 7921G Web Pages

You can access the Cisco Unified Wireless IP Phone 7921G web pages to set up the WLAN settings in the network profile. For a new phone with the factory default settings, you must use the USB cable to connect the phone to your PC. For more information and instructions, see [Chapter 4, “Using the Cisco Unified Wireless IP Phone 7921G Web Pages.”](#)

Network Profile Menu on the Cisco Unified Wireless IP Phone 7921G

You can use the Settings menu on the phone and access the Network Profiles menu to set up the network configuration and the WLAN configuration. For more information and instructions, see [Chapter 5, “Configuring Settings on the Cisco Unified Wireless IP Phone 7921G.”](#)

Using a Headset

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

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

Cisco Systems recommends the use of good quality external devices, like headsets that are screened against unwanted radio frequency (RF) and audio frequency (AF) signals. Depending on the quality of these devices and their proximity to other devices such as cell phones and two-way radios, some audio noise may still occur. See the [“Using External Devices with Your Cisco Unified IP Phone” section on page 3-22](#) for more information.

The primary reason that support of a headset would be inappropriate for an installation is the potential for an audible hum. This hum can either be heard by the remote party or by both the remote party and the Cisco Unified IP Phone user.

Some potential humming or buzzing sounds can be caused by a range of outside sources, for example, electric lights, being near electric motors, large PC monitors. See the “[Safety Information](#)” section on page 3-6 for more information.

Audio Quality Subjective to the User

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

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

<http://www.plantronics.com>

<http://www.jabra.com>

Connecting a Headset

To connect a headset to the Cisco Unified Wireless IP Phone 7921G, plug it into the headset port on the right side of the phone.

You can use the headset with all of the features on the Cisco Unified Wireless IP Phone 7921G, including the Volume and Mute buttons. Use these buttons to adjust the ear piece volume and to mute the speech path from the headset microphone.

Using External Devices with Your Cisco Unified IP Phone

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

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

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

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

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

**Caution**

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

Powering On the Cisco Unified Wireless IP Phone 7921G

After charging the battery and configuring the wireless IP phone, you are ready to power on the phone and connect to the WLAN. Use the following sections for more information about starting up the phone:

- [Active and Standby Phone Modes, page 3-25](#)
- [Understanding the Phone Startup Process, page 3-26](#)

To power on the Cisco Unified Wireless IP Phone 7921G, press and hold the Power On button until the phone begins its startup process by cycling through these steps:

1. The phone displays the Cisco Systems screen.

2. The phone screen displays these messages as the phone starts up:
 - Locating Network Services
 - Configuring IP
 - Network Up
 - Configuring CMList
 - Registering
3. The following information displays on the main phone screen:
 - Current time and date
 - Primary directory number
 - Main screen icons for four menus and Help
 - “Your current options” on status line
 - Softkey labels (Messages and Options)

When the phone passes through these stages with no errors, the phone started up properly. Now the phone is in standby mode and is ready to place or receive calls.

The signal icon in the upper left corner shows the strength of the signal between the wireless access point and the phone. The phone must have an adequate signal to successfully place or receive calls. If the signal icon displays only one bar, the weak signal can cause problems with phone performance.

**Note**

The status message, “Leaving Service Area” indicates that the phone is not receiving a strong signal.

If the phone does not complete these steps successfully, see the [“Resolving Startup and Connectivity Problems”](#) section on page 9-1.

Related Topics

- [Active and Standby Phone Modes](#), page 3-25
- [Understanding the Phone Startup Process](#), page 3-26

Active and Standby Phone Modes

When the Cisco Unified Wireless IP Phone 7921G is powered on, it can be in one of these two modes:

- Active mode
- Standby mode

Active mode

The phone is in active mode when there is an active RTP stream. When the phone is performing one of these actions, it is consuming power:

- Connected to an active call
- Scanning for channels
- Sending CDP packets
- Sending keep-alive messages
- Reregistering with Cisco Unified CallManager

The standard battery provides up to 10 hours of talk time in active mode and the extended battery provides up to 12 hours of talk time.

Standby mode

The phone goes into standby mode two seconds after a scan is complete.

The phone will awake from standby mode in response to these events:

- Pressing keys on the keypad
- Roaming between APs
- Power cycling the phone
- Losing network connectivity
- Losing RF connectivity
- Transmitting scheduled CDP or keep-alive packets.

The standard battery provides up to 80 hours of standby time and the extended battery provides up to 100 hours of standby time.

Related Topics

- [Understanding the Phone Startup Process, page 3-26](#)
- [Resolving Startup and Connectivity Problems, page 9-1](#)

Understanding the Phone Startup Process

When connecting to the wireless VoIP network, the Cisco Unified Wireless IP Phone 7921G goes through a standard startup process, as described in [Table 3-6](#). Depending on your specific network configuration, not all of these steps may occur on your unified IP phone.

Table 3-6 Cisco Unified Wireless IP Phone Startup Process

Step	Description	Related Topics
1. Powering on the phone	The Cisco Unified Wireless IP Phone 7921G 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.	Providing Power to the Phone, page 3-10 Resolving Startup and Connectivity Problems, page 9-1

Table 3-6 Cisco Unified Wireless IP Phone Startup Process (continued)

Step	Description	Related Topics
2. Scanning for an access point	<p>The Cisco Unified Wireless IP Phone 7921G scans the RF coverage area with its radio. The phone searches its network profiles and scans for access points that have a matching SSID and authentication type. The phone associates with the access point with the highest RSSI that matches with its network profile.</p>	<p>Interacting with Cisco Unified Wireless Access Points, page 2-12</p> <p>Resolving Startup and Connectivity Problems, page 9-1</p>
3. Authenticating with access point	<p>The Cisco Unified Wireless IP Phone 7921G begins the authenticating process.</p> <ul style="list-style-type: none"> • If set for Open, then any device can authenticate to the access point. For added security, static WEP encryption might optionally be used. • If set to Shared Key, the phone encrypts the challenge text using the WEP key and the access point must verify that the WEP key was used to encrypt the challenge text before network access is available. • If set for LEAP or EAP-FAST, then the user name and password are authenticated by the RADIUS server before network access is available. • If set for Auto (AKM), the phone looks for an access point with one of the following key management options enabled: <ul style="list-style-type: none"> – WPA, WPA2, or CCKM—The username and password are authenticated by the RADIUS server before network access is available. – WPA-Pre-shared key, WPA2-Pre-shared key—The phone authenticates with the access point using the pre-shared key. 	<p>Authentication Mechanisms in the Wireless Network, page 2-19</p>

Table 3-6 Cisco Unified Wireless IP Phone Startup Process (continued)

Step	Description	Related Topics
4. Configuring IP network	<p>If the 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 a static IP address to each phone locally.</p> <p>In addition to assigning an IP address, the DHCP server directs the unified IP phone to a TFTP server. If the phone has a statically defined IP address, you must configure the TFTP server IP address locally on the phone; the phone then contacts the TFTP server directly.</p>	<ul style="list-style-type: none"> • Configuring DHCP Settings, page 5-8 • Disabling DHCP, page 5-8 • Resolving Startup and Connectivity Problems, page 9-1
5. Downloading Load ID	<p>The unified IP phone checks to verify that the proper firmware is installed or if new firmware is available to download.</p> <p>Cisco Unified CallManager informs devices using .cnf or .cnf.xml format configuration files of their load ID. Devices using .xml format configuration files receive the load ID in the configuration file.</p>	<ul style="list-style-type: none"> • Phone Configuration Files and Profile Files, page 2-25
6. Downloading config file	<p>The TFTP server has configuration files and profile files. A configuration file includes parameters for connecting to Cisco Unified CallManager and information about which image load a phone should be running. A profile file contains various parameters and values for phone and network settings.</p>	<ul style="list-style-type: none"> • Configuring an Alternate TFTP Server, page 5-10 • Phone Configuration Files and Profile Files, page 2-25 • Resolving Startup and Connectivity Problems, page 9-1

Table 3-6 Cisco Unified Wireless IP Phone Startup Process (continued)

Step	Description	Related Topics
7. Connecting to Cisco Unified CallManager	The configuration file defines how the Cisco Unified IP Phone communicates with Cisco Unified CallManager. After obtaining the file from the TFTP server, the phone attempts to make a TCP connection to the highest priority Cisco Unified CallManager on the list.	<ul style="list-style-type: none"> • Interacting with Cisco Unified CallManager, page 2-24 • Resolving Startup and Connectivity Problems, page 9-1
8. Registering to Cisco Unified CallManager	If the phone was manually added to the database, Cisco Unified CallManager identifies and registers 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.	<ul style="list-style-type: none"> • Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager, page 1-17 • Adding Users to Cisco Unified CallManager, page 6-22

Related Topics

- [Configuring Cisco Unified Wireless IP Phones in Cisco Unified CallManager, page 6-2](#)
- [Phone Configuration Files and Profile Files, page 2-25](#)



CHAPTER 4

Using the Cisco Unified Wireless IP Phone 7921G Web Pages

You can use the Cisco Unified Wireless IP Phone 7921G web pages to setup and configure these settings for the phone:

- Network Profiles that include WLAN settings
- USB port settings
- Trace settings

This chapter describes how to set up your PC to initially configure a Cisco Unified Wireless IP Phone 7921G through a USB connection and how to remotely access a configured phone over the WLAN.

After you have initially configured phones, you can make adjustments to network settings on the phone by using the Settings menu and Network Profile menu options. For more information, see [Chapter 5, “Configuring Settings on the Cisco Unified Wireless IP Phone 7921G.”](#)

This chapter includes these topics:

- [Using the USB Connection for Initial Phone Configuration, page 4-2](#)
- [Updating Phones Remotely, page 4-6](#)
- [Configuring Network Profiles, page 4-10](#)
- [Configuring USB Settings, page 4-25](#)
- [Configuring Trace Settings, page 4-27](#)
- [Using System Settings, page 4-29](#)

Using the USB Connection for Initial Phone Configuration

To setup new phones for deployment to users, use your PC to enter the initial configuration for the wireless network settings and network profiles. To save time during initial deployment, you can create a standard network profile template and export it to several phones. For more information, see the [“Backup Settings for Phone Configuration”](#) section on page 4-30.

See these sections for information about initial phone configuration:

- [Setting Up Your PC to Configure the Cisco Unified Wireless IP Phone 7921G](#), page 4-2
- [Accessing the Phone Web Page](#), page 4-5
- [Setting Configuration Privileges for the Phone Web Page](#), page 4-7
- [Accessing the Configuration Web Page for a Phone](#), page 4-7

Setting Up Your PC to Configure the Cisco Unified Wireless IP Phone 7921G

Before you can configure phones using the USB connection, you must install drivers and set up the USB ports on the phone and PC.

To interface with the phone and web pages using the USB cable, the PC must run one of these operating systems:

- Windows 2000 Professional
- Windows XP

These sections provide information about setting up your PC:

- [Installing the USB Drivers](#), page 4-3
- [Configuring the USB LAN on the PC](#), page 4-4
- [Using the USB Cable to Configure Phones](#), page 4-6

Installing the USB Drivers

To install the drivers on your PC, follow these steps:

Procedure

- Step 1** Download the installation package and “read me” file for the USB drivers from this location:

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



Note Before proceeding, review the “read me” file for specific instructions for your PC operating system.

- Step 2** Double-click on the **USB-Install-7921.1-0-1.exe** file to start the installation program.

- Step 3** Follow the prompts in the InstallShield Wizard.



Note If you receive a Hardware Installation warning message stating that the software has not passed Microsoft Windows Logo testing, click **Continue**.

- Step 4** The driver installation is complete when you see the Finished screen. You can close the wizard.

- Step 5** Plug the USB cable into the USB port on the PC and into the USB connector on the phone.

The Found New Hardware Wizard dialog opens.

- Step 6** To update the new software, click the button next to **Yes, this time only** and click **Next**.

- Step 7** Click the button next to **Install the Software automatically (Recommended)**.

After 2-3 minutes, the software installs and a message appears on the task bar stating “Found New Hardware - Software installed and ready to use.”

- Step 8** Click **Finish** when the installation is complete.

The phone briefly displays “USB Connected” on the status line.

Configuring the USB LAN on the PC

To configure the USB LAN connection on your PC, follow these steps:

Procedure

- Step 1** To setup the USB LAN connection, do one of the following:
- For Windows XP—Click **Start > Control Panel > Network Connections**.
 - For Windows 2000—Click **Start > Settings > Control Panel > Network and Dial Up Connections**.
- Step 2** Locate and double-click the new LAN connection to open the Local Area Connection Status window, then click **Properties**.
- Step 3** Scroll to the **Internet Protocol (TCP/IP)** component and click **Properties**.
- Step 4** In the Internet Protocol (TCP/IP) Properties window, choose **Use the following IP address**:
- Step 5** In the IP address field, enter a static IP address for the PC: **192.168.1. (1-254** -except 100), for example: *192.168.1.11*



Note

- By default, the Cisco Unified Wireless IP Phone 7921G is configured with 192.168.1.100 so you cannot use this IP address for the PC.
 - Make sure to use an IP address that is not in use on any other interface on the PC.
-

- Step 6** Enter the subnet mask: **255.255.255.0**
- Step 7** Click **OK** to make the changes.
-

Related Topics

- [Accessing the Phone Web Page, page 4-5](#)

- [Setting Configuration Privileges for the Phone Web Page, page 4-7](#)
- [Accessing the Configuration Web Page for a Phone, page 4-7](#)

Accessing the Phone Web Page

After setting up the USB interface on the PC, you are ready to use the USB cable connection to the phone.

To access the phone web page, follow these steps:

Procedure

- Step 1** Open a Windows browser.
- Step 2** In the address field, enter **https://192.168.1.100** to locate the wireless IP phone web page.



Note When the Security Alert dialog box displays a notice to accept the Trust Certificate, click **Yes** or **Always** to accept the application.

The Summary web page for the phone displays. See [Table 4-1](#) for details about this web page.

- Step 3** Use the hyperlinks in the left column of the web page to configure settings for the phones. For information, see these sections:
- [Configuring Network Profiles, page 4-10](#)
 - [Configuring IP Network Settings, page 4-21](#)
 - [Configuring USB Settings, page 4-25](#)
 - [Viewing Trace Logs, page 4-30](#)
 - [Using System Settings, page 4-29](#)
- Step 4** After entering the new settings, disconnect the USB cable from the phone. The settings are active immediately.
- Step 5** Check that the phone can access the network successfully.
-

Using the USB Cable to Configure Phones

You are ready to use the USB cable to set up other phones. Before plugging the USB cable into another phone, wait approximately 12-15 seconds for the USB interface on the PC to shut down.

To connect to another phone, follow these steps:

Procedure

- Step 1** Plug the USB cable into a Cisco Unified Wireless IP Phone 7921G.
The phone briefly displays “USB Connected” on the status line.
- Step 2** Access the web page for the new phone by following the steps in [“Accessing the Phone Web Page”](#) section on page 4-5.
-

Related Topics

- [Installing the USB Drivers, page 4-3](#)
- [Configuring the USB LAN on the PC, page 4-4](#)
- [Using the USB Cable to Configure Phones, page 4-6](#)
- [Accessing the Phone Web Page, page 4-5](#)

Updating Phones Remotely

You might have to update settings on a Cisco Unified Wireless IP Phone 7921G that is already configured and in use. You can use the wireless LAN to remotely access and configure these phones.

Use these sections for information about remotely updating phones:

- [Setting Configuration Privileges for the Phone Web Page, page 4-7](#)
- [Accessing the Configuration Web Page for a Phone, page 4-7](#)

Setting Configuration Privileges for the Phone Web Page

To make changes to the phone by using the web page, you must use Cisco Unified CallManager Administration to change **Web Access**.

To allow configuration privileges, follow these steps:

Procedure

- Step 1** Log into Cisco Unified CallManager Administration.
 - Step 2** Search for the phone in Cisco Unified CallManager by choosing **Devices > Phones** and enter search information such as the directory number.
 - Step 3** Open the Phone Configuration page and scroll down to Product Specific Configuration.
 - Step 4** In the **Web Access** field, click the drop-down arrow and select **Full**.
 - Step 5** Click **Update** to make the change.
 - Step 6** You must reset the phone to enable configuration privileges on the web pages for this phone.
-

Accessing the Configuration Web Page for a Phone

You can access the web page for any Cisco Unified Wireless IP Phone 7921G that is connected to the WLAN. Be sure the phone is powered on and connected.

To access the web page for the Cisco Unified Wireless IP Phone 7921G follow these steps:

Procedure

- Step 1** Obtain the IP address of the Cisco Unified Wireless IP Phone 7921G using one of these methods:
 - Search for the phone in Cisco Unified CallManager by choosing **Devices > Phones**. Phones registered with Cisco Unified CallManager display the IP address on the Find and List Phones web page and at the top of the Phone Configuration web page.

- On the Cisco Unified Wireless IP Phone 7921G, press **Settings > Device Information > 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:

https://<IP_address>



Note When the Security Alert dialog box displays a notice to accept the Trust Certificate, click **Yes** or **Always** to accept the application.

Step 3 Log in to the web pages with username: **admin** and enter the password: **Cisco** for the phone web pages.

The Summary web page for the phone displays. See [Table 4-1](#) for details about this web page.

Step 4 Make changes to configurable pages as needed. For information, see these sections:

- [Configuring Network Profiles, page 4-10](#)
- [Configuring USB Settings, page 4-25](#)
- [Configuring Trace Settings, page 4-27](#)
- [Using System Settings, page 4-29](#)

Step 5 Return to the Phone Configuration web page in Cisco Unified CallManager Administration and set the Web Access field back to **ReadOnly** or **Disabled**.

Step 6 Reset the phone from Cisco Unified CallManager to disable full access to the web pages.

Be sure to change the Web Access privileges and reset the phone to prevent users from making configuration changes on the phone web pages.



Note If a wireless IP phone was previously registered to Cisco Unified CallManager Release 4.x, and then registers to Cisco Unified CallManager 5.x, the Phone Configuration web page password might be reset to “Cisco.”

Summary Information Web Page

The Summary Information area on a phone's web page displays device settings and related information for the phone. [Table 4-1](#) describes these items.

Table 4-1 Summary Information Area Items

Item	Description
Phone DN	Directory number assigned to this phone
Wireless Information	
Active Network Profile	Name of the profile that the phone is currently using
SSID	SSID that the phone is currently using
Access Point	Name of the access point to which the phone is associated
MAC Address	Media Access Control (MAC) address of the phone
Network Information	
IP Address	Internet Protocol (IP) address of the phone
Subnet Mask	Subnet mask used by the phone
Default Router	IP address for the default gateway that the phone is using
TFTP Server	IP address for the Primary Trivial File Transfer Protocol (TFTP) server that the phone is using
CallManager Information	
Active CallManager	IP address for the Cisco Unified CallManager server to which the phone is registered
Directory Number	Primary directory number for the phone

Related Topics

- [Accessing the Phone Web Page, page 4-5](#)
- [Configuring Network Profiles, page 4-10](#)
- [Configuring USB Settings, page 4-25](#)

- [Configuring Trace Settings, page 4-27](#)
- [Using System Settings, page 4-29](#)

Configuring Network Profiles

You can configure up to four different profiles for a phone to take advantage of different WLAN environments. You can add names to the profiles and enable one or more of the profiles for the phone to use. The Network Profiles area displays this information about each profile:

- Enabled Profile—A check mark designates an enabled profile
- Name—Lists the name for the profile
- SSID—Lists the SSID used by this profile
- Status—Identifies which profile the phone is using

To display the Network Profiles list, access the web page for the phone as described in the “[Accessing the Phone Web Page](#)” section on [page 4-5](#), and then click the **Network Profiles** hyperlink.

For more information about configuring network profiles, see these sections:

- [Network Profile Settings, page 4-10](#)
- [Configuring Wireless Settings in a Network Profile, page 4-15](#)
- [Setting the Wireless LAN Security Mode, page 4-16](#)
- [Setting the Wireless Security Credentials, page 4-18](#)
- [Setting Wireless Encryption, page 4-20](#)
- [Configuring IP Network Settings, page 4-21](#)
- [Configuring the Alternate TFTP Server, page 4-23](#)
- [Configuring Advanced Settings, page 4-24](#)

Network Profile Settings

You can configure the settings for a profile by using this web page area. You can also modify or view configured profiles from this web page area. [Table 4-2](#) describes these items and provides references for more information.

To display Network Profile(1-4) Settings, access the web page for the phone as described in the “[Accessing the Phone Web Page](#)” section on page 4-5, and then click the **Profile (1-4)** hyperlink.

Table 4-2 Network Profile Settings Items

Item	Description	For More Information, See...
Wireless Settings		
Profile Name	Provides a name for the profile to make it easy to identify; up to 63 alphanumeric characters.	Configuring Wireless Settings in a Network Profile, page 4-15
SSID	Assigns the Service Set Identifier (SSID) to this profile. You must assign the same SSID to the phone that is also assigned to access points in the wireless network.	Connecting to the Wireless Network, page 2-4
Single Access Point	Determines scanning frequency: True—Minimizes the scanning for APs False—Frequent scanning of all access points within range for best match	Roaming in a Wireless Network, page 2-14
Call Power Save Mode	Set for the type of power saving mode used in the WLAN. Options are: <ul style="list-style-type: none"> • U-APSD/PS-Poll • None 	The 802.11 Standards for Wireless LAN Communications, page 2-3
802.11 Mode	Determines the signal mode or priority for selecting signal modes available in the WLAN. Options are: <ul style="list-style-type: none"> • 802.11 b/g—Use only 2.4 GHz band • 802.11a—Use only 5 GHz band • Auto, 802.11b/g preferred over 802.11a (dual band) • Auto, 802.11a preferred over 802.11b/g (dual band) • Auto, signal strength (RSSI)—Use strongest signal in dual band environment 	The 802.11 Standards for Wireless LAN Communications, page 2-3

Table 4-2 Network Profile Settings Items (continued)

Item	Description	For More Information, See...
WLAN Security Mode		
Authentication Method	Sets the authentication and encryption methods for this profile: <ul style="list-style-type: none"> • Open—Open access to APs • Open+WEP—Open access with WEP encryption (requires an encryption key) • Shared+WEP—Shared key authentication with WEP (requires an encryption key) • LEAP—Cisco proprietary authentication and encryption using a RADIUS server (requires a username and password) • EAP-FAST—Authentication and encryption using TLS and RADIUS server (requires a username and password) • Auto (AKM)—Automatic authenticated key management using: <ul style="list-style-type: none"> – WPA, WPA2 (requires a username and password) – WPA-Pre-shared key, WPA2-Pre-shared key (requires a passphrase/pre-shared key) – CCKM (requires a username and password) 	Setting the Wireless LAN Security Mode, page 4-16
Export Security Credentials	Controls whether the wireless security credential data can be exported in the configuration file. <ul style="list-style-type: none"> • True—Allows exporting the data • False—Blocks exporting the data 	Backup Settings for Phone Configuration, page 4-30

Table 4-2 Network Profile Settings Items (continued)

Item	Description	For More Information, See...
Wireless Security Credentials	Required for LEAP, EAP-FAST, and Auto (AKM) authentication methods	
Username	Assigns the network authentication username for this profile	Configuring the Username and Password, page 4-18
Password	Assigns the network authentication password for this profile	
WPA Pre-shared Key Credentials	Sets the Pre-shared key for this profile	
Pre-shared Key Type	Determines the key type: Hex or ASCII	Configuring the Pre-shared Key, page 4-19
Pre-shared Key	Identifies the key	
Wireless Encryption	Required for Open+WEP and Shared+WEP authentication methods	
Key Type	Determines the encryption key type: Hex or ASCII	Setting Wireless Encryption, page 4-20
Encryption Key 1-4	Identifies the Transmit Key: <ul style="list-style-type: none"> • Encryption Key character string • Key Size of 40 or 128 characters 	
IP Network Configuration		
Obtain IP address and DNS servers automatically	Enables DHCP	Configuring IP Network Settings, page 4-21
Use the following IP address and DNS servers	Disables DHCP and uses these static settings: <ul style="list-style-type: none"> • IP Address • Subnet Mask • Default Router • Primary DNS • Secondary DNS • Domain Name 	

Table 4-2 Network Profile Settings Items (continued)

Item	Description	For More Information, See...
TFTP		
Obtain TFTP servers automatically	Determines whether DHCP assigns the TFTP server	Configuring the Alternate TFTP Server, page 4-23
Use the following TFTP servers	Assigns static TFTP server IP addresses for: <ul style="list-style-type: none"> • TFTP Server 1 • TFTP Server 2 	
Network Profile Advanced Settings		
TSPEC Settings		Configuring Advanced Settings, page 4-24
Minimum PHY Rate	Minimum data rate that outbound traffic uses	
Surplus Bandwidth	Excess bandwidth beyond application requirements	
802.11G Power Settings	Enabled—Identifies enabled channels in WLAN to improve scanning for the phone Max Tx Power—Sets the maximum transmit power for the phone	
802.11A Power Settings	Enabled—Identifies enabled channels in WLAN to improve scanning for the phone Max Tx Power—Sets the maximum transmit power for the phone	

**Note**

If you uncheck all channels in the 802.11 G Power Settings or 802.11 A Power Settings, the phone will not be able to access the WLAN.

Related Topics

- [Accessing the Phone Web Page, page 4-5](#)
- [Configuring Wireless Settings in a Network Profile, page 4-15](#)
- [Setting the Wireless LAN Security Mode, page 4-16](#)
- [Setting the Wireless Security Credentials, page 4-18](#)


- [Setting Wireless Encryption, page 4-20](#)

Configuring Wireless Settings in a Network Profile

You must configure these wireless settings in a profile to enable the phone to access the wireless network.

To configure the wireless settings, refer to [Table 4-2](#) and follow these steps:

Procedure

-
- Step 1** Choose the network profile that you want to configure.
- Step 2** To give the profile a recognizable name, in the Profile Name field, enter a name up to 63 characters and numbers in length.
- Step 3** To identify the SSID that the phone uses to associate with access points, in the SSID field, enter an SSID that is already configured in the WLAN.
-  **Note** The SSID is case sensitive; you must enter it exactly as configured in the network.
-
- Step 4** To determine the scanning frequency of the phone, in the Single Access Point field, choose **True** (less frequent scanning) or **False** (more frequent scanning).
- Step 5** To conserve battery power, in the Call Power Save Mode, choose the type (U-APSD or PS-Poll) and option that is being used in the WLAN.
- Step 6** Choose the signal mode or priority of signal modes in the 802.11 Mode field that is used by your WLAN,
-

Setting the Wireless LAN Security Mode

The Cisco Unified Wireless IP Phone 7921G supports many types of authentication. Authentication methods might require a specific encryption method or you can choose between several encryption methods. When configuring a network profile, you can choose one of these authentication methods:

- **Open**—Provides access to all access points without WEP Key authentication/encryption.
- **Open plus WEP**—Provides access to all access points and authentication through the use of one or more WEP Keys at the local access point.
- **Shared Key plus WEP**—Provides shared key authentication through the use of WEP Keys at the local access point.
- **LEAP**—Exchanges a username and cryptographically secure password with a RADIUS server for authentication in the network. LEAP is a Cisco proprietary version of EAP.
- **EAP-FAST**—Exchanges a username and password and with a RADIUS server for authentication in the network.
- **Auto(AKM)**—Automatic authenticated key management in which the phone selects the AP and type of key management scheme, that can include WPA, WPA2, WPA-Pre-shared key, WPA2-Pre-shared key, or CCKM which uses a wireless domain server (WDS).

The type of authentication and encryption schemes that you are using with your WLAN determine how you set up the authentication, security, and encryption options in the network profiles for the Cisco Unified Wireless IP Phones.

[Table 4-3](#) provides a list of supported authentication and encryption schemes that you can configure on the Cisco Unified Wireless IP Phone 7921G.

Table 4-3 Authentication and Encryption Configuration Options

Authentication Method	Wireless Encryption	Wireless Security Credentials
Open	None	None—access to all APs
Open plus WEP	Static WEP Requires WEP Key	None—access to all APs

Table 4-3 Authentication and Encryption Configuration Options

Authentication Method	Wireless Encryption	Wireless Security Credentials
Shared Key plus WEP	Static WEP Requires WEP Key	Uses shared-key with AP
LEAP (with optional CCKM)	Uses WEP	Requires Username and Password
EAP-FAST (with optional CCKM)	Uses WEP or TKIP	Requires Username and Password
Auto (AKM) with WPA (with optional CCKM)	Uses TKIP	Requires Username and Password
Auto (AKM) with WPA2	Uses AES	Requires Username and Password
Auto (AKM) with WPA Pre-Shared Key	Uses TKIP	Requires Passphrase
Auto (AKM) with WPA2 Pre-Shared Key	Uses AES	Requires Passphrase
Auto (AKM) with CCKM	Uses TKIP or AES	Requires Username and Password

Configuring the Authentication Method

To select the Authentication Method for this profile, follow these steps:

Procedure

-
- Step 1** Choose the network profile that you want to configure.
- Step 2** In the Authentication Method field, click the drop-down arrow and select one of the following:
- Open
 - Open+WEP
 - Shared+WEP

- LEAP
- EAP-FAST
- Auto (AKM)



Note Depending on what you selected, you must configure additional options in Wireless Security or Wireless Encryption. See [Table 4-3](#) for more information.

Step 3 Click **Save** to make the change.

Setting the Wireless Security Credentials

When your network uses EAP-FAST, LEAP, or Auto (AKM) with WPA, WPA2, or CCKM for user authentication, you must configure both the username and a password on the Access Control Server (ACS) and the phone.



Note If you use domains within your network, you must enter the username with the domain name, in this format: *domain\username*.

For information about setting security credentials, see these topics:

- [Configuring the Username and Password, page 4-18](#)
- [Configuring the Pre-shared Key, page 4-19](#)
- [Setting Wireless Encryption, page 4-20](#)

Configuring the Username and Password

To enter or change the username or password for the network profile, you must use the same username and the same password string that is configured in the RADIUS server. The maximum length of the username or password entry is 32 characters.

To setup the username and password in Wireless Security Credentials, follow these steps:

Procedure

- Step 1** Choose the network profile that uses LEAP, EAP-FAST, or Auto (AKM).
 - Step 2** In the Username field, enter the network username for this profile.
 - Step 3** In the Password field, enter the network password string for this profile.
 - Step 4** Click **Save** to make the change.
-

Configuring the Pre-shared Key

When using Auto (AKM) with WPA Pre-shared key or WPA2 with Pre-shared key for authentication, you must configure a Passphrase/Pre-shared key in the Wireless Security Credentials area.

Pre-shared Key Formats

The Cisco Unified Wireless IP Phone 7921G supports ASCII and hexadecimal formats. You must use one of these formats when setting up a WPA Pre-shared key:

Hexadecimal

For hexadecimal keys, you must enter 64 hex digits (0-9 and/or A-F); for example, AB123456789CD01234567890EFAB123456789CD01234567890EF3456789C

ASCII

For ASCII keys, you must enter a character string that uses 0-9, A-Z (upper and lower case), including symbols and is from 8 to 63 characters in length; for example, GREG12356789ZXYW

To setup a Pre-shared key in the Wireless Credentials area, follow these steps:

Procedure

- Step 1** Choose the network profile that uses Auto (AKM) to enable the WPA Pre-shared key or WPA2 Pre-shared key.

- Step 2** In the Key Type area, choose one of these character formats:
- **Hex**
 - **ASCII**
- Step 3** Enter an ASCII string or Hex digits in the Passphrase/Pre-shared key field. See [“Pre-shared Key Formats” section on page 4-19](#).
- Step 4** Click **Save** to make the change.
-

Setting Wireless Encryption

If your wireless network uses WEP encryption, and you have set the Authentication Method as Open + WEP or Shared Key + WEP, you must enter an ASCII or hexadecimal WEP Key.

The WEP Keys for the phone must match the WEP Keys assigned to the access point. Cisco Unified Wireless IP Phone 7921G and Cisco Aironet Access Points support both 40-bit and 128-bit encryption keys.

WEP Key Formats

You must use one of these formats when setting up a WEP key:

Hexadecimal

For hexadecimal keys, you can use one of the following key sizes:

- 40-bit—You must enter a 10-digit encryption key string that uses the hex digits (0-9 and/or A-F); or example, ABCD123456.
- 128-bit—You must enter a 26-digit encryption key string that uses the hex digits (0-9 and/or A-F); or example, AB123456789CD01234567890EF.

ASCII

For ASCII keys, you must enter a character string that uses 0-9, A-Z (upper and lower case), and all symbols.

- 40-bit—You must enter a 5-character string; for example, GREG5.
- 128-bit—You must enter a 13-character string; for example, GREGSSECRET13.

Entering Wireless Encryption Keys

To setup WEP keys, follow these steps:

Procedure

- Step 1** Choose the network profile that uses Open+WEP or Shared+WEP.
- Step 2** In the Key Type area, choose one of these character formats:
- **Hex**
 - **ASCII**
- Step 3** For Encryption Key 1, click **Transmit Key**.
- Step 4** In the Key Size area, choose one of these character string lengths:
- **40**
 - **128**
- Step 5** In the Encryption Key field, enter the appropriate key string based on the selected Key Type and Key Size. See the “[WEP Key Formats](#)” section on page 4-20.
- Step 6** Click **Save** to make the change.
-

Related Topics

- [Configuring IP Network Settings, page 4-21](#)
- [Configuring the Alternate TFTP Server, page 4-23](#)
- [Configuring Advanced Settings, page 4-24](#)

Configuring IP Network Settings

The Cisco Unified IP Phones enable DHCP, by default, to automatically assign IP addresses to devices when you connect them to the network. If you do not use DHCP in your network, then you must disable DHCP and manually enter network configuration information. For more information, see “[Interacting with the DHCP Server](#)” section on page 2-25.

When DHCP is disabled in the network, you must configure the following settings in the Static Settings menu:

- IP address
- Subnet mask
- Default Router
- DNS server 1 and 2
- TFTP server 1

Use these guidelines when manually configuring the IP settings:

- Ensure the TFTP server has an IP address.
- Ensure the default router IP address is on the same subnet as the host IP address.

Enabling DHCP

To enable the use of DHCP in the Network Profile, follow these steps:

Procedure

- Step 1** Choose the network profile that you want to configure.
- Step 2** Under the IP Network Configuration area, choose this option:
Obtain IP address and DNS servers automatically
- Step 3** Click **Save** to make the change.
-

Disabling DHCP

To disable the use of DHCP in the Network Profile, follow these steps:

Procedure

- Step 1** Choose the network profile that you want to configure.
- Step 2** Under the IP Network Configuration area, choose this option:
Use the following IP addresses and DNS servers

- Step 3** You must enter these required IP addresses. See [Table 4-4](#) for descriptions of these fields.
- Step 4** Click **Save** to make the change.

Table 4-4 *Static IP Addresses When DHCP is Disabled*

Static Setting	Description
IP Address	Internet Protocol (IP) address of the phone
Subnet Mask	Subnet mask used by the phone
Default Router 1	Primary gateway used by the phone
DNS Server 1	Primary DNS server used by the phone
DNS Server 2	Optional backup DNS server used by the phone
TFTP Server 1	Primary TFTP server used by the phone.
TFTP Server 2	Optional backup TFTP server used by the phone
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides

Configuring the Alternate TFTP Server

If you use DHCP to direct the Cisco Unified IP Phones to a TFTP server, you can also assign an alternative TFTP server to some phones instead of the one assigned by DHCP.



Note If you disable DHCP, then you must use these steps to set up the TFTP server for the phone.

To assign an alternate TFTP server to a phone, follow these steps:

Procedure

- Step 1** Choose the network profile that you want to configure.

- Step 2** Under the TFTP area, choose this option:
Use the following TFTP servers
- Step 3** You must enter the required IP addresses. See [Table 4-4](#) for descriptions of these fields.
- Step 4** Click **Save** to make the change.
-

Configuring Advanced Settings

The network profiles provide a web page for setting QoS, bandwidth, and power settings. The Traffic Specification (TSPEC) parameters are used to advertise information about generated traffic for Call Admission Control (CAC) to the AP.

Minimum PHY rate—Lowest rate that outbound traffic is expected to use before the phone roams to another AP

Surplus Bandwidth Allowance—Fractional number that specifies the excess allocation of time and bandwidth above application rates required to transport a MAC service data unit (MSDU) in a TSPEC frame.



Note

If your wireless LAN has access points that use 802.11b and you plan to use Call Admission Control (CAC) with TSPEC, then you need to modify the PHY rate to a supported rate for your 802.11b access points.

To make changes to the advanced settings, follow these steps:

Procedure

- Step 1** Choose the network profile that you want to configure.
- Step 2** Click the Advanced Profile link at the top of the page.
- Step 3** In the TSPEC Setting area, keep the Minimum PHY Rate: **12 Mbps**



Note

If you are using 802.11b APs and plan to use Call Admission Control (CAC) with TSPEC, then set the PHY Rate to a rate that the APs support such as 11 Mbps.

- Step 4** In the Surplus Bandwidth field, enter the appropriate values.
- Step 5** In the 802.11G Power Settings area, check only the channels that are used in your WLAN. By doing this, the phone scans for only those channels.
- In the Max Tx Power field, keep the default value.
- Step 6** In the 802.11A Power Settings area, check only the channels that are used in your WLAN. By doing this, the phone scans for only those channels.
- In the Max Tx Power field, keep the default value.

**Caution**

You must check at least one channel after using “Clear All,” to enable the phone to access the WLAN.

- Step 7** Click **Save** to make the change.

Related Topics

- [Accessing the Configuration Web Page for a Phone, page 4-7](#)
- [Network Profile Settings, page 4-10](#)
- [Configuring Wireless Settings in a Network Profile, page 4-15](#)
- [Setting the Wireless LAN Security Mode, page 4-16](#)
- [Setting the Wireless Security Credentials, page 4-18](#)
- [Configuring the Pre-shared Key, page 4-19](#)
- [Configuring IP Network Settings, page 4-21](#)
- [Configuring the Alternate TFTP Server, page 4-23](#)

Configuring USB Settings

To use the USB cable from your PC to a phone, you must configure the USB settings to work with the USB port on the PC. The phone has a default USB IP address of 192.168.1.100. You can change the USB port configuration on the phone in these ways:

- To obtain the IP address automatically, by getting an IP address from the PC that has DHCP set up.
- To use the IP address and subnet mask assigned in this area.

To display the USB Settings area, access the web page for the phone as described in the [“Accessing the Phone Web Page”](#) section on page 4-5, and then click the **USB Settings** hyperlink.

To change the USB port settings for the phone, follow these steps:

Procedure

- Step 1** On the phone’s web page, choose the USB Settings hyperlink.
- Step 2** Choose one of the following options:
- Obtain IP address automatically
 - Use the following IP address
- Step 3** To change the static IP address, in the IP Address field, enter a new IP address that is not assigned on the subnet.
- Step 4** To change the subnet for the new IP address, in the Subnet Mask field, enter the appropriate subnet address.
- Step 5** Click **Save** to make the change.
-

Related Topics

- [Accessing the Phone Web Page, page 4-5](#)
- [Configuring Network Profiles, page 4-10](#)
- [Configuring Trace Settings, page 4-27](#)
- [Using System Settings, page 4-29](#)

Configuring Trace Settings

You can use the Trace Settings area on the web page to configure how the phone creates and saves trace files. Because trace files are stored in the memory of the phone, you can control the number of files and the data that you want to collect. [Table 4-5](#) describes these configurable items.

**Note**

When preserving trace logs, choose only the logs that need to be saved after the phone is powered off and powered on to avoid using up phone memory.

To display the Trace Settings area, access the web page for the phone as described in the [“Accessing the Phone Web Page” section on page 4-5](#), and then click the **Trace Settings** hyperlink under Setup.

To change the trace settings for the phone, follow these steps:

Procedure

-
- Step 1** On the phone’s web page, choose the Trace Settings hyperlink.
- Step 2** In the Number of Files field, choose the number of trace files to save, from 2 to 10.
- Step 3** In the Remote Syslog Server area, check the box to enable a server to collect the trace files.
- Step 4** If you enabled the syslog server, then you must complete these fields:
- IP Address—Enter server IP address
 - Port—Enter a port number (514, 1024-65535)
- Step 5** In the Module Trace Level area, check only the modules for which you want data:
- Kernel
 - Configuration
 - Call Control
 - Network Services
 - Security Subsystem
 - User Interface
 - Wireless

Configuring Trace Settings

- Audio System
- System

Step 6 In the Advanced Trace Settings area, in the Preserve Logs field, choose one of the following:

- True—Save the trace logs to flash memory on the phone.
- False—Save the trace logs to RAM.



Note

- When set to False, the trace logs are lost when the phone is powered off.
- When the phone is powered off, then powered back on, the Preserve Logs field is reset to False, the default value.

Step 7 Click **Save** to make the change.

Table 4-5 Trace Settings Area Items

Item	Description
General	
Number of Files	Choose the number of trace files that the phone saves, from 2-10 files.
Remote Syslog Server	
Enable Remote Syslog	Set up a remote server to store trace logs IP Address—Enter server IP address Port—Enter a port number (514, 1024-65535)
Module Trace Level	
Kernel	Operating System data
Configuration	Phone configuration data
Call Control	Cisco Unified CallManager data
Network Services	DHCP, TFTP, CDP data
Security Subsystem	Application level security data
User Interface	Key strokes, softkeys, MMI data
Wireless	Channel scanning, authentication data

Table 4-5 Trace Settings Area Items (continued)

Item	Description
Audio System	RTP, SRTP, RTCP, DSP data
System	Firmware, upgrade data
Advanced Trace Settings	
Preserve Logs	True—Save trace logs after powering off the phone False—Delete trace logs

Related Topics

- [Accessing the Phone Web Page, page 4-5](#)
- [Configuring Network Profiles, page 4-10](#)
- [Configuring USB Settings, page 4-25](#)
- [Using System Settings, page 4-29](#)

Using System Settings

In addition to phone settings, the web page includes these areas for system management:

- Trace Logs
- Backup Settings
- Phone Upgrade
- Change Password

For information about the remaining web page topics, see the [Chapter 8](#), “Monitoring the Cisco Unified Wireless IP Phone Remotely.”

Viewing Trace Logs

You can use the Trace Logs area on the web page to view and manage trace files. System trace logs appear in a list on this page. You define how many messages are saved in the Trace Settings area. To view a trace log, click on the “Message.<n>”. The trace log appears in ASCII text. You can save the text file in a directory or on a disk to send to TAC for troubleshooting purposes.

**Note**

Trace logs are erased when the phone is powered off. To preserve trace logs, see the [“Configuring Trace Settings”](#) section on page 4-27.

To display the Trace Logs area, access the web page for the phone as described in the [“Setting Up Your PC to Configure the Cisco Unified Wireless IP Phone 7921G”](#) section on page 4-2, and then click the **Trace Logs** hyperlink.

Related Topics

- [Using System Settings, page 4-29](#)
- [Backup Settings for Phone Configuration, page 4-30](#)
- [Upgrading Phone Firmware, page 4-34](#)
- [Changing the Admin Password, page 4-35](#)

Backup Settings for Phone Configuration

You can use the Backup Settings area on the web page to export the phone configuration. You must set up an encryption key that encrypts the phone settings to keep them secure. When you export a configuration, all the settings in the network profiles, phone settings, USB settings, and trace are copied. None of the statistics or information fields are copied from the web pages.

**Note**

To import a file to a phone, you must enter the same encryption key that was used to export the file.

To display the Backup Settings area, access the web page for the phone as described in the [“Accessing the Configuration Web Page for a Phone”](#) section on page 4-7, and then click the **Backup Settings** hyperlink. Table 4-6 describes the items in this area.

Table 4-6 Backup Settings Area Items

Item	Description
Import Configuration	
Encryption Key	Enter the alphanumeric string up to 8-20 characters for encrypting the phone settings.
Import File	Enter the path and filename or use the Browse button to locate the file.
Import button	Click the button to import the phone settings file into the phone.
Export Configuration	
Encryption Key	Enter the alphanumeric string up to 8-20 characters for encrypting the phone settings.
Export button	Click the button to export the phone settings file to a location on your PC or to a disc.

Using Network Profile Templates

At initial phone deployment, you can create a typical network profile and export the phone settings to a location that you specify, such as a folder on your PC or your network. Then, you can import the network profile template to several phones to save time.

Creating a Configuration Template

To create a phone configuration template, follow these steps:

Procedure

-
- Step 1** Connect the USB cable to the phone and access the phone's web page using the instructions on [“Accessing the Phone Web Page”](#) section on page 4-5.
- Step 2** On the phone's web page, choose the **Network Profiles** hyperlink and configure the Network Profile settings for your template configuration.



Note You can leave the Username and Password fields blank so they can be configured individually.

- Step 3** Next, configure the USB Settings and Trace Settings for your template configuration.
- Step 4** Choose the **Backup Settings** hyperlink, to access the export and import settings.
- Step 5** In the Export Configuration area, enter an encryption key of from 8 to 20 characters.
- Record this key because you must enter this key to import the configuration template on other phones.
- Step 6** Click **Export** and the File Download dialog displays, and then click **Save**.
- Step 7** Give your configuration a new file name such as *7921template.cfg*.
- Step 8** Choose a location on your PC or on the network for the file and then click **Save**.
- Step 9** The encrypted configuration file contains these settings:
- Profile Name
 - SSID
 - Single Access Point
 - Call Power Save Mode
 - 802.11 Mode
 - WLAN Security
 - Authentication Method
 - User name
 - Password
 - Passphrase

- Encryption keys
- Use DHCP to get IP address and DNS servers
- Static Settings (if configured)
 - IP Address
 - Subnet Mask
 - Default Router
 - Primary DNS Server
 - Secondary DNS Server
- Use DHCP to get TFTP Server
- Static TFTP Settings (if configured)
 - TFTP Server 1
 - TFTP Server 2

Advanced Network Profile Settings

- Minimum PHY rate
- Surplus Bandwidth
- 802.11G Power Settings (checked ones)
- 802.11A Power Settings (checked ones)

USB Settings (use one of these)

- Obtain IP address from server
or
- Static settings (if configured)
 - IP address
 - Subnet Mask

Trace Settings

- Number of Files
- Syslog Server (enabled/disabled)
 - IP address
 - Port

- Modules and error level for collection
- Preserving Logs (true/false)

Importing a Configuration Template

To import a phone configuration template, follow these steps:

Procedure

-
- Step 1** Connect the USB cable to an unconfigured phone and access the phone's web page using the instructions on "[Accessing the Phone Web Page](#)" section on [page 4-5](#).
 - Step 2** On the phone's web page, choose the **Backup Settings** hyperlink.
 - Step 3** In the Import Configuration area of the page, enter the Encryption Key.



Note

You must enter the same key that you used to export the configuration template.

- Step 4** Use the Browse button to locate the configuration template and click **Open**.
The configuration file downloads to the phone.
 - Step 5** You can use the web pages to add missing configuration items such as the username and password or make other changes at this time.
-

Related Topics

- [Using System Settings, page 4-29](#)
- [Viewing Trace Logs, page 4-30](#)
- [Upgrading Phone Firmware, page 4-34](#)
- [Changing the Admin Password, page 4-35](#)

Upgrading Phone Firmware

You can use the Phone Upgrade area on the web page to upgrade firmware files on the phones by using the USB connection or by using the WLAN.

To display the Phone Upgrade area, access the web page for the phone as described in the “[Accessing the Configuration Web Page for a Phone](#)” section on page 4-7, and then click the **Phone Upgrade** hyperlink.

To upgrade the phone software, enter the phone software TAR (firmware file name) or use the Browse button to locate the firmware file on the network.

Related Topics

- [Using System Settings, page 4-29](#)
- [Viewing Trace Logs, page 4-30](#)
- [Backup Settings for Phone Configuration, page 4-30](#)
- [Changing the Admin Password, page 4-35](#)

Changing the Admin Password

Cisco Unified CallManager 4.1 or Later

If you are running Cisco Unified CallManager 4.1 or later, you can use the Change Password area on the web page to change the administration password for the phone web pages.

To change the password on the web page, you must first enter the old password. Enter the new password and then reenter the new password to confirm the change.

To display the Change Password area, access the web page for the phone as described in the “[Accessing the Configuration Web Page for a Phone](#)” section on page 4-7, and then click the **Change Password** hyperlink.

Cisco Unified CallManager 5.0 or Later

If you are running Cisco Unified CallManager 5.0 or later, you must set the password in Cisco Unified CallManager Administration on the Phone Configuration page. The password set in Cisco Unified CallManager takes precedence over the password that is set on the web pages.



Caution

When setting the Administration Password in the Product Specific Configuration section in Cisco Unified CallManager 5.0 Administration, you must enable TFTP encryption. Otherwise, the password appears in readable text in the phone configuration file and can be viewed from any host that has access to TFTP server.

Related Topics

- [Using System Settings, page 4-29](#)
- [Viewing Trace Logs, page 4-30](#)
- [Upgrading Phone Firmware, page 4-34](#)
- [Backup Settings for Phone Configuration, page 4-30](#)



CHAPTER 5

Configuring Settings on the Cisco Unified Wireless IP Phone 7921G

The Settings menu on the Cisco Unified Wireless IP Phone 7921G provides access to view and change network profile settings and several phone settings for users. The Settings menu includes these configurable menus:

- Network Profiles
- Phone Settings
- Security Configuration
- USB Configuration

The Settings menu also provides view only access to network, device, and other phone status information. For information about these menus, see the [Chapter 7, “Viewing Security, Device, Model, and Status Information on the Phone.”](#)

These sections provide details about configuring network and phone settings on the phone:

- [Accessing Network and Phone Settings, page 5-2](#)
- [Configuring Network Profile Settings, page 5-3](#)
- [Changing Phone Settings, page 5-15](#)
- [Configuring the Security Certificate on the Phone, page 5-17](#)
- [Changing the USB Configuration, page 5-19](#)

Accessing Network and Phone Settings

You can view and change many network configuration options and phone settings for the Cisco Unified Wireless IP Phone 7921G by using the Settings menu.





Note

You can control whether a Cisco Unified Wireless IP Phone 7921G has access to the Settings menu from the Cisco Unified CallManager Administration Phone Configuration page. Use the Settings Access field in the Product Specific Configuration section of the phone configuration page. For more information, see the [“Specific Configuration Options for the Cisco Unified Wireless IP Phone 7921G” section on page 6-15](#).

To access the Settings menu, follow these steps:

Procedure

Step 1 Press  on the Navigation button for  (Settings).

Step 2 Use these menu options to view or change settings:

- **Phone Settings**
- **Network Profiles**
- **Security Configuration**
- **USB Configuration**




Note These options are configurable; other options are display only.

Step 3 To select the item that you want to configure or view, do one of these actions:

- Use the Navigation button to scroll to the item and then press the **Select** button.
- Use the keypad to enter the number that corresponds to the item.

Step 4 If a menu option is locked , you must press **** #** on the keypad.

When the menu is unlocked,  displays.

Related Topics

- [Configuring Network Profile Settings, page 5-3](#)
- [Changing Phone Settings, page 5-15](#)
- [Configuring the Security Certificate on the Phone, page 5-17](#)
- [Changing the USB Configuration, page 5-19](#)

Configuring Network Profile Settings

On the Cisco Unified Wireless IP Phone 7921G, you can configure a network profile for the wireless network settings for a specific WLAN.

Users with wireless IP phones, who travel between company locations, can have separate network profiles for each wireless LAN (WLAN) location. You can set up profiles with the local SSID, WLAN settings, and authentication information for each location.

These sections provide information about configuring network profiles:

- [Accessing a Network Profile, page 5-3](#)
- [Changing the Profile Name, page 5-4](#)
- [Changing Network Configuration Settings, page 5-6](#)
- [Configuring DHCP Settings, page 5-8](#)
- [Configuring Wireless Settings for the Network Profile, page 5-11](#)

Accessing a Network Profile




To view or configure the Network Profile menu on a Cisco Unified Wireless IP Phone 7921G, follow these steps:



Note

You can control whether a Cisco Unified Wireless IP Phone 7921G has access to the Network Profiles menu from the Cisco Unified CallManager Administration Phone Configuration page. Use the Settings Access field in the Product Specific Configuration section of the phone configuration page. For more information, see the [“Specific Configuration Options for the Cisco Unified Wireless IP Phone 7921G”](#) section on page 6-15.

Procedure

- Step 1** Choose **Settings > Network Profiles**.
- Step 2** To select the profile name that you want to configure, do one of these actions:
- Use the Navigation button to scroll to the item and then press the **Select** button.
 - Use the keypad to enter the number that corresponds to the item.
- The Network Config list is locked . To unlock the network settings in the profile, press * * # and  displays.
- Step 3** To display the profile settings, press **Change**.
- Step 4** Scroll to and select one of these menu options:
- **Profile Name**
 - **Network Configuration**
 - **WLAN Configuration**
- Step 5** Make changes to the settings. For more information, see [Table 5-1](#).
- Step 6** To save changes to settings in the Profile menu, press **Save**.
- Step 7** To use the modified profile, scroll to the profile name and press **Select**. The  appears by enabled profiles. You can enable from 1 to 4 profiles.
-

Changing the Profile Name

You can change the default name of the network profile to one that is more meaningful to the user, such as, “Headquarters” or “Branch office.” You can change the name before or after you have made changes to the network profile.

To rename the profile, follow these steps:







Procedure

- Step 1** Choose **Settings > Network Profiles**.

- Step 2** To select the profile name that you want to change, use the Navigation button to scroll to the item and then press the Select button.
- Step 3** Enter ****#** to unlock the profile.
- Step 4** Select **Profile Name**.
- Step 5** Press **Edit** and enter a new name in the New Profile Name field.
See [Guidelines for Editing Settings in the Network Profile, page 5-5](#).
- Step 6** Press **Options > Save** to complete the name change.
-

Guidelines for Editing Settings in the Network Profile

When you edit the value of an option on the Network Profile, you can enter characters, numbers, and special characters from the phone keypad. Use the numeric keys on the keypad to enter the number or the assigned characters. Each press moves to another character choice. Use the following guidelines when entering values:

- Enter characters—Press the numeric key to move to the desired character (lowercase, then upper case).
- Enter numbers—Press the numeric key to enter the number.
- Delete the last character—Press << to delete the last character or number in the string.
- Enter a space—Press  to enter a space between characters.
- Enter a dot—Press  to enter a dot between numbers.
- Enter special characters and symbols—Press one of the following keys to display and enter these characters:
 - Press  to enter * + - / = \ : ;
 - Press  to enter a space , . ‘ “ | _ ~ ‘
 - Press  to enter # ? () [] { }
 - Press  to enter ! @ < > \$ % ^ &
- Save an entry—Press **Options > Save**
- Cancel editing mode—Press **Options > Cancel** as needed to return to the menu option or main screen.

Related Topics

- [Accessing Network and Phone Settings, page 5-2](#)
- [Configuring DHCP Settings, page 5-8](#)
- [Configuring an Alternate TFTP Server, page 5-10](#)
- [Configuring Wireless Settings for the Network Profile, page 5-11](#)

Changing Network Configuration Settings

After accessing a network profile, you can use [Table 5-1](#) for descriptions and reference information for network profile settings.

Table 5-1 *Network Configuration Settings*

Network Setting	Description	For More Information, See...
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address	Configuring DHCP Settings, page 5-8
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
DHCP Enabled	Yes —Allows the Dynamic Host Configuration Protocol (DHCP) to obtain an IP address for the phone No —Disables the use of DHCP. You must configure the static settings for the phone	Configuring DHCP Settings, page 5-8

Table 5-1 Network Configuration Settings (continued)

Network Setting	Description	For More Information, See...
IP Address	Internet Protocol (IP) address of the phone	Configuring DHCP Settings, page 5-8
Subnet Mask	Subnet mask used by the phone	
Default Router 1	Primary gateway used by the phone	
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides	
DNS Server 1	Primary DNS server used by the phone	
DNS Server 2	Optional backup DNS server used by the phone	
Alternate TFTP	Yes—This option assigns an alternative Trivial File Transfer Protocol (TFTP) server No—This option uses the TFTP server assigned by DHCP	Configuring an Alternate TFTP Server, page 5-10
TFTP Server 1	IP address for the primary TFTP server used by the phone. If you set Alternate TFTP option to Yes, you must enter a non-zero value for this option	
TFTP Server 2	Optional backup TFTP server the phone uses if the primary TFTP server is not available	
Load Server	IP address for the server where the phone receives firmware updates	<i>Cisco Unified CallManager Configuration Guides.</i>
CDP Enabled	Enables or disables Cisco Discovery Protocol (CDP) for the phone	Changing the Cisco Discovery Protocol Settings, page 5-10
DHCP Address Released	Enables or disables the DHCP server to release the IP address	
Erase Configuration	Deletes the phone configuration and sets to factory defaults	

Table 5-1 Network Configuration Settings (continued)

Network Setting	Description	For More Information, See...
Handset Only Mode	<p>Yes—Indicates that the speakerphone is disabled on the phone</p> <p>No—Indicates that the speakerphone is enabled on the phone</p>	Specific Configuration Options for the Cisco Unified Wireless IP Phone 7921G, page 6-15

Configuring DHCP Settings

The Cisco Unified IP Phones enable DHCP, by default, to automatically assign IP addresses to devices when you connect them to the network. If you do not use DHCP in your network, then you must disable DHCP and manually enter the network configuration information. For more information, see [“Interacting with the DHCP Server” section on page 2-25](#).

Use these guidelines when manually configuring the IP settings:

- Ensure the TFTP server has an IP address.
- Ensure the default router IP address is on the same subnet as the host IP address.



Note

When DHCP is enabled, you cannot configure IP settings, but you can configure and alternate TFTP server.

Disabling DHCP

To disable DHCP on the phone and manually configure IP settings, follow these steps:

Procedure

-
- Step 1** Choose **Settings >Network Profile**.
 - Step 2** Scroll to the profile name that you want to configure and press **Select**.
 - Step 3** Enter ****#** to unlock the profile and press **Edit**.

- Step 4** Select **Network Configuration**.
- Step 5** Scroll to **DHCP Enabled** and press **No**.
- Step 6** Scroll to **IP Address** and press **Select**.
- Step 7** In the New IP Address: field, enter the static IP address for the phone.
- Step 8** Press **Options > Validate** to save the entry or press **Cancel**.

You must enter the other required static fields. See [Table 5-2](#) for descriptions of these fields.

For information about entering values, see the “[Guidelines for Editing Settings in the Network Profile](#)” section on page 5-5.

Table 5-2 *Static Settings When DHCP is Disabled*

Static Setting	Description
IP Address	IP address, the unique identifier assigned by the system administrator for the phone.
Subnet Mask	Used to partition the IP address into a network identifier and host identifier so TCP/IP can distinguish between them.
Default Router 1	Identifies the gateway that provides connectivity to the IP network beyond the subnet to which the phone belongs.
Domain Name	Identifies the Domain Name System (DNS) domain in which the phone resides.
DNS Server 1 DNS Server 2	If the system is configured to use host names for servers instead of IP addresses, identify the primary and secondary DNS server to resolve host names.
Alternate TFTP server	Identifies whether you are using an alternate TFTP server. See Configuring an Alternate TFTP Server, page 5-10 .
TFTP Server 1	Identifies the TFTP server that the phone uses to obtain configuration files.

Configuring an Alternate TFTP Server

If you use DHCP to direct the Cisco Unified IP Phones to a TFTP server, you can also assign an alternative TFTP server to some phones instead of the one assigned by DHCP.

To assign an alternate TFTP server to a phone, follow these steps:

Procedure

- Step 1** Choose **Settings > Network Profile**.
 - Step 2** To select the profile name that you want to configure, scroll to the item and then press the **Select** button.
 - Step 3** Enter ****#** to unlock the profile and press **Edit**.
 - Step 4** Select **Network Configuration**.
 - Step 5** Scroll to **Alternate TFTP** and press **Yes**.
 - Step 6** Scroll to **TFTP Server 1** and press **Select**.
 - Step 7** In the **New TFTP Server 1:** field, enter the IP address for the server.
See [Table 5-2](#) for descriptions of these fields.
For information about entering values, see the “[Guidelines for Editing Settings in the Network Profile](#)” section on page 5-5.
 - Step 8** Press **Options > /Validate** to save the entry or press **Cancel**.
-

Changing the Cisco Discovery Protocol Settings

Some network devices do not use Cisco Discovery Protocol (CDP).

To change whether the phone transmits CDP packets and settings associated with CDP, follow these steps:

Procedure

- Step 1** Choose **Settings > Network Profile**.

- Step 2** To select the profile name that you want to configure, scroll to the item and then press the **Select** button.
- Step 3** Enter ****#** to unlock the profile and press **Edit**.
- Step 4** Select **Network Configuration**.
- Step 5** Scroll to **CDP Enabled** and press **Yes** to enable or **No** to disable CDP.
-

Erasing the Configuration

You can erase the network profile configuration and return to the default settings. To erase the configuration, follow these steps:

Procedure

- Step 1** Choose **Settings >Network Profile**.
- Step 2** To select the profile name that you want to configure, scroll to the item and then press the **Select** button.
- Step 3** Enter ****#** to unlock the profile and press **Edit**.
- Step 4** Select **Network Configuration**.
- Step 5** Scroll to **Erase Configuration** and press **Yes** to erase or **No**.
-

Related Topics

- [Changing the Profile Name, page 5-4](#)
- [Configuring Wireless Settings for the Network Profile, page 5-11](#)

Configuring Wireless Settings for the Network Profile

The WLAN Configuration menu contains settings that the phone uses to authenticate with an access point. These settings include the SSIDs, authentication type, and encryption data that the phone uses.

This section includes these topics for configuring wireless settings:

- [Accessing the WLAN Configuration Menu, page 5-12](#)
- [Changing WLAN Configuration Settings, page 5-12](#)

Accessing the WLAN Configuration Menu

To access the WLAN Configuration menu options on a Cisco Unified Wireless IP Phone 7921G, follow these steps:

Procedure

-
- Step 1** Choose **Settings > Network Profiles**.
- Step 2** To select the profile name that you want to configure, scroll to the item and then press the **Select** button.
- Step 3** Enter ****#** to unlock the profile and press **Edit**.
- Step 4** Scroll to and select **WLAN Configuration**.
- Step 5** To view or change the menu options, press **Edit**.
For descriptions of the settings, see [Table 5-3](#).
- Step 6** Press **Options > /Save** to save the entry or press **Cancel**.
-

Changing WLAN Configuration Settings

After accessing the WLAN settings, use [Table 5-3](#) for descriptions and reference information for these settings.

Table 5-3 *WLAN Configuration Settings*

Network Setting	Description	For More Information, See...
SSID	Unique identifier for accessing wireless access points	Configuring Wireless Settings in a Network Profile, page 4-15

Table 5-3 *WLAN Configuration Settings (continued)*

Network Setting	Description	For More Information, See...
802.11 Mode	The wireless signal standard used in the WLAN. Options are: <ul style="list-style-type: none"> • 802.11b/g • 802.11a • Auto-b/g • Auto-a • Auto-RSSI 	The 802.11 Standards for Wireless LAN Communications, page 2-3
Single Access Point	Sets the phone to scan frequently for APs (Disabled) or to minimize scanning for APs (Enabled)	Roaming in a Wireless Network, page 2-14
Call Power Save Mode	The type of power saving mode used in the WLAN. Options are: <ul style="list-style-type: none"> • U-APSD/PS-Poll • None 	Networking Protocols Used with Cisco Unified Wireless IP Phones, page 2-8

Table 5-3 WLAN Configuration Settings (continued)

Network Setting	Description	For More Information, See...
Security Mode	<p>The type of authentication that the phone uses to access the WLAN. Options are:</p> <ul style="list-style-type: none"> • Open—Access to all APs without WEP key authentication/encryption • Open+WEP—Access to all APs and authentication through WEP keys at the local AP • Shared Key+WEP—Shared key authentication through WEP keys at the local AP • LEAP—Exchanges a username and cryptographically secure password with a RADIUS server in the network (Cisco proprietary version of EAP) • EAP-FAST—Exchanges a username and cryptographically secure password with a RADIUS server in the network • Auto (AKM)—Phone selects the AP and type of key management scheme, either WPA, WPA2, WPA-PSK, WPA2-PSK, or CCKM that must use a wireless domain server (WDS) 	Setting the Wireless LAN Security Mode, page 4-16
UserName	User name for the wireless network (up to 32 characters)	Configuring the Username and Password, page 4-18
Password	Password for the wireless network (up to 32 characters)	Configuring the Username and Password, page 4-18

Related Topics

- [Accessing Network and Phone Settings, page 5-2](#)
- [Configuring Network Profile Settings, page 5-3](#)
- [Configuring the Security Certificate on the Phone, page 5-17](#)
- [Changing Phone Settings, page 5-15](#)

Changing Phone Settings

The Phone Settings menu contains settings to customize individual phones with different ring tones or volume levels, display, and keypad settings.



Note

You can control whether a Cisco Unified Wireless IP Phone 7921G has access to the Phone Settings menu from the Cisco Unified CallManager Administration Phone Configuration page. Use the Settings Access field in the Product Specific Configuration section of the phone configuration page. For more information, see the [“Specific Configuration Options for the Cisco Unified Wireless IP Phone 7921G”](#) section on page 6-15.

To access the Phone Settings menu options on a Cisco Unified Wireless IP Phone 7921G, follow these steps:

Procedure

- Step 1** Choose **Settings > Phone Settings**.
- Step 2** Press the number for the setting that you want to configure (or you can scroll to the setting and press the **Select** button).
- Step 3** Press the number for the setting category.
- Step 4** Press the number for the setting that you want to change.

For descriptions of the settings, see [Table 5-4](#). For specific instructions to change these settings, refer to “Using Phone Settings,” in the *Cisco Unified Wireless IP Phone 7921G Guide*.

Table 5-4 Configurable Settings for the Phone Sounds, Display, and Keypad

Phone Setting	Description
Sound Settings	
Ring Tone	Assigns the ring tone for each line on the phone.

Table 5-4 Configurable Settings for the Phone Sounds, Display, and Keypad (continued)

Phone Setting	Description
Volumes	
Ring	Sets the ring volume level for the phone.
Speaker	Sets the volume for the speaker.
Handset	Sets the volume for the handset.
Headset	Sets the volume for the headset.
Docking Speaker	Sets the volume for the desktop charger speakerphone.
Docking Ring	Sets the ring volume level for the desktop charger.
Alert Pattern	Sets the ring, vibrate, or combination to alert the user of an incoming call.
Ring Output	Sets the phone to ring through speaker, headset, or both speaker and headset.
Display Settings	
Display Brightness	Sets the brightness for the phone screen.
Display Timeout	Sets the length of time for the phone screen to display before turning off or disables the timer so screen always displays.
LED Coverage Indicator	Enables or disables the LED blink to indicate that the phone is in service and within the coverage area.
Keypad Settings	
Any Key Answer	Enables or disables using any key or button on the phone to answer a ringing call.
Keypad Auto Lock	Sets the length of time for the keypad to lock automatically after no keypad activity or disables auto lock.
Keypad Tone	Enables or disables tones for keypad presses.

Related Topics

- [Accessing Network and Phone Settings, page 5-2](#)
- [Configuring Network Profile Settings, page 5-3](#)

- [Configuring the Security Certificate on the Phone, page 5-17](#)
- [Changing the USB Configuration, page 5-19](#)

Configuring the Security Certificate on the Phone

Security 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 1-9. 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 Certificate Authority Proxy Function (CAPF). You can use Cisco Unified CallManager Administration to configure an LSC, as described in *Cisco Unified CallManager Security Guide*.

Alternatively, you can initiate the installation of an LSC from the Security Configuration menu on the phone. This menu also lets you update or remove an LSC.

Before you do so, make sure that the appropriate Cisco Unified CallManager and the CAPF security configurations are complete:

- The CTL file should have a CAPF certificate.
- The CAPF certificate must exist in the /usr/local/cm/.security/certs folder in every server in the cluster.
- The CAPF is running and configured.

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

Depending on how you have configured the CAPF, this procedure installs an LSC, updates an existing LSC, or removes an existing LSC.

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

Procedure

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

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

Step 3 To open the menu, press the **Select** button.

Step 4 Scroll to LSC and press * * # to unlock the option.

Step 5 Press the **Update** softkey.

The phone prompts for an authentication string.

Step 6 Enter the authentication string 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, “Failed,” the authorization string may be incorrect or the phone may not be enabled for upgrading. Refer to error messages generated by the CAPF and take appropriate actions.

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

Related Topic

[Understanding Security Features for Cisco Unified IP Phones, page 1-9](#)

Changing the USB Configuration

When using the USB cable to configure a phone, you might need to change the USB configuration. The phone has a default USB IP address of 192.168.1.100 that you can use with the USB connection to the PC. If you need to change the USB port configuration, these options are available:

- Obtain the IP address automatically, by getting an IP address from the PC with DHCP set up.
- Use the IP address and subnet mask assigned in this area.

To view or configure the USB port configuration on a Cisco Unified Wireless IP Phone 7921G, follow these steps:

Procedure

-
- Step 1** Choose **Settings > USB Configuration**.
- Step 2** To open the menu, press the **Select** button.
- Step 3** Press * * # to unlock the menu.
- Step 4** To configure **DHCP**, press **Select** button and choose one of these options:
- To obtain an IP address automatically from the PC, choose **Enable**
- or
- To use a static IP address, choose **Disable**.
- Press **Save** to keep the option.



Note If you disabled DHCP, you must enter an IP address and a subnet mask by following these steps:

- Step 5** To change the static IP address, scroll to **IP Address**, and press **Select** button.
- Step 6** Enter a new IP address that is not assigned on the subnet.
- Step 7** Press **Options > Validate** to verify the entry.
- Step 8** To save the changes, press **Save**.
- Step 9** To change the subnet for the new IP address, scroll to **Subnet Mask** and press **Select** button.

- Step 10** Enter the appropriate subnet address.
- Step 11** Press **Options > Validate** to verify the entry.
- Step 12** To save the changes, press **Save**.
-

Related Topics

- [Accessing Network and Phone Settings, page 5-2](#)
- [Configuring Network Profile Settings, page 5-3](#)
- [Changing Phone Settings, page 5-15](#)



CHAPTER 6

Configuring Features, Templates, Services, and Users

After you install and configure your wireless voice network, you can add wireless IP phones by using Cisco Unified CallManager Administration to configure telephony features, modify softkey 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 providing users with information for using the phone and features, see [Appendix A, “Providing Information to Users By Using a Website.”](#)

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

This chapter includes these topics:

- [Configuring Cisco Unified Wireless IP Phones in Cisco Unified CallManager, page 6-2](#)
- [Telephony Features Available for the Phone, page 6-2](#)
- [Specific Configuration Options for the Cisco Unified Wireless IP Phone 7921G, page 6-15](#)
- [Configuring Softkey Templates, page 6-16](#)
- [Modifying Phone Button Templates, page 6-18](#)
- [Setting Up Services, page 6-19](#)
- [Configuring Corporate and Personal Directories, page 6-20](#)

- [Adding Users to Cisco Unified CallManager](#), page 6-22
- [Managing the User Options Web Pages](#), page 6-23
- [Creating Custom Phone Rings](#), page 6-25

Configuring Cisco Unified Wireless IP Phones in Cisco Unified CallManager

To provide telephony call routing and call control features for the Cisco Unified Wireless IP Phone 7921G, you must use the Cisco Unified CallManager Administration application. For instructions about adding these devices, refer to the “Cisco Unified IP Phone Configuration” chapter in the *Cisco Unified CallManager Administration Guide*.

Telephony Features Available for the Phone

[Table 6-1](#) describes supported telephony features, that you can configure using Cisco Unified CallManager Administration for the Cisco Unified Wireless IP Phone 7921G. The table provides references to documentation that contains configuration procedures and feature information.

For information about using the features on the phone, refer to *Cisco Unified Wireless IP Phone 7921G Guide*. For a comprehensive listing of features on the phone, refer to *Cisco Unified IP Phone Features A-Z*.



Note

Cisco Unified CallManager Administration also provides several service parameters that you can use to configure various telephony functions. For more information about service parameters and the functions that they control, you can use the **I or ? button** on the Cisco Unified CallManager configuration page.

Table 6-1 **Telephony Features for the Cisco Unified Wireless IP Phone 7921G**

Feature	Description	Configuration Reference
Abbreviated Dialing	<p>Allows users to speed dial a phone number by entering an assigned index code (1-99) on the phone keypad.</p> <p>Users assign index codes from the User Options web pages.</p>	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phone” chapter.
Auto Answer	<p>Connects incoming calls automatically after a ring or two.</p> <p>Auto Answer works with either the speaker or the headset mode.</p>	<p>For more information, refer to <i>Cisco Unified CallManager Administration Guide</i>, “Configuring Directory Numbers” chapter.</p>
Auto-pickup	<p>Allows a user to use one-touch, pickup functionality for call pickup, group call pickup, and other group call pickup.</p>	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>Cisco Unified CallManager 4.x Administration Guide</i>, “Call Pickup Group Configuration” chapter. • <i>Cisco Unified CallManager 4.x System Guide</i>, “Call Pickup” chapter. • <i>Cisco Unified CallManager 5.x Features and Services Guide</i>, “Call Pickup Group” chapter.

Table 6-1 Telephony Features for the Cisco Unified Wireless IP Phone 7921G (continued)

Feature	Description	Configuration Reference
Barge	<p>Allows a user to join a non-private call on a shared phone line. Barge features include cBarge and Barge.</p> <ul style="list-style-type: none"> • cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features. • Barge adds a user to a call but does not convert the call into a conference. <p>The phones support Barge in two conference modes:</p> <ul style="list-style-type: none"> • 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. 	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Barge and Privacy” chapter.
Block external to external transfer	Prevents users from transferring an external call to another external number.	For more information, refer to <i>Cisco Unified CallManager Features and Services Guide</i> , “External Call Transfer Restrictions” chapter.
Call display restrictions	Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call.	<p>For more information, refer to:</p> <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Understanding Route Plans” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Call Display Restrictions” chapter.

Table 6-1 Telephony Features for the Cisco Unified Wireless IP Phone 7921G (continued)


Feature	Description	Configuration Reference
Call Forward	Allows users to redirect incoming calls to another number.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager 4.x Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager 5.x Administration Guide</i>, “Configuring Directory Numbers” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter.
Call park	Allows users to park (temporarily store) a call and then retrieve the call by using another phone in the Cisco Unified CallManager system.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Call Park” chapter.
Call pickup	Allows users to redirect a call that is ringing on another phone within their pickup group to their phone. You can configure an audio and/or visual alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group.  Note The audio/visual alert is only available for phones on Cisco Unified CallManager release 4.2	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager 4.x Administration Guide</i>, “Call Pickup Group Configuration” chapter. • <i>Cisco Unified CallManager 4.x System Guide</i>, “Call Pickup” chapter. • <i>Cisco Unified CallManager 5.x Features and Services Guide</i>, “Call Pickup Group” chapter.

Table 6-1 **Telephony Features for the Cisco Unified Wireless IP Phone 7921G (continued)**

Feature	Description	Configuration Reference
Call waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. Displays incoming call information on the phone screen.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter.
Caller ID	Displays caller identification such as a phone number, name, or other descriptive text on the phone screen.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Administration Guide</i>, “Configuring Cisco Unified IP Phones” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Understanding Route Plans” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Call Display Restrictions” chapter.
Cisco Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Cisco Call Back” chapter.

Table 6-1 **Telephony Features for the Cisco Unified Wireless IP Phone 7921G (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: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Administration Guide</i>, “Client Matter Codes” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Client Matter Codes and Forced Authorization Codes” chapter.
Conference	Allows a user to talk simultaneously with multiple parties by calling each participant individually. Conference features include Conference, Join, cBarge, and Meet-Me.	For more information, refer to <i>Cisco Unified CallManager System Guide</i> , “Cisco Unified IP Phones” chapter.
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: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter.
Direct transfer	Allows users to connect two calls to each other (without remaining on the line).	For more information, refer to <i>Cisco Unified CallManager System Guide</i> , “Cisco Unified IP Phones” chapter.
Extension Mobility Service	Allows users to temporarily apply their phone number and phone settings to a shared Cisco Unified Wireless IP Phone by logging into the Extension Mobility service on that phone.	For more information, refer to <i>Cisco Unified CallManager Features and Services Guide</i> , “Cisco Unified CallManager Extension Mobility” chapter.

Table 6-1 Telephony Features for the Cisco Unified Wireless IP Phone 7921G (continued)

Feature	Description	Configuration Reference
Fast Dial Service	Allows a user to enter a Fast Dial code to place a call. Fast Dial codes can be assigned to phone numbers or Personal Address Book entries. (See “Services” in this table.)	For more information, refer to <i>Cisco Unified CallManager System Guide</i> , “Cisco Unified IP Phone Services” chapter.
Forced authorization codes (FAC)	Controls the types of calls that certain users can place.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager System Guide</i>, “Forced Authorization Codes (FAC)” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Client Matter Codes and Forced Authorization Codes” chapter.
Group call pickup	Allows a user to answer a call ringing on a phone in another group by using a group pickup code.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager 4.x Administration Guide</i>, “Call Pickup Group Configuration” chapter. • <i>Cisco Unified CallManager 4.x System Guide</i>, “Call Pickup” chapter. • <i>Cisco Unified CallManager 5.x Features and Services Guide</i>, “Call Pickup Group” chapter.
Hold	Allows users to move connected calls from an active state to a held state.	Requires no configuration, unless you want to use music on hold; see “Music-on- hold” in this table for information.

Table 6-1 Telephony Features for the Cisco Unified Wireless IP Phone 7921G (continued)

Feature	Description	Configuration Reference
Hunt group	Provides load sharing for calls to a main directory number. A hunt group contains a series of directory numbers that can answer the incoming calls. When the first directory number in the hunt group is busy, the system hunts in a predetermined sequence for the next available directory number in the group and directs the call to that phone.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Administration Guide</i>, “Hunt Group Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Understanding Route Plans” chapter.
Immediate Divert	Allows users to transfer an incoming call directly to the voice-messaging system.	For more information, refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Immediate Divert” chapter.
Join	Allows user to join two or more calls that are on one line to create a conference call and remain on the call.	For more information, refer to <i>Cisco Unified CallManager System Guide</i> , “Cisco Unified IP Phones” chapter.
Log out of hunt groups	Allows users to log out of hunt groups and temporarily block calls from ringing their phone when they are not available to take calls. Logging out of hunt groups does not prevent non-hunt group calls from ringing their phones.	For more information, refer to <i>Cisco Unified CallManager System Guide</i> , “Understanding Route Plans” chapter.
Malicious caller identification (MCID)	Allows users to notify the system administrator about suspicious calls that are received.	For more information refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Malicious Call Identification” chapter.

Table 6-1 Telephony Features for the Cisco Unified Wireless IP Phone 7921G (continued)

Feature	Description	Configuration Reference
Meet-Me conference	Allows a user to host a Meet-Me conference in which other participants call a predetermined number at a scheduled time.	For more information refer to <i>Cisco Unified CallManager Administration Guide</i> , “Meet-Me Number/Pattern Configuration” chapter.
Message waiting indicator	A light on the handset that indicates that indicates that a user has one or more new voice messages.	For more information refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Administration Guide</i>, “Message Waiting Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Voice Mail Connectivity to Cisco Unified CallManager” chapter.
Multilevel Precedence and Preemption (MLPP)	Provides a method of prioritizing calls within your phone system. Use this feature when users work in an environment where they need to make and receive urgent or critical calls.	For more information refer to <i>Cisco Unified CallManager Features and Services Guide</i> , “Multilevel Precedence and Preemption” chapter.
Music-on- hold	Plays music while callers are on hold.	For more information refer to <i>Cisco Unified CallManager Features and Services Guide</i> , “Music On Hold” chapter.
Onhook call transfer	Allows a user to press a single Transfer softkey and then go onhook to complete a call transfer.	For more information refer to <i>Cisco Unified CallManager System Guide</i> , “Cisco Unified IP Phones” chapter.

Table 6-1 **Telephony Features for the Cisco Unified Wireless IP Phone 7921G (continued)**

Feature	Description	Configuration Reference
Other group pickup	<p>Allows a user to answer a call ringing on a phone in another group that is associated with the user's group.</p> <p>(See also “Call pickup” and “Group call pickup” in this table.)</p>	<p>For more information refer to:</p> <ul style="list-style-type: none"> • <i>Cisco Unified CallManager 4.x Administration Guide</i>, “Call Pickup Group Configuration” chapter. • <i>Cisco Unified CallManager 4.x System Guide</i>, “Call Pickup” chapter. • <i>Cisco Unified CallManager 5.x Features and Services Guide</i>, “Call Pickup Group” chapter.
Privacy	<p>Prevents users who share a line from adding themselves to a call and from viewing information on their phone screens about the other user's calls.</p>	<p>For more information refer to:</p> <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i> “Barge and Privacy” chapter.
Push to Talk	<p>Allows users to call a target phone number or group and announce a message (similar to a two-way radio) by using a configurable applications button.</p>	<p>For more information, see “Setting Up Services” section on page 6-19. Requires an XML application to provide Push to Talk service.</p>

Table 6-1 Telephony Features for the Cisco Unified Wireless IP Phone 7921G (continued)

Feature	Description	Configuration Reference
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: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Quality Report Tool” chapter.
Redial	Allows users to call the most recently dialed phone number by using a softkey option.	Requires no configuration.
Ring setting	Identifies ring type used for a line when a phone has another active call.	For more information refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager 4.x Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager 5.x Administration Guide</i>, “Configuring Directory Numbers” chapter. • <i>Cisco Unified CallManager Features and Services Guide</i>, “Custom Phone Rings” chapter. • “Creating Custom Phone Rings” section on page 6-25.

Table 6-1 **Telephony Features for the Cisco Unified Wireless IP Phone 7921G (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: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phone Services” chapter.
Shared Line	Allows users to have multiple phones that share the same phone number or allows users to share a phone number with a coworker.	For more information refer to <i>Cisco Unified CallManager System Guide</i> , “Cisco Unified IP Phones” chapter.
Speed-dialing	Dials a specified number that has been previously stored.	For more information refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Cisco Unified IP Phones” chapter.
Time-of-Day Routing	Restricts access to specified telephony features by time period.	For more information refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Administration Guide</i>, “Time Period Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Time-of-Day Routing” chapter.

Table 6-1 **Telephony Features for the Cisco Unified Wireless IP Phone 7921G (continued)**

Feature	Description	Configuration Reference
Transfer	Allows users to redirect connected calls from their phones to another number.	Requires no configuration.
Voice message system	Enables callers to leave messages if calls are unanswered.	For more information refer to: <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Administration Guide</i>, “Cisco Voice-Mail Port Configuration” chapter. • <i>Cisco Unified CallManager System Guide</i>, “Voice Mail Connectivity to Cisco Unified CallManager” chapter.

**Note**

For detailed information about using telephony features on the wireless IP phone, refer to the *Cisco Unified Wireless IP Phone 7921G Guide*.

Related Topics

- [Configuring Softkey Templates, page 6-16](#)
- [Setting Up Services, page 6-19](#)
- [Configuring Corporate and Personal Directories, page 6-20](#)
- [Adding Users to Cisco Unified CallManager, page 6-22](#)
- [Creating Custom Phone Rings, page 6-25](#)

Specific Configuration Options for the Cisco Unified Wireless IP Phone 7921G

Each Cisco Unified IP Phone has special configuration options that are available for that phone model. You can configure the specific options by using Cisco Unified CallManager Administration. These product specific configuration options are available for the 7921 device type:

- **Disable Speakerphone**—Turns off the speakerphone capability of the handset. Options are False or True.
- **Gratuitous ARP**—Enables or disables the ability for the phone to learn MAC addresses from Gratuitous ARP. This capability is required to monitor or record voice streams. Options are Enabled or Disabled.
- **Settings Access**—Enables, disables, or restricts access to local configuration settings in the Settings menus. With restricted access, only the Phone Settings menu is accessible. With disabled access, no options appear when you access the Settings menu on the phone. Options are Enabled, Disabled, and Restricted.
- **Web Access**—Determines the level of access to the web pages for the phone. Provides Disabled, Read only, and Full access to a phone's web pages through a web browser. Options are Read Only, Full, Disabled.
- **Profile 1-4**—Locks or unlocks the network profiles. If locked, the phone user cannot modify the network profile. Options are Unlocked and Locked.
- **Load Server**—Identifies the alternate server that the phone will use to obtain firmware loads and upgrades. Enter an IP address or host name for the server.
- **Admin Password (Cisco Unified CallManager 5.0 and later)**—Password to access the configuration web pages for the phone. Default password is "CiscoCisco." Password must be 8-32 characters.

**Caution**

When setting the Administration Password in the Product Specific Configuration section in Cisco Unified CallManager 5.0 Administration, you must enable TFTP encryption. Otherwise, the password appears in readable text in the phone configuration file and can be viewed from any host that has access to TFTP server.

- **Special Numbers**—Identifies special phone numbers that do not require unlocking the keypad to call, such as 911 or an emergency number. Enter numbers up to 16 digits in length.
- **Push-to-talk URL**—Specifies the URL that the phone contacts when pressing the configurable Applications button for services such as Push to Talk or directories.

To configure product specific options, follow these steps:

Procedure

-
- Step 1** From Cisco Unified CallManager 4.x Administration, choose **Device > Phone**. Click **Add a Phone**, then choose **Phone Type > Cisco 7921**.
or
From Cisco Unified CallManager 5.x Administration, choose **Device > Phone**. Click **Add Phone**, then choose **Phone Type > Cisco 7921**.

- Step 2** In the Phone Configuration page, locate the **Product Specific Configuration** area.

- Step 3** Make changes to the settings as needed.



Note For detailed information about these settings, click the **I or ? button** for Product Specific Configuration Help.

- Step 4** You must reset the phone before the changes take effect.
-

Configuring Softkey Templates

Administrators can change the order of softkeys for the Cisco Unified Wireless IP Phone 7921G by using Cisco Unified CallManager Administration. Unlike other Cisco Unified IP Phones that have buttons for some functions, the Cisco Unified Wireless IP Phone 7921G has two non-configurable softkeys that are set for:

- Message
- Options

When you configure a softkey template for the Cisco Unified Wireless IP Phone 7921G, you can only configure the Cisco Unified CallManager softkeys and their sequence in the Options menu. The order of softkeys in the softkey template corresponds to the phone softkey list in the Options menu. When you set up the softkey template for users that prefer to have a particular softkey appear during a connected call, place the desired softkey in the first position for the Connected phone state.

Softkey Templates for the Cisco Unified Wireless IP Phone 7921G

The standard softkey template displays the Hold softkey when connected to a call. Some users want the Transfer softkey to appear for a connected call instead of Hold.

The administrator sets up a non-standard softkey template that places Transfer in the first position for the Connected state. The administrator assigns this non-standard softkey template to the 7921G devices assigned to users that want these softkeys.



Note

To ensure that users hear the voice-messaging greeting when they are transferred to the voice message system, you must set up a softkey template with Transfer as the first softkey for a connected call.

Changing Softkeys in a Template

Use the procedures in the online Help topic, “Adding Non-Standard Softkey Templates” to change the softkeys and their sequence. Softkey templates now support up to 16 softkeys when using applications. For more information about softkey templates, see the “Softkey Templates” Chapter in the *Cisco Unified CallManager System Guide*.

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

Related Topics

- [Configuring Cisco Unified Wireless IP Phones in Cisco Unified CallManager, page 6-2](#)
- [Setting Up Services, page 6-19](#)
- [Configuring Corporate and Personal Directories, page 6-20](#)
- [Adding Users to Cisco Unified CallManager, page 6-22](#)

Modifying Phone Button Templates

Phone button templates let you assign lines and features to positions in the Line View.

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. For more information about modifying phone button templates, refer to “Cisco Unified IP Phones” chapter in the *Cisco Unified CallManager System Guide* for your release.

The Cisco Unified Wireless IP Phone 7921G can have up to six lines and up to 24 connected calls. The default button template uses position 1 for lines and assigns position 2 through 6 as speed dial. You can assign these features to button positions:

- Service URL
- Privacy
- Speed dial

Use softkey features in the Options menu to access other phone features, such as call park, call forward, redial, hold, resume, conferencing, and so on.

Setting Up Services

The Services menu on the Cisco Unified Wireless IP Phone 7921G 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 Push to Talk, directories, stock quotes, and weather reports. Some services, such as Push to Talk, can use the configurable Applications button located on the side of the phone.

To create customized XML applications for your site, refer to the [Cisco Unified IP Phone Service Application Development Notes](#).

Before a user can access any service, two important tasks must be completed:

- You as the system administrator 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.

To set up IP Phone services, follow these steps:

Procedure

-
- Step 1** 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.

Step 2 To set up these services in Cisco Unified CallManager 4.x Administration, choose **Feature > Cisco IP Phone Services**

or

To set up these services in Cisco Unified CallManager 5.x Administration, choose **Device > Device Settings > Phone Services**

For more information about phone services, refer to the “Cisco Unified IP Phone Services” chapter in the *Cisco Unified CallManager System Guide* for more information.

Step 3 After you configure these services, verify that your users have access to the Cisco Unified CallManager User Options web-based application, from which they can select and subscribe to configured services. See the “[How Users Configure Phone Features and Services](#)” section on page A-6 for a summary of the information that you must provide to end users.

**Note**

For information about extension mobility services for users, refer to the “Cisco Extension Mobility” chapter in the *Cisco Unified CallManager Features and Services Guide*.

Related Topics

- [Configuring Cisco Unified Wireless IP Phones in Cisco Unified CallManager, page 6-2](#)
- [Configuring Softkey Templates, page 6-16](#)
- [Configuring Corporate and Personal Directories, page 6-20](#)
- [Adding Users to Cisco Unified CallManager, page 6-22](#)
- [Creating Custom Phone Rings, page 6-25](#)

Configuring Corporate and Personal Directories

The **Directory** menu on the Cisco Unified Wireless IP Phone 7921G 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 6-21](#) 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 6-21](#) for more information.

Configuring Corporate Directories

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

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

After the LDAP directory configuration completes, users can use the Corporate Directory service on your Cisco Unified Wireless IP Phone 7921G to look up users in the corporate directory.

Configuring Personal Directory

Personal Directory consists of the following features:

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

Users can access Personal Directory features by these methods:

- From a web browser—Users can access the PAB and Fast Dials features from the Cisco Unified CallManager User Options web pages

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

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

To synchronize with Microsoft Outlook, users must install the TABSynch utility, provided by you. To obtain the TABSynch software to distribute to users:

- From Cisco Unified CallManager 4.x Administration, choose **Application > Install Plugins**, then locate and click **Cisco IP Phone Address Book Synchronizer**.
- From Cisco Unified CallManager 5.x Administration, choose **Application > Plugins > Find**, then locate and click **Cisco IP Phone Address Book Synchronizer**.

Adding Users to Cisco Unified CallManager

Adding users to Cisco Unified CallManager allows you to display and maintain information about users and allows each user to perform the following 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 from Cisco Unified CallManager 4.x Administration, choose **User > Add a New User**.

To add users individually from Cisco Unified CallManager 5.x Administration, choose **User Management > End User > Add New**.

Refer to “Adding a New User” chapter in *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. This method also enables you to set an identical default password for all users.

For detailed information, refer to *Bulk Administration Tool User Guide* (Cisco Unified CallManager 4.1 or later) or *Cisco Unified CallManager Bulk Administration Guide* (Cisco Unified CallManager 5.0 or later).

Related Topics

- [Configuring Cisco Unified Wireless IP Phones in Cisco Unified CallManager, page 6-2](#)
- [Configuring Softkey Templates, page 6-16](#)
- [Setting Up Services, page 6-19](#)
- [Configuring Corporate and Personal Directories, page 6-20](#)
- [Creating Custom Phone Rings, page 6-25](#)

Managing the User Options Web Pages

From the User Options web page, users can customize and control several phone features and settings. For detailed information about the User Options web pages, refer to *Cisco Unified Wireless IP Phone 7921G Guide*.

Giving Users Access to the User Options Web Pages

Before a user can access the User Options web pages, you must use Cisco Unified CallManager Administration to configure the user as an End User. You must also associate appropriate phones with the user. To perform these procedures:

- From Cisco Unified CallManager 4.x Administration, choose **User > Add a New User**.
- From Cisco Unified CallManager 5.x Administration, choose **User Management > End User > Add New**.

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

**Note**

You can use Cisco Unified CallManager Administration to control user access to the phone web pages. For information about setting Web Access for users, see [“Specific Configuration Options for the Cisco Unified Wireless IP Phone 7921G”](#) section on page 6-15.

Specifying Options that Appear on the User Options Web Pages

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

- Show Ring Settings
- Show Line Text Label Settings

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

**Note**

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

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

Procedure

-
- Step 1** From Cisco Unified CallManager Administration, choose **System > Enterprise Parameters**.

The Enterprise Parameters Configuration page appears.

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

True—Option appears on all the User Options web pages (default).

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

Creating Custom Phone Rings

You can customize the phone ring types available at your site by using a set of phone ring sounds that are provided by Cisco Unified CallManager or by creating your own pulse code modulation (PCM) files and editing the RingList.xml file. Refer to the “Custom Phone Rings” chapter in the *Cisco Unified CallManager Features and Services Guide* for more information about customized ring tones.

Related Topics

- [Configuring Cisco Unified Wireless IP Phones in Cisco Unified CallManager, page 6-2](#)
- [Configuring Softkey Templates, page 6-16](#)
- [Setting Up Services, page 6-19](#)
- [Configuring Corporate and Personal Directories, page 6-20](#)
- [Adding Users to Cisco Unified CallManager, page 6-22](#)



CHAPTER 7

Viewing Security, Device, Model, and Status Information on the Phone

This chapter describes how to use the Settings menus on the Cisco Unified Wireless IP Phone 7921G to view information:

- Security Configuration menu—Displays information about security on the phone.
- Device Information menu—Displays information about the current phone configuration.
- 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.
- Call Statistics screen—Displays counters and statistics for the current call.

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

You can also obtain much of this information from the web page for the phone. For more information, see [Chapter 8, “Monitoring the Cisco Unified Wireless IP Phone Remotely.”](#)

For more information about troubleshooting the Cisco Unified IP Phone, [Chapter 9, “Troubleshooting the Cisco Unified Wireless IP Phone 7921G.”](#)

This chapter includes these topics:

- [Viewing Security Information, page 7-2](#)
- [Viewing Device Information, page 7-6](#)

- [Viewing Model Information, page 7-10](#)
- [Viewing the Phone Status Menu, page 7-12](#)

Viewing Security Information

To view the Security Configuration screen on the Cisco Unified Wireless IP Phone 7921G and see information about the security settings, follow these steps:

Procedure

-
- Step 1** Choose the **Settings > Security Configuration**.
- Step 2** Use the Navigation button to scroll through the items in the Security Configuration screen.
- Step 3** [Table 7-1](#) describes the items that appear in this screen.
- Step 4** To exit the Security Configuration screen, press the **Back** softkey.
-

Table 7-1 Security Configuration Screen Items

Item	Description
Web Access	<p>Indicates web access capability for the phone.</p> <ul style="list-style-type: none"> • Disabled—No user options web page access • ReadOnly—Can view information • Full—Can use configuration pages <p>You configure web access in Cisco Unified CallManager Administration.</p>
Security Mode	<p>Displays the security mode that is set for the phone. You configure the device security mode in Cisco Unified CallManager Administration.</p>

Table 7-1 Security Configuration Screen Items (continued)

Item	Description
MIC	Indicates whether a manufacturing installed certificate (used for the security features) is installed on the phone (Yes) or is not installed on the phone (No). For information about how to manage the MIC for your phone, refer to the “Using the Certificate Authority Proxy Function” chapter in <i>Cisco Unified CallManager Security Guide</i> .
LSC	Indicates whether a locally significant certificate (used for the security features) is installed on the phone or is not installed on the phone. For information about how to manage the LSC for your phone, refer to the “Using the Certificate Authority Proxy Function” chapter in <i>Cisco Unified CallManager Security Guide</i> .
CTL File	<p>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 Not Installed. (If security is configured for the phone, the CTL file installs automatically when the phone reboots or resets. For more information about this file, refer to the “Configuring the Cisco CTL Client” chapter in <i>Cisco Unified CallManager Security Guide</i>.)</p> <p>If a CTL file is installed on the phone, also provides access to the CTL File screen. For more information, see the “Accessing the CTL File Screen” section on page 7-4.</p>
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 or host name and the port of the CAPF that the phone uses.


Accessing the CTL File Screen


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



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

The CTL File screen contains these options:

- **CTL File**—Displays the MD5 hash of the certificate trust list (CTL) file that is installed in the phone, and provides access to the CTL File menu. If no CTL file is installed on the phone, this field displays Not Installed. (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*.)

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 / TFTP Server**—IP address of a Cisco Unified CallManager and TFTP server used by the phone. Also displays a certificate  icon if a certificate is installed for this server.



Note

When the wireless IP phone is connected to a Cisco Unified CallManager Release 5.0 or later, you can have multiple security profiles assigned to a phone. When the phone has more than one security profile using different secure Cisco Unified CallManager clusters, you must delete the CTL file from the current profile before enabling another profile. See [“Understanding Security Profiles” section on page 1-14](#).

If neither the primary TFTP (TFTP Server 1) server nor the backup TFTP server (TFTP Server 2) is listed in the CTL file, you must unlock the CTL file before you can save changes that you make to the TFTP Server 1 option or to the TFTP Server 2 option on the Network Configuration menu. (For information about changing these options, see the [“Configuring DHCP Settings” section on page 5-8.](#))

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

Procedure

- Step 1** Scroll to the CTL File menu and press Select.
- Step 2** Press ****#** to unlock options on the CTL File menu.
- If you decide not to continue, press ****#** again to lock options on this menu.
- Step 3** Scroll to the CTL option that you want to change and press **Erase**.
- After you make the change, the CTL file will be locked automatically.
-




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 access the Trust List screen by choosing **Settings > Security Configuration > Trust List**.

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

The Trust List screen contains these options:

- 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 / TFTP Server—IP address of a Cisco Unified CallManager and TFTP server used by the phone. Also displays a certificate  icon if a certificate is installed for this server.
- 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.

Related Topics

- [Viewing the Status Messages, page 7-12](#)
- [Viewing Call Statistics, page 7-18](#)
- [Viewing Firmware Versions, page 7-22](#)

Viewing Device Information

You can access the Device Information screen on the Cisco Unified Wireless IP Phone 7921G and to view information about the current configuration:

- Cisco CallManager servers
- Network settings
- WLAN information
- HTTP information
- Locale information
- Security settings
- QoS information

To view the Device Information screen, follow these steps:

Procedure

-
- Step 1** Choose **Settings menu > Device Information**.
- Step 2** Use the Navigation button to scroll to one of the categories in the Device Information screen and press **Select**.
- The list of items under the category displays.
- Step 3** [Table 7-2](#) describes the categories and items that appear in this screen.
- Step 4** To exit the Device Information screen, press the **Back** softkey.
-

Table 7-2 *Device Information Categories and Items*

Item	Description
Step 1 CallManager Information	
Call Manager 1–5	<p>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.</p> <p>Each available server displays the Cisco Unified CallManager server IP address and one of the following states:</p> <ul style="list-style-type: none"> • 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.
Network Information	
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address.
MAC Address	Media Access Control (MAC) address of the phone.
Host Name	Unique, fixed name that is automatically assigned to the phone based on the MAC address.
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.

Table 7-2 *Device Information Categories and Items (continued)*

Item	Description
TFTP Server 2	Secondary Trivial File Transfer Protocol (TFTP) server used by the phone.
Default Router 1	IP address for the default gateway used by the phone.
DNS Server 1	Primary Domain Name System (DNS) server used by the phone.
DNS Server 2	Backup DNS server used by the phone.
Load Server	Host name or IP address for the alternate server that the phone uses for firmware upgrades.
CDP Enabled	Indicates whether the network is using Cisco Discovery Protocol (CDP).
DHCP Enabled	Indicates whether this phone is using DHCP for its IP address assignment or not.
Alternate TFTP	Indicates whether this phone uses a TFTP server other than the one assigned by DHCP.
WLAN Information	
Profile Name	Name of the network profile that the phone is currently using.
SSID	Service Set ID that the phone is currently using.
802.11 Mode	Wireless signal mode that the phone is currently using.
Single Access Point	Indicates if the phone minimizes scanning (Enabled) or scans for APs frequently (Disabled).
Call Power Save Mode	Type of power save mode that the phone uses to save battery power—PS-Poll or U-APSD.
Security Mode	Authentication method that the phone is currently using in the wireless network.
Encryption Type	Encryption method that the phone is currently using in the wireless network.
Key Management	Encryption key management that the phone is currently using in the wireless network.
Tx Power	Transmit power setting for the phone.

Table 7-2 *Device Information Categories and Items (continued)*

Item	Description
HTTP Information	
Information URL	URL of the help text that appears on the phone.
Directories URL	URL of the server from which the phone obtains directory information.
Messages URL	URL of the server from which the phone obtains message services.
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.
Idle URL	Not used.
Proxy Server URL	Not used.
Authentication URL	URL that the phone uses to validate requests made to the phone web server.
Locale Information	
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.
Security Information	
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.
Security Mode	Security mode assigned to the phone.

Table 7-2 *Device Information Categories and Items (continued)*

Item	Description
Web Access	Indicates web access capability for the phone. <ul style="list-style-type: none"> Disabled—No user options web page access ReadOnly—Can view information only Full—Can use configuration pages You configure web access in Cisco Unified CallManager Administration.
QoS Information	
DSCP for Call Control	Differentiated Services Code Point (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 service.

Related Topics

- [Viewing Security Information, page 7-2](#)
- [Viewing Model Information, page 7-10](#)
- [Viewing the Phone Status Menu, page 7-12](#)

Viewing Model Information

You can view the Model Information screen on the Cisco Unified Wireless IP Phone 7921G to see information about the hardware and software.

To view this screen, follow these steps:

Procedure

-
- Step 1** Choose **Settings > Model Information**.
- Step 2** Use the Navigation button to scroll through the items in the Model Information screen.

Step 3 [Table 7-3](#) describes the items that appear in this screen.

Step 4 To exit the Model Information screen, press the **Back** softkey.

Table 7-3 *Model Information Screen Items*

Item	Description
Model Number	Model number of the phone.
MAC Address	MAC address of the phone.
App Load ID	Identifier of the factory-installed load running on the phone.
Serial Number	Serial number of the phone.
WLAN Regulatory Domain	Identifier for the wireless regulatory domain in which this phone must operate. <ul style="list-style-type: none"> • 1050—North America • 3051—Europe (ETSI) • 4153—Japan • 5252—World mode including Australia/New Zealand, Asia, and Pacific
USB Vendor ID	Unique code that identifies the vendor as a Cisco Systems.
USB Product ID	Unique code that identifies the phone as a Cisco Systems product.
RNDIS Device Address	Manufacturer-assigned unique MAC address for the USB Remote Network Driver Interface Specification (RNDIS) for the phone.
RNDIS Host Address	Manufacturer-assigned unique MAC address for the USB RNDIS for the host.

Related Topics

- [Viewing Security Information, page 7-2](#)
- [Viewing Device Information, page 7-6](#)

- [Viewing the Phone Status Menu, page 7-12](#)

Viewing the Phone Status Menu

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

- **Status Messages**—Displays the Status Messages screen, which shows a log of important system messages. For more information, see the [“Viewing the Status Messages” section on page 7-12](#).
- **Network Statistics**—Displays the Network Statistics screen, which shows Ethernet traffic statistics. For more information, see the [Viewing Network Statistics, page 7-16](#).
- **Call Statistics**—Displays the Call Statistics screen, which shows counters, statistics, and voice quality metrics. For more information, see the [Viewing Call Statistics, page 7-18](#).
- **Firmware Versions**—Displays the Firmware Versions screen, which shows information about the firmware running on the phone. For more information, see the [Viewing Firmware Versions, page 7-22](#).

Viewing the Status Messages

You can use the Settings menu and Status menu to view status messages for the Cisco Unified Wireless IP Phone 7921G. The Status Messages screen displays up to 10 of the 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 indicated errors.

To view status messages, follow these steps:

-
- Step 1** Choose **Settings > Status**.
- Step 2** Select **Status Messages**.; the list of the status messages displays.

To erase the messages, press the **Clear** softkey

Step 3 To exit the screen, press the **Back** softkey.

Table 7-4 *Status Messages*

Message	Description	Possible Explanation and Action
Bad MIC on phone	The manufacturing installed certificate (MIC) that is used for security features is bad.	For information about how to manage the MIC for your phone, refer to the “Using the Certificate Authority Proxy Function” chapter in <i>Cisco Unified CallManager Security Guide</i> .
CFG file not found	The name-based and default configuration file was not found on the TFTP Server.	<p>The configuration file for a phone is created when the phone is added to the Cisco Unified CallManager database. If the phone has not been added to the Cisco Unified CallManager database, the TFTP server generates a <code>CFG File Not Found</code> response.</p> <ul style="list-style-type: none"> • 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 “Methods for Adding Phones to Cisco Unified CallManager” section on page 3-3 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 “Configuring IP Network Settings” section on page 4-21 for details on assigning a TFTP server.

Table 7-4 Status Messages (continued)

Message	Description	Possible Explanation and Action
CTL Installed	A certificate trust list (CTL) file is installed in the phone.	None. This message is informational only. For more information about the CTL file, refer to <i>Cisco Unified CallManager Security Guide</i> .
CTL update failed	The phone could not update its certificate trust list (CTL) file.	Problem with the CTL file on the TFTP server. For more information, refer to <i>Cisco Unified CallManager Security Guide</i> .
Duplicate IP	Another device is using the IP address assigned to the phone.	<ul style="list-style-type: none"> • If the phone has a static IP address, verify that you have not assigned a duplicate IP address. See the “Configuring IP Network Settings” section on page 4-21 section for details. • If you are using DHCP, check the DHCP server configuration.
LCS operation failed	The locally significant certificate (LSC) that is used for the security features did not install properly.	For information about how to manage the LSC for your phone, refer to the “Using the Certificate Authority Proxy Function” chapter in <i>Cisco Unified CallManager Security Guide</i> .
LCS operation complete	The LCS was updated successfully on the phone.	For information about how to manage the LSC for your phone, refer to the “Using the Certificate Authority Proxy Function” chapter in <i>Cisco Unified CallManager Security Guide</i> .
TFTP Error	The phone does not recognize an error code provided by the TFTP server.	Contact the Cisco TAC.

Table 7-4 **Status Messages (continued)**

Message	Description	Possible Explanation and Action
TFTP server not authorized	The specified TFTP server could not be found in the phone CTL.	<ul style="list-style-type: none"> • The DHCP server is not configured properly and is not providing 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.	<ul style="list-style-type: none"> • Network is busy—The errors should resolve themselves when the network load reduces. • No network connectivity between the TFTP server and the phone—Verify the network connections. • TFTP server is down—Check configuration of TFTP server.

Viewing the Current Configuration

You can use the Settings menu and Status menu to determine the name of the configuration file for the Cisco Unified Wireless IP Phone 7921G.

To locate the configuration file name, follow these steps:

Procedure

Step 1 Choose **Settings > Status**.

Step 2 Select **Status Messages**.

The phone displays the name of the configuration file in the following format: SEP*macaddress*.cnf.xml or SEP*macaddress*.cnf.xml.enc.sgn.

Step 3 To exit the screen, press the **Back** softkey.

Related Topics

- [Viewing the Status Messages, page 7-12](#)
- [Viewing Network Statistics, page 7-16](#)
- [Viewing Call Statistics, page 7-18](#)
- [Viewing Firmware Versions, page 7-22](#)

Viewing Network Statistics

You can use the Settings menu and Status menu to view information about the phone and network performance.

To view the Network Statistics follow these steps:

Procedure

Step 1 Press the **Settings > Status**.

Step 2 Select **Network Statistics**; the list of statistics displays.

Step 3 Use the Navigation button to scroll through the items in the Network Statistics screen.

Step 4 [Table 7-5](#) describes the items that appear in this screen.

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

Table 7-5 Network Statistics Screen Items

Item	Description
Up Time	Amount of elapsed time in days and hours since the phone connected to Cisco Unified CallManager
RxPkts	Number of packets received by the phone
RxErr	Number of errored packets received by the phone
RxUcast	Number of unicast packets received by the phone
RxMcast	Number of multicast packets received by the phone
RxBcast	Number of broadcast packets received by the phone
FcsErr	Number of packets with frame checksum (FCS) errors
Tx Failed	Number of packet transmissions that failed
RcvBeacons	Number of beacons received by the phone
AssocRej	Number of AP association rejections
AssocTmOut	Number of AP association timeouts
AuthRej	Number of authentication rejections
AuthTmOut	Number of authentication timeouts
The following network statistics items display two values for these AP queues: Best Effort and Voice	
TxPkts	Number of packets transmitted by the phone
TxErr	Number of transmit errors
TxUcast	Number of unicast packets transmitted by the phone
TxMcast	Number of multicast packets transmitted by the phone
TxBcast	Number of broadcast packets transmitted by the phone
RTSFail	Number of request to send (RTS) failures
ACKFail	Number of packet acknowledgements that failed
Retry	Number of times the phone retried to send packets
MRetry	Number of times the phone retried to send multicast packets

Table 7-5 Network Statistics Screen Items (continued)

Item	Description
RetryFail	Number of times the phone retried and failed to send packets
AgedPkts	Number of packets removed from the transmit queue due to transmission timeout
OtherFail	Number of packets that failed to transmit due to other reasons
Success	Number of packets successfully transmitted
MaxFail	Maximum sequence of failure due to maximum retry limit

Related Topics

- [Viewing the Status Messages, page 7-12](#)
- [Viewing Call Statistics, page 7-18](#)
- [Viewing Firmware Versions, page 7-22](#)

Viewing Call Statistics

You can access the Call Statistics screen on the phone to display counters, statistics, and voice quality metrics in these ways:

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

**Note**

You can remotely view the call statistics information by using a web browser to access the Streaming Statistics web page. For more information about remote monitoring, see [Chapter 8, “Monitoring the Cisco Unified Wireless IP Phone Remotely.”](#)

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

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

Procedure

-
- Step 1** Press **Settings > Status**.
- Step 2** Scroll to and select **Call Statistics**; the list of statistics appears.
- Step 3** Use the Navigation button to scroll through the items in the Call Statistics screen. [Table 7-6](#) describes the items that appear in this screen.
- Step 4** To exit the Call Statistics screen, press the **Back** softkey.
-

Table 7-6 *Call Statistics Items*

Item	Description
Rcvr Codec	Type of voice stream received (RTP streaming audio): G.729, G.711 u-law, G.711 A-law, or Lin16k.
Sender Codec	Type of voice stream transmitted (RTP streaming audio): G.729, G.711 u-law, G.711 A-law, or Lin16k.
Rcvr Size	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).
Sender Size	Size of voice packets, in milliseconds, in the transmitting voice stream.

Table 7-6 Call Statistics Items (continued)

Item	Description
Rcvr Packets	<p>Number of RTP voice packets received since voice stream was opened.</p> <p>Note This number is not necessarily identical to the number of RTP voice packets received since the call began because the call might have been placed on hold.</p>
Sender Packets	<p>Number of RTP voice packets transmitted since voice stream was opened.</p> <p>Note This number is not necessarily identical to the number of RTP voice packets transmitted since the call began because the call might have been placed on hold.</p>
Avg Jitter (value1/value2)	<p>Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network).</p> <ul style="list-style-type: none"> • Value 1 is the average jitter in milliseconds (ms). • Value 2 is the current audio frame buffer depth in millisecond (ms).
Max Jitter	<p>Maximum jitter observed since the receiving voice stream was opened.</p>
Rcvr Discarded	<p>Number of RTP packets in the receiving voice stream that have been discarded (bad packets, too late, and so on).</p> <p>Note The phone will discard payload type 19 comfort noise packets that are generated by Cisco Gateways, which will increment this counter.</p>
Rcvr Lost Packets	<p>Missing RTP packets (lost in transit).</p>

Table 7-6 Call Statistics Items (continued)

Item	Description
Voice Quality Metrics	
MOS LQK	<p>Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see the “Monitoring the Voice Quality of Calls” section on page 9-17.</p> <p>Note The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.</p>
Avg MOS LQK	Average MOS LQK score observed for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream.
Max MOS LQK	<p>Baseline or highest MOS LQK score observed from start of the voice stream.</p> <p>These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss:</p> <ul style="list-style-type: none"> • G.711 gives 4.5 • G.729 A /AB gives 3.7
MOS LQK Version	Version of the Cisco proprietary algorithm used to calculate MOS LQK scores.
CumConcealRatio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
IntConcealRatio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.

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

Item	Description
MaxConcealRatio	Highest interval concealment ratio from start of the voice stream.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
SevConcealSecs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.

Related Topics

- [Viewing the Status Messages, page 7-12](#)
- [Viewing Network Statistics, page 7-16](#)
- [Viewing Firmware Versions, page 7-22](#)

Viewing Firmware Versions

You can verify the firmware versions that are used on the Cisco Unified Wireless IP Phone 7921G by viewing the Firmware Info screen.

The firmware version name is in this format:

```
Product_Name-Model-Protocol.Version Number.Filetype
```

Examples of firmware releases are these

- Cisco Unified CallManager 4.1 and later
cmterm-7921-sccp.X-0-0.exe
- Cisco Unified CallManager 5.04 and later
cmterm-7921-sccp.X-0-0.cop.sgn

Table 7-7 explains the information that is displayed on this screen.

To display the firmware information, follow these steps:

Procedure

-
- Step 1** Choose **Settings > Status**.
- Step 2** Select **Firmware Versions**.
To view one of the items, scroll to the item and press **Select**.
- Step 3** To exit the Firmware Versions screen, press **Back**.
-

Table 7-7 *Firmware Version Information*

Item	Description
App Load ID	Identifies the phone firmware version running in the phone
Boot Load ID	Identifies the factory-installed load running on the phone
WLAN Driver ID	Identifies the version of the wireless LAN driver
WLAN Firmware ID	Identifies the Wireless LAN firmware version running in the phone

Related Topics

- [Viewing the Status Messages, page 7-12](#)
- [Viewing Network Statistics, page 7-16](#)
- [Viewing Call Statistics, page 7-18](#)

■ Viewing the Phone Status Menu



CHAPTER 8

Monitoring the Cisco Unified Wireless IP Phone Remotely

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

- Home—Summary information about the phone
- Setup—Configurable settings for network profiles, USB port, and trace data
- Information—Network and device static information
- Statistics—Wireless LAN and IP network data
- Stream Statistics—Displays counters and statistics for the current call
- System—Configurable settings for trace logs, backup, phone upgrades, and web page password

You can use Setup pages and System pages to configure settings for the Cisco Unified Wireless IP Phone 7921G. For information about using these web pages, see [Chapter 4, “Using the Cisco Unified Wireless IP Phone 7921G Web Pages.”](#)

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

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

For more information about troubleshooting the Cisco Unified IP Phone, [Chapter 9, “Troubleshooting the Cisco Unified Wireless IP Phone 7921G.”](#)

This chapter includes these topics:

- [Accessing the Web Page for a Phone, page 8-2](#)
- [Summary Information, page 8-3](#)
- [Network Configuration Information, page 8-4](#)
- [Device Information, page 8-9](#)
- [Wireless LAN Statistics, page 8-11](#)
- [Network Statistics, page 8-13](#)
- [Stream Statistics, page 8-16](#)

Accessing the Web Page for a Phone

To access the web page for a Cisco Unified IP Phone, follow these steps:

Procedure

-
- Step 1** Obtain the IP address of the Cisco Unified Wireless IP Phone 7921G using one of these methods:
- Search for the phone in Cisco Unified CallManager by choosing **Devices > Phones**. Phones registered with Cisco Unified CallManager display the IP address on the Find and List Phones web page and at the top of the Phone Configuration web page.
 - On the Cisco Unified Wireless IP Phone 7921G, press **Settings > Device Information > Network** 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:

`https://<IP_address>`



Note When the Security Alert dialog box displays a notice to accept the Trust Certificate, click **Yes** or **Always** to accept the application.

- Step 3** Log in to the web pages with username: **admin** and enter the password: **Cisco** for the phone web pages.

The web pages for a Cisco Unified Wireless IP Phone 7921G includes these items for monitoring the phone:

- **Summary Information**—Displays general information about the phone. For more information, see the [“Summary Information” section on page 8-3](#).
- **Network Information**—Displays network configuration information and information about other phone settings. For more information, see the [“Network Configuration Information” section on page 8-4](#).
- **Device Information**—Displays device settings and related information for the phone. For more information, see the [“Device Information” section on page 8-9](#).
- **Wireless LAN Statistics**—Provides information about the wireless LAN configuration. For more information, see the [“Wireless LAN Statistics” section on page 8-11](#).
- **Network Statistics**—Provides information about network traffic. For more information, see the [“Network Statistics” section on page 8-13](#).
- **Stream Statistics**—Provides information about voice quality items. For more information, see the [“Stream Statistics” section on page 8-16](#).

Summary Information

The Summary Information area on the phone’s web page displays network configuration information and information about other phone settings. [Table 8-1](#) describes these items.

To display the Summary Information page, access the web page for the phone as described in the [“Accessing the Web Page for a Phone” section on page 8-2](#), and the Home: Summary page displays.

Table 8-1 Home: Summary Items

Item	Description
Phone DN	Directory number assigned to this phone

Table 8-1 Home: Summary Items (continued)

Item	Description
Wireless Information	
Active Network Profile	Name of the profile that the phone is currently using
SSID	SSID that the phone is currently using
Access Point	Name of the access point to which the phone is associated
MAC Address	Media Access Control (MAC) address of the phone
Network Information	
IP Address	Internet Protocol (IP) address of the phone
Subnet Mask	Subnet mask used by the phone
Default Router	IP address for the default gateway that the phone is using
TFTP Server	IP address for the Primary Trivial File Transfer Protocol (TFTP) server that the phone is using
CallManager Information	
Active CallManager	IP address for the Cisco Unified CallManager server to which the phone is registered
Phone Directory Number	Primary directory number for the phone

Network Configuration Information

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

To display the Network Information page, 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** hyperlink under the Information section.

Table 8-2 Network Information Items

Item	Description
IP Information	
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IP address.
BootP Server	Not used.
MAC Address	Media Access Control (MAC) address of the phone.
Host Name	Unique, fixed name that is automatically assigned to the phone based on the MAC address.
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.
Default Router 1	IP address for the default gateway used by the phone.
DNS Server 1	Primary Domain Name System (DNS) server used by the phone.
DNS Server 2	Backup DNS server used by the phone.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone.
Alternate TFTP Server Enabled	Displays Yes if enabled and No if disabled.
TFTP Server 2	Secondary Trivial File Transfer Protocol (TFTP) server used by the phone.
CallManager Information	

Table 8-2 *Network Information Items (continued)*

Item	Description
Call Manager 1–5	<p>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.</p> <p>Each available server shows the Cisco Unified CallManager server IP address and one of the following states:</p> <ul style="list-style-type: none"> • 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.

Table 8-2 *Network Information Items (continued)*

Item	Description
SRST Information	
SRST Reference IP	<p>The IP Address for the Survivable Remote Site Telephony (SRST) designation, which identifies an SRST router capable of providing Cisco Unified CallManager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified CallManager servers become unreachable. The SRST Cisco Unified CallManager always appears last in the list of servers, even if it is active.</p> <p>An item will include a shield icon if the phone has an authenticated connection to the Cisco Unified CallManager server. It will display a padlock icon if the phone has an authenticated connection to the Cisco Unified CallManager server.</p>
SRST Reference Port	Port number for TCP connection.
SRST Reference Option	Identifies the default gateway or disables SRST.
Connection Monitor Duration	The amount of time that the IP phone monitors its connection to Cisco Unified CallManager before it unregisters from SRST and re-registers to Cisco Unified CallManager.
MLPP Information	
MLPP Domain ID	Identifies the MLPP Domain that is assigned to the phone.
MLPP Indication Status	Indicates whether the phone uses special precedence rings and tones.

Table 8-2 *Network Information Items (continued)*

Item	Description
Preemption	Identifies call preemption capability set for this phone. Forceful—The phone allows higher priority calls to preempt lower priority calls. Disabled—The phone does not preempt lower priority calls with higher priority calls. Default—The phone uses the device pool setting.
QoS Information	
DSCP for Call Control	Differentiated Services Code Point (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 service.
Security Information	
GARP Enabled	Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.
Web Access Enabled	Indicates whether access to phone web pages is enabled (Yes) or disabled (No).
Settings Enabled	Indicates whether the Settings menu on the phone is accessible.
Security Mode	Indicates the security mode assigned to the phone
URL Information	
Information URL	URL of the help text that appears on the phone.
Directories URL	URL of the server from which the phone obtains directory information.
Messages URL	URL of the server from which the phone obtains message services.
Services URL	URL of the server from which the phone obtains Cisco Unified IP Phone services.
Idle URL	Not used.
Idle URL Timer	Not used.

Table 8-2 Network Information Items (continued)

Item	Description
Proxy Server URL	Not used.
Authentication URL	URL that the phone uses to validate requests made to the phone web server.
Locale Information	
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.
User Locale Version	Version of the user locale loaded on the phone.
User Locale Char Set	Character set that the phone uses for the user locale.
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.
Network Locale Version	Version of the network locale loaded on the phone.

Device Information

The Device Information web page displays device settings and related information for the phone. [Table 8-3](#) 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** hyperlink under the information area.

Table 8-3 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
Directory Number	Directory number assigned to the phone
System Load ID	Identifier of the firmware running on the phone
Version	Version of the phone hardware
Serial Number	Serial number of the phone
Model Number	Model number of the phone
Message Waiting	Indicates if there is a voice message waiting on any line for this phone
UDI	Displays the following Cisco Unique Device Identifier (UDI) information about the phone: <ul style="list-style-type: none"> • Device Type—Indicates hardware type such as phone • Device Description—Displays the name of the phone associated with the model type. • Product Identifier—Specifies the phone model • Version Identifier—Represents the hardware version of the phone • Serial Number—Displays the phone's unique serial number
Time	Time from the Date/Time Group in Cisco Unified CallManager
TimeZone	Time zone obtained from the Date/Time Group in Cisco Unified CallManager
Date	Date obtained from the Date/Time Group in Cisco Unified CallManager
Hardware Revision	Version of the phone hardware

Table 8-3 Device Information Area Items (continued)

Item	Description
WLAN Regulatory Domain	Identifier for the wireless regulatory region in which this phone must operate
USB Vendor/Product ID	Unique code that identifies the phone as a Cisco Systems product
USB RNDIS Device Address	Manufacturer-assigned unique MAC address for the USB Remote Network Driver Interface Specification (RNDIS) for the phone
USB RNDIS Host Address	Manufacturer-assigned unique MAC address for the USB RNDIS for the host

Wireless LAN Statistics

The Wireless LAN Statistics area on a phone's web page provides information about wireless network traffic on the phone. [Table 8-4](#) describes the items in this area.

To display a wireless LAN 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 **Wireless LAN** hyperlink under Statistics.

Table 8-4 Wireless LAN Statistics Items

Item	Description
Rx Statistics	
Rx OK Frames	Number of packets received successfully
Rx Error Frames	Number of packets received with errors
Rx Unicast Frames	Number of packets received that are unicast traffic
Rx Multicast Frames	Number of packets received that are multicast traffic
Rx Broadcast Frames	Number of packets received that are broadcast traffic
Rx FCS Frames	Number of packets received frames checksum error
Rx Beacons	Number of received beacons

Table 8-4 *Wireless LAN Statistics Items (continued)*

Item	Description
Association Rejects	Number of rejected association attempts
Association Timeouts	Number of failed association attempts due to timeout
Authentication Rejects	Number of authentication attempts that the AP rejected
Authentication Timeouts	Number of failed authentication attempts due to timeout
Tx Statistics (Best Effort)	
Tx OK Frames	Number of frames transmitted with successfully
Tx Error Frames	Number of frames transmitted with errors
Tx Unicast Frames	Number of frames transmitted that are unicast traffic
Tx Multicast Frames	Number of frames transmitted that are multicast traffic
Tx Broadcast Frames	Number of frames transmitted that are broadcast traffic
RTS Fail Counter	Number of RTS transmissions that did not result in transmitted frames
ACK Fail Counter	Number of failed acknowledgements by the AP
Retries Counter	Number of frames that were retransmitted
Multiple Retries Counter	Number of frames for which retransmission was attempted
Failed Retries Counter	Number of frames without acknowledgements
Tx Timeout Counter	Number of frames that could not be retransmitted due to timeout
Other Fail Counter	Number of frames with failed transmission due to other causes
Success Counter	Number of frames transmitted successfully
Max Retry Limit Counter	Number of times the maximum retry limit was reached

Table 8-4 *Wireless LAN Statistics Items (continued)*

Item	Description
Tx Statistics (Voice)	
Tx OK Frames	Number of frames transmitted with successfully
Tx Error Frames	Number of frames transmitted with errors
Tx Unicast Frames	Number of frames transmitted that are unicast traffic
Tx Multicast Frames	Number of frames transmitted that are multicast traffic
Tx Broadcast Frames	Number of frames transmitted that are broadcast traffic
RTS Fail Counter	Number of RTS transmissions that did not result in transmitted frames
ACK Fail Counter	Number of failed acknowledgements by the AP
Retries Counter	Number of frames that were retransmitted
Multiple Retries Counter	Number of frames for which retransmission was attempted
Failed Retries Counter	Number of frames without acknowledgements
Tx Timeout Counter	Number of frames that could not be retransmitted due to timeout
Other Fail Counter	Number of frames with failed transmission due to other causes
Success Counter	Number of frames transmitted successfully
Max Retry Limit Counter	Number of times the maximum retry limit was reached

Network Statistics

These Network Statistics area on a phone's web page provides information about network traffic on the phone. [Table 8-5](#) describes the items in this area.

To display the 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 **Network** hyperlink under Statistics.

Table 8-5 Network Statistics Screen Items

Item	Description
IP Statistics	
IpInReceives	Number of input datagrams received from interfaces including those received in error
IpInHdrErrors	Number of input datagrams discarded due to errors in IP headers
IpInAddrErrors	Number of input datagrams discarded because IP address in header destination field was not valid
IpInForwDatagrams	Number of input datagrams that were forwarded to another IP destination
IpInUnknownProtos	Number of datagrams discarded because of an unknown or unsupported protocol
IpInDiscards	Number of input datagrams discarded for reasons other than errors, such as lack of buffer space
IpInDelivers	Number of input datagrams successfully delivered to IP user-protocols
IpInOutRequests	Number of IP datagrams supplied to IP in request for transmission; does not include IPForwDatagram count
IpInOutDiscards	Number of output datagrams discarded for reasons other than errors, such as lack of buffer space
IpInOutNoRoutes	Number of output datagrams discarded because no route found to transmit them to destination
IpInReasmTimeout	Maximum number of seconds which received fragments are held while awaiting reassembly
IpReasmReqds	Number of IP fragments received that need to be reassembled
IpInReasmOKs	Number of IP fragments successfully reassembled
IpInReasmFails	Number of IP fragment reassembly failures
IpInFragOK	Number of IP datagrams that have been successfully fragmented

Table 8-5 *Network Statistics Screen Items (continued)*

Item	Description
IpInFragFails	Number of IP datagrams that were discarded because they could not be fragmented
IpInFragCreates	Number of IP datagram fragments generated
TCP Statistics	
TcpRtoAlgorithm	Determines timeout value used for retransmitting unacknowledged octets
TcpRtoMin	Minimum value for retransmission timeout in milliseconds
TcpRtoMax	Maximum value for retransmission timeout in milliseconds
TcpMaxConn	Number limit for total TCP connections that are supported; if dynamic, displays value of -1
TcpActiveOpens	Number of times TCP connections made a transition to SYN-SENT state from CLOSED state
TcpPassiveOpens	Number of times TCP connections made a transition to SYN-RCVD state from LISTEN state
TcpAttemptFails	Number of times TCP connections made a transition to CLOSED state from SYN-SENT or SYN-RCVD state, plus number of times transitioned to LISTEN state from SYN-RCVD state
TcpEstablishResets	Number of times TCP connections made a transition to CLOSED state from either ESTABLISHED or CLOSE-WAIT state
TcpCurrEstab	Number of times TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT state
TcpInSegs	Number of segments received including those in error on current connections
TcpOutSegs	Number of segments sent including those on current connections; excludes segments containing only retransmit octets

Table 8-5 Network Statistics Screen Items (continued)

Item	Description
TcpRetransSegs	Number of TCP segments transmitted containing previously transmitted octets
TcpInErrs	Number of segments with bad TCP checksum
TcpOutRsts	Number of TCP segments sent containing RST flag
UDP Statistics	
UdpInDatagrams	Number of UDP datagrams delivered to UDP users
UdpNoPorts	Number of received UDP datagrams for which there was not application at the destination port
UdpInErrors	Number of received UDP datagrams not delivered for reasons other than no application at port
UdpOutDatagrams	Number of datagrams sent

Stream Statistics

A phone streams information when it is on a call or running a service that sends or receives audio or data. The call statistics area on a phone's web page provides information about this stream. [Table 8-6](#) 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 **Stream 1** or **Stream 2** hyperlink under Stream Statistics.

Table 8-6 Stream Statistics Items

Item	Description
Domain Name	Domain of the phone
Remote Address	IP address of the destination stream
Remote Port	Port number of the destination
Local Address	IP address of the phone
Local Port	Port number of the phone

Table 8-6 Stream Statistics Items (continued)

Item	Description
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	Indicates whether the phone is streaming
Host Name	Host name for the phone
Sender Packets	Number of RTP voice packets transmitted since voice stream was opened Note This number is not necessarily identical to the number of RTP voice packets transmitted since the call began because the call might have been placed on hold.
Sender Octets	Total number of octets sent by the phone
Sender Tool	Type of audio encoding used for the stream: G.729, G.711 u-law, G.711 A-law, or Lin16k
Sender Reports	Number of times this streaming statistics report has been accessed from the web page (resets when the phone resets)
Sender Report Time	Internal time stamp indicating when this streaming statistics report was generated
Sender Start Time	Time that the stream started

Table 8-6 Stream Statistics Items (continued)

Item	Description
Receiver Packets	<p>Number of RTP voice packets received since voice stream was opened</p> <p>Note This number is not necessarily identical to the number of RTP voice packets received since the call began because the call might have been placed on hold.</p>
Receiver Octets	Total number of octets received by the phone
Receiver Tool	Type of audio encoding used for the stream: G.729, G.711 u-law, G.711 A-law, or Lin16k
Receiver Lost Packets	Number of missing RTP packets (lost in transit)
Receiver Jitter	Maximum RTP packet jitter (dynamic delay that a packet encounters when going through the network) observed since the receiving voice stream was opened
Receiver Reports	Number of times this streaming statistics report has been accessed from the web page (resets when the phone resets)
Receiver Start Time	Internal time stamp indicating when Cisco Unified CallManager requested that the phone start receiving packets
Voice Quality Metrics	
MOS LQK	<p>Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. For more information, see the “Monitoring the Voice Quality of Calls” section on page 9-17</p> <p>Note The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.</p>
Avg MOS LQK	Average MOS LQK score observed for the entire voice stream

Table 8-6 Stream Statistics Items (continued)

Item	Description
Min MOS LQK	Lowest MOS LQK score observed from start of the voice stream
Max MOS LQK	<p>Baseline or highest MOS LQK score observed from start of the voice stream</p> <p>These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss:</p> <ul style="list-style-type: none"> • G.711 gives 4.5 • G.729 A /AB gives 3.7
MOS LQK Version	Version of the Cisco proprietary algorithm used to calculate MOS LQK scores
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds)
Severely Conceal Secs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream

Related Topic

[Monitoring the Voice Quality of Calls, page 9-17](#)



CHAPTER 9

Troubleshooting the Cisco Unified Wireless IP Phone 7921G

This chapter provides information that can assist you in troubleshooting problems with your Cisco Unified Wireless IP Phone, in your IP telephony network, or with using the Cisco Unified Wireless IP Phone 7921G web pages.

For additional troubleshooting information, you can refer to the *Cisco Unified CallManager Troubleshooting Guide*.

This chapter includes the following sections:

- [Resolving Startup and Connectivity Problems, page 9-1](#)
- [Resolving Voice Quality and Roaming Problems, page 9-11](#)
- [General Troubleshooting Information, page 9-20](#)
- [Erasing the Local Configuration, page 9-25](#)

Resolving Startup and Connectivity Problems

After installing a unified IP phone on your network and adding it to Cisco Unified CallManager, the phone should start up as described in the [“Understanding the Phone Startup Process”](#) section on page 3-26. If the phone does not start up properly, see the following sections for troubleshooting information:

- [Symptom: The unified IP phone Does Not Complete the Normal Start Up Process, page 9-2](#)

- [Symptom: The Wireless IP Phone Does Not Associate with a Cisco Aironet Access Point, page 9-3](#)
- [Symptom: The unified IP phone Does Not Register with Cisco Unified CallManager, page 9-5](#)

Symptom: The unified IP phone Does Not Complete the Normal Start Up Process

When a unified IP phone connects to the wireless network, the phone should go through its normal startup process and the phone screen should display information. If the phone does not complete the startup process, the cause might be due to low RF signal strength, network outages, a dead battery in the phone, or the phone might not be functional.

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

1. Verify that the wired network is accessible by placing calls to and from other wired Cisco Unified IP Phones.
2. Verify that the wireless network is accessible:
 - Power on another previously functional Cisco Unified Wireless IP Phone 7921G to verify that the access point is active.
 - Power on the wireless IP phone that will not start up and move to a different access point location that is known to be good.
3. Verify that the phone is receiving power:
 - If you see “Low Battery” on the phone screen, the battery might be dead.
 - Insert a new or fully charged battery in the wireless IP phone that will not start up.
 - If you are using the battery, try plugging in the external power supply instead.
4. If the phone does not power up successfully, and never shows the Main screen, try using Recovery Mode:
 - Press both the Push to Talk button and the Speaker button and then press the Power-on button.

- The phone goes into recovery mode and checks the integrity of the firmware files.
- If error messages display indicating “recovery required,” then plug the USB cable into the phone and a PC. See [“Using the USB Connection for Initial Phone Configuration”](#) section on page 4-2.
- Using a browser, access the web page for the phone. See [“Accessing the Phone Web Page”](#) section on page 4-5 for instructions.
- Go to the Phone Recovery section on the web page and upload a new Phone Software TAR file.

If, after attempting these solutions, the phone still does not start up, contact a Cisco technical support representative for additional assistance.

Symptom: The Wireless IP Phone Does Not Associate with a Cisco Aironet Access Point

After the Greeting Message displays, if a phone continues to cycle through messages displaying on the phone screen, the phone is not associating with the access point properly. The phone cannot successfully start up unless it associates and authenticates with an access point.

Verifying Access Point Settings

The Cisco Unified Wireless IP Phone 7921G must first authenticate and associate with an access point before it can obtain an IP address. The phone follows this start up process with the access point:

1. Scans for an access point
2. Associates with an access point
3. Authenticates using a preconfigured authentication method (if configured, can use LEAP, EAP-FAST, Auto (AKM), or others)
4. Obtains an IP address

Check the SSID settings on the access point and on the phone to be sure the SSID matches.

Check the authentication type settings on the access point and on the phone to be sure authentication/encryption settings match.



Note If the message, “No Service - IP Config Failed,” DHCP failed because the encryption between the access point and phone do not match.

If using static WEP, check the WEP key on the phone to be sure it matches the WEP key on the access point. Reenter the WEP key on the phone to be sure it is correct.



Note If open authentication is set, the phone is able to associate to an access point although the WEP keys are incorrect or mismatched.

Error Messages During Authentication

If you see the following error messages, check these problems:

Authentication failed, No AP found

- Check if the correct authentication method and related encryption settings are enabled on the access point.
- Check that the correct SSID is entered on the phone.
- Check that the correct username and password are configured when using LEAP, EAP-FAST or Auto (AKM) authentication.
- If you are using A WPA Preshared key or WPA2 Preshared Key, check that you have the correct passphrase configured.
- You might need to enter the user name on the phone in the domain\username format when authenticating with a Windows domain.

EAP authentication failed

- If you are using EAP, you might need to enter the EAP user name on the phone in the *domain\username* format when authenticating with a Windows domain.
- Check that the correct EAP username and password are entered on phone.

AP Error—Cannot support all requested capabilities

On the access point, check that CKIP/CMIC is not enabled for the voice VLAN SSID. The Cisco Unified Wireless IP Phone 7921G does not support these features.

Symptom: The unified IP phone Does Not Register with Cisco Unified CallManager

If a phone proceeds past the first stage (authenticating with access point), and, continues to cycle through the messages displaying on the phone screen, the phone is not starting up properly. The phone cannot successfully start up until it connects to the LAN and registers with a Cisco Unified CallManager server.

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

- [Registering the Phone with Cisco Unified CallManager, page 9-5](#)
- [Checking Network Connectivity, page 9-6](#)
- [Verifying TFTP Server Settings, page 9-6](#)
- [Verifying IP Addressing, page 9-7](#)
- [Verifying DNS Settings, page 9-8](#)
- [Verifying Cisco Unified CallManager Settings, page 9-8](#)
- [Cisco Unified CallManager and TFTP Services Are Not Running, page 9-9](#)
- [Creating a New Configuration File, page 9-10](#)

Registering the Phone with Cisco Unified CallManager

A Cisco Unified Wireless IP Phone 7921G can register with a Cisco Unified CallManager server only if the phone has been added to the server or if auto-registration is enabled. If you see the error message, “Registration Rejected,” review the information and procedures in the [“Adding Users to Cisco Unified CallManager” section on page 6-22](#) to ensure that the phone has been added to the Cisco Unified CallManager database.

To verify that the phone is in the Cisco Unified CallManager database, choose **Device > Phone > Find** from Cisco Unified CallManager Administration to search for the phone based on its MAC Address. (To determine the MAC address of a phone, see the [“Viewing Device Information”](#) section on page 7-6.)

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 9-10 for assistance.

Checking Network Connectivity

If the network is down between the access point and the TFTP server or Cisco Unified CallManager, the phone cannot start up properly. Ensure that IP connectivity exists between the WLAN and the Cisco Unified CallManager and TFTP servers.

Verifying TFTP Server Settings

The Cisco Unified Wireless IP Phone 7921G uses the TFTP server setting to identify the primary TFTP server to use. If the TFTP server does not respond to the request, then the CallManager1 (CM1) shows as TFTP_AS_CM if the phone has not registered with Cisco Unified CallManager before.



Note If the phone has previously registered with Cisco Unified CallManager, the Cisco Unified CallManager list information is cached in memory. If TFTP fails, you must power cycle the phone to connect to the TFTP server.

The phone tries to create a TCP connection to the TFTP IP address and then to the gateway. If Cisco Unified CallManager service is not running on the TFTP server, or if SRST is not running on the gateway, the wireless IP phone may continually cycle while attempting to contact the identified TFTP server.

The Cisco Unified Wireless IP Phone 7921G does not cache the IP information passed from the DHCP server, so the TFTP request must be sent and responded to every time the phone power cycles.

If you have assigned a static IP address to the phone, you must manually enter this setting. See the [“Configuring IP Network Settings”](#) section on page 4-21.

If you are using DHCP, the phone obtains the address for the TFTP server from the DHCP server. Check the IP address configured in Option 150 or Option 66. Refer to *Configuring Windows 2000 DHCP Server for Cisco Unified Call Manager* available at this URL:

http://www.cisco.com/warp/customer/788/AVVID/win2000_dhcp.html

You can also enable the phone to use a static TFTP server. Such a setting is particularly useful if the phone was recently moved from one location to another.

For information about determining and changing TFTP server settings, see “Configuring IP Network Settings” section on page 4-21 or “Viewing the Current Configuration” section on page 7-15.

Verifying IP Addressing

You should verify the IP addressing for the Cisco Unified Wireless IP Phone 7921G. 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.



Note

When the wireless IP phone loses the RF signal (goes out of the coverage area), the phone will not release the DHCP server unless it reaches the time-out state.

Check for these problems:

- 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. If you are using a DHCP server, and the wireless IP phone gets a response from the DHCP server, the information is automatically configured. Refer to *Troubleshooting Switch Port Problems*, available at this URL:
<http://www.cisco.com/warp/customer/473/53.shtml>
- IP Address, Subnet Mask, Primary Gateway—If you have assigned a static IP address to the phone, you must configure settings for these options. See the “Configuring IP Network Settings” section on page 4-21.

If you are using DHCP, check the IP addresses distributed by your DHCP server. Be aware of DHCP conflicts and duplicate IP addresses. 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>

For information about determining and changing IP addressing, see “[Configuring IP Network Settings](#)” section on page 4-21

Verifying DNS Settings

If you are using DNS to refer to Cisco Unified CallManager, you must ensure that you have specified a DNS server. You should also verify that there is a CNAME entry in the DNS server for the Cisco Unified CallManager system.

You must also ensure that DNS is configured to do reverse look-ups. The default setting on Windows 2000 is to perform forward-only look-ups.

For information about determining and changing DNS settings, see “[Configuring IP Network Settings](#)” section on page 4-21.

Verifying Cisco Unified CallManager Settings

The Cisco Unified Wireless IP Phone 7921G attempts to open a TCP connection to all the Cisco Unified CallManager servers that are part of the assigned Cisco Unified CallManager group. Take one of these actions to verify Cisco Unified CallManager settings:

- On the Cisco Unified Wireless IP Phone 7921G, choose **Menu > Network Config > Current Configuration** and look at the **CallManager 1–4** options. (See “[Viewing the Current Configuration](#)” section on page 7-15.)
- If none of the Cisco Unified CallManager 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 9-5 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 might not be able to start up properly. However, in such situations, 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 check that all services are running, follow these steps:

Procedure

-
- Step 1** From Cisco Unified CallManager Administration, choose **Application > Cisco 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.
-



Note For more information about services, refer to *Cisco Unified CallManager Administration Guide* for more information.

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 might be corrupted.

To create a new configuration file, follow these steps:

Procedure

- Step 1** From Cisco Unified CallManager, select **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 Users to Cisco Unified CallManager”](#) section on page 6-22 for details.
- Step 4** Power cycle the wireless IP 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 directory number (DN) remains in the Cisco Unified CallManager database as an unassigned DN. You can assign these DNs to other devices or 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.

Related Topics

- [Resolving Startup and Connectivity Problems, page 9-1](#)
- [Resolving Voice Quality and Roaming Problems, page 9-11](#)
- [General Troubleshooting Information, page 9-20](#)

Resolving Voice Quality and Roaming Problems

Cisco Unified Wireless IP Phone 7921G users might have problems with voice quality and connectivity when roaming with their phones. See the following sections for troubleshooting information:

- [Symptom: unified IP phone Resets Unexpectedly, page 9-11](#)
- [Symptom: The unified IP phone Has Audio Problems, page 9-14](#)
- [Symptom: The unified IP phone Does Not Roam Properly, page 9-15](#)
- [Monitoring the Voice Quality of Calls, page 9-17](#)

Symptom: unified IP phone Resets Unexpectedly

If users report that their phones are resetting during calls or resetting while idle on their desk, you should investigate the cause. If the network connection and Cisco Unified CallManager connection are stable, a Cisco Unified Wireless IP Phone 7921G should not reset on its own.

Typically, a phone resets if it has problems connecting to the access point and LAN or to Cisco Unified CallManager. These sections can help you identify the cause of a phone resetting in your network:

- [Verifying Access Point Settings, page 9-11](#)
- [Identifying Intermittent Network Outages, page 9-12](#)
- [Verifying DHCP Settings, page 9-12](#)
- [Verifying Voice VLAN Configuration, page 9-12](#)
- [Verifying that the Phones Have Not Been Intentionally Reset, page 9-13](#)
- [Eliminating DNS or Other Connectivity Errors, page 9-13](#)

Verifying Access Point Settings

Verify that the wireless configuration is correct. For example, check if the particular access point or switch to which the phone is connected is down. See the [“Voice Over IP Wireless Network Configuration”](#) section on page 2-27 for information about access point settings.

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. The phone can retransmit and attempt to recover, or if the phone reaches the maximum retransmit rate, it drops the packets or loses association with the access point.

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

Verifying DHCP Settings

To determine if the phone has been properly configured to use DHCP, follow these steps:

-
- Step 1** Verify that you have properly configured the phone to use DHCP. See the [“Configuring DHCP Settings” section on page 5-8](#) for details.
 - Step 2** Verify that the DHCP server has been set up properly.
 - Step 3** Verify the DHCP lease duration. Your local policy determines this setting.

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.

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 access point and switch as phone), it is likely that you do not have a voice VLAN or the appropriate QoS settings configured.

By isolating the wireless phones on a separate auxiliary VLAN, you can use QoS to prioritize the voice traffic over data traffic and improve the voice quality. See the [“Voice Quality in a Wireless Network” section on page 2-16](#) for details.

Verifying that the Phones Have Not Been Intentionally Reset

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

Eliminating DNS or Other Connectivity Errors

If the phone does not register with Cisco Unified CallManager, check to see if you are using host names or IP addresses for Cisco Unified CallManager servers.

To eliminate DNS or other connectivity errors, follow these steps:

Procedure

-
- Step 1** Reset the phone to factory defaults. See the [“Erasing the Local Configuration” section on page 9-25](#) for details.
- Step 2** Modify DHCP and IP settings:
- a. Disable DHCP. See the [“Configuring DHCP Settings” section on page 5-8](#) for details.
 - b. Assign static IP values to the phone. See the [“Configuring DHCP Settings” section on page 5-8](#) for details. Use the same default router setting used for other functioning Cisco Unified IP Phones.
 - c. Assign a TFTP server. See the [“Configuring an Alternate TFTP Server” section on page 5-10](#) for details. Use the same TFTP server used for other functioning Cisco Unified IP Phones.
- Step 3** From Cisco Unified CallManager, choose **System > Server** and verify that the server is referred to by its IP address and not by its host name.



Note Cisco recommends that you configure IP addresses only and not host names to eliminate the DNS resolution in the phone registration process.

- Step 4** From Cisco Unified CallManager, select **Device > Phone** and verify that you have assigned the correct MAC address to this Cisco Unified IP Phone.
- To determine the MAC address of a phone, see the [“Viewing Device Information” section on page 7-6](#).
- Step 5** Power cycle the phone.
-

Symptom: The unified IP phone Has Audio Problems

When users report that active phone calls have poor voice quality that includes choppy audio, static or gaps in audio, or no audio, you can use the following suggestions to identify the cause of the problem.

These sections can assist you with the following symptoms:

- [No Audio During a Connected Call, page 9-14](#)
- [One-Way Audio During a Connected Call, page 9-14](#)

No Audio During a Connected Call

If you are using a release earlier than 2.0, then you must disable TKIP and MIC features on the access point. These features are only supported with release 2.0 and later on the Cisco Unified Wireless IP Phone 7921G.

One-Way Audio During a Connected Call

Use the following list to identify possible causes for the problem:

- Check the access point to see that the transmit power setting matches the transmit power setting on the phone. One-way audio is common when the access point power setting is greater (100mW) than that of the phone (20mW).

Cisco Unified Wireless IP Phone 7921G Firmware supports dynamic transmit power control (DTPC). The phone uses the transmit power that the access point advertises upon association.



Note With DTCP, if Client Transmit Power is set in the access point, the phone automatically uses the same client power setting. If the access point is set for the maximum setting (Max), the access point uses the Transmit Power setting on the phone.

- Check that the access point is enabled for ARP caching. When the Cisco Unified Wireless IP Phone 7921G is in power save mode or scanning, the access point can respond to the wireless IP phone only when ARP caching is enabled.

See the [“Voice Over IP Wireless Network Configuration”](#) section on [page 2-27](#) for more information.

- Check your gateway and IP routing for voice problems.
- Check if a firewall or NAT is in the path of the RTP packets. If so, you can use Cisco IOS and PIXNAT to modify the connections so that two-way audio is possible.
- Check that the Data Rate setting for the phone and the access point are the same. These settings should match or the phone should be set for Auto.
- Check the phone hardware to be sure the speaker is functioning properly.
- Check the volume settings in the Phone Settings menu.

Symptom: The unified IP phone Does Not Roam Properly

If users report that when engaged in an active phone call and walking from one location to another (roaming), the voice quality deteriorates or the connection is lost, you can use the following suggestions to identify the cause of the problem.

These sections can assist you with the following symptoms:

- [Voice Quality Deteriorates While Roaming, page 9-16](#)
- [Delays in Voice Conversation While Roaming, page 9-16](#)
- [Phone Loses Connection with Cisco Unified CallManager While Roaming, page 9-16](#)

Voice Quality Deteriorates While Roaming

Check the RSSI on the destination access point to see if the signal strength is adequate. The next access point should have an RSSI value of 35 or greater.

Check the site survey to determine if the channel overlap is adequate for the phone and the access point to hand off the call to the next access point before the signal is lost from the previous access point.

Check to see if noise or interference in the coverage area is too great.

Check that signal to noise ratio (SNR) levels are 25 db or higher for acceptable voice quality.

Delays in Voice Conversation While Roaming

Use the Site Survey Utility on the Cisco Unified Wireless IP Phone 7921G to see if there is another acceptable access point as a roaming option. The next access point should have an RSSI value of 35 or greater to roam successfully.

Check the Cisco Catalyst 45xx switch to see if it has the correct version of Supervisor (SUP) blades. The blades must be versions SUP2+ or higher to prevent roaming delays.

Phone Loses Connection with Cisco Unified CallManager While Roaming

Check for the following configuration or connectivity issues between the phone and the access point:

- The RF signal strength might be weak. Use the Site Survey Tool and check the RSSI value for the next access point.
- The next access point might not have connectivity to Cisco Unified CallManager.
- There might be an authentication type mismatch between the phone and the next access point.
- The access point might be in a different subnet from the previous access point. The Cisco Unified Wireless IP Phone 7921G is capable of Layer 2 roaming only. Layer 3 roaming requires WLSM that uses GRE. For more information, see [“Roaming in a Wireless Network” section on page 2-14](#).

- If using EAP-FAST, LEAP, or Auto (AKM) authentication, the access point might be using filters to block TCP ports. The ACS server uses port 1645 for authentication and 1646 for accounting and the RADIUS server uses port 1812 for authentication and 1813 for accounting.

Related Topics

- [Resolving Startup and Connectivity Problems, page 9-1](#)
- [Resolving Voice Quality and Roaming Problems, page 9-11](#)
- [General Troubleshooting Information, page 9-20](#)
- [Monitoring the Voice Quality of Calls, page 9-17](#)

Monitoring the Voice Quality of Calls

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

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

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

**Note**

Concealment ratio and concealment seconds are primary measurements based on frame loss while MOS LQK scores project a “human-weighted” version of the same information on a scale from 5 (excellent) to 1 (bad) for measuring listening quality.

Listening quality scores (MOS LQK) relate to the clarity or sound of the received voice signal. Conversational quality scores (MOS CQ such as G.107) include impairment factors, such as delay, that degrade the natural flow of conversation.

For information about configuring voice quality metrics for phones, refer to the “Phone Features” section in the “Cisco Unified IP Phone” chapter in *Cisco Unified CallManager System Guide*.

You can access voice quality metrics remotely by using Streaming Statistics (see [Chapter 8, “Monitoring the Cisco Unified Wireless IP Phone Remotely.”](#))

Using Voice Quality Metrics

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

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

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

- G.711 codec gives 4.5 score
- G.719A/ AB gives 3.7 score

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

Troubleshooting Tips

When you observe significant and persistent changes to metrics, use [Table 9-1](#) for general troubleshooting information.

Table 9-1 *Changes to Voice Quality Metrics*

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

**Note**

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

General Troubleshooting Information

The following topics provide general information and tips for troubleshooting the Cisco Unified Wireless IP Phone 7921G.

- [Common Phone Status Messages, page 9-20](#)
- [Troubleshooting Tips for the Cisco Unified Wireless IP Phone 7921G, page 9-22](#)
- [Logging Information for Troubleshooting, page 9-24](#)

Common Phone Status Messages

[Table 9-2](#) provides a list of common status messages that display on the phone screen. The table provides possible causes and recommended actions to assist with troubleshooting the problem.

Table 9-2 Common Phone Status Messages

Message	Description	Possible Explanation and Action
Network Busy	The phone is unable to complete a call.	<p>The WLAN is not able to allocate bandwidth for the phone to complete the call.</p> <p>Wait a few minutes and try the call again. If the problem persists, the WLAN might be congested. Consider increasing the WLAN bandwidth.</p>
Leaving Service Area	The phone is unable to place or receive calls. The no signal icon displays on the phone screen.	<ul style="list-style-type: none"> • The phone cannot detect any access point (AP) beacons. <p>The phone is out of range of all APs. Move to a location that is within the coverage area.</p> <ul style="list-style-type: none"> • The AP has failed. Run diagnostic tests on the AP and replace if defective.

Table 9-2 Common Phone Status Messages (continued)

Message	Description	Possible Explanation and Action
Locating Network Services	The phone is searching for an AP.	<p>The phone is searching all beacons and scanning for a channel and SSID to use.</p> <p>Wait for the phone to complete the searching and scanning process. Depending on the signal strength of the available WLAN, this process can take a few minutes.</p>
Authentication Failed	The phone is unable to access the WLAN, and the main phone screen is not active.	<p>The authentication server does not accept the security credentials.</p> <p>Verify that the security mode and credentials are correct by viewing the Network profile. For information about accessing and changing Network profiles, see the “Configuring Network Profile Settings” section on page 5-3.</p>
Configuring IP	The main phone screen is not active.	<p>The phone is attempting to obtain network parameters such as its IP address, or the IP address of the gateway or router from the DHCP server.</p> <p>Wait a few minutes for the phone to obtain the network parameters.</p> <p>If the phone unable to retrieve the IP address, then check that the DHCP server is up and running.</p>
Configuring CM List	The main phone screen is not active.	<p>The phone is downloading its configuration files from the TFTP server.</p> <p>Wait a few minutes for the phone to download all of its configuration files.</p>

Troubleshooting Tips for the Cisco Unified Wireless IP Phone 7921G

Table 9-3 provides general troubleshooting information for the wireless IP phone.

Table 9-3 *unified IP phone Troubleshooting Tips*

Summary	Explanation
Phone is resetting	<p>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 access point problems, switch outages, and switch reboots.</p> <p>See the “Symptom: unified IP phone Resets Unexpectedly” section on page 9-11.</p>
Time on phone is incorrect	<p>Sometimes the time or date on the phone is incorrect. The Cisco Unified Wireless IP Phone 7921G gets its time and date when it registers with Cisco Unified CallManager. Power cycle the phone to reset the time or date.</p> <p>The time shows in either 12 hour or 24 hour format.</p>
Ring volume is too low	<p>To see if the ring volume is set correctly on the phone, choose Settings > Phone Settings > Sound Settings > Volumes. Scroll up for the highest volume</p> <p>You can also press the volume button on the side of the phone and the volume setting appears on the phone screen.</p>
Phone does not ring	<p>To see if the phone is set to ring, choose Settings > Phone Settings > Sound Settings > Alert Pattern, and check that it a ring setting is selected.</p> <p>To see if a ring tone has been set for the phone, choose Settings > Phone Settings > Ring Tone. If none is set, add a ring tone for the phone.</p> <p>To see if the speaker is functioning properly, adjust the ring volume settings to the highest level. Enable keypad tones or call the phone to check the speaker.</p>

Table 9-3 *unified IP phone Troubleshooting Tips (continued)*

Summary	Explanation
One-way audio on phone	<p>Check that the speaker is functioning properly. Adjust the speaker volume setting and call the phone to check the speaker.</p> <p>Check that ARP caching has been set on the AP. See “Voice Over IP Wireless Network Configuration” section on page 2-27.</p>
Delays when roaming from one location to another	<p>If Cisco Catalyst 45xx series switches are being used as the main Layer 3 switches in the network, ensure that the supervisor blades are a minimum SUP2+ or later version. The Cisco Unified Wireless IP Phone 7921G (or any wireless client) experiences roaming delays when an earlier version (SUP 1 or SUP2) blade is used.</p>
Phone firmware downgrades	<p>After applying a Cisco Unified CallManager upgrade or patch, that is older than the current Cisco Unified Wireless IP Phone 7921G firmware, the phones could automatically downgrade to the load contained in the patch. Check the Cisco Unified CallManager 7921G device default image in the TFTP folder to fix this problem.</p>
Battery life is shorter than specified	<p>An unstable RF environment can cause the phone to remain in active mode because it is constantly seeking an AP. This reduces the battery life considerably. When leaving an area of coverage, shut down the phone.</p> <p>Higher phone transmit power can affect battery life.</p> <p>To maximize idle time on the phone and conserve battery life, you need to optimize the registration time so the phone can go into power save mode more often.</p>

Related Topics

- [Logging Information for Troubleshooting, page 9-24](#)
- [General Troubleshooting Information, page 9-20](#)

Logging Information for Troubleshooting

The following options can help you gather troubleshooting information:

- [Using a System Log Server, page 9-24](#)
- [Using the Trace Logs on the unified IP phone, page 9-24](#)

Using a System Log Server

To gather information about problems with the wired network that can cause roaming delays or no connectivity, set up a system log server. Enable “syslog” on the network switches and access points that is logged to the system log server. Also enable Network Time Protocol (NTP) so that all access points and switches use the same times.

For information about setting up a system log server, see [“Configuring Trace Settings” section on page 4-27](#).

Using the Trace Logs on the unified IP phone

When you are experiencing problems with registering with Cisco Unified CallManager, or call connections, you can use this function to trace the path of a packet from the phone to Cisco Unified CallManager. The result shows the number of hops and the IP address of each hop to reach the Cisco Unified CallManager server. You can use this information to check connectivity between the phone, Cisco Unified CallManager servers and gateways during a call.

For information about setting up trace logs and a system log server, see the [“Viewing Trace Logs” section on page 4-30](#).

Related Topics

- [Resolving Startup and Connectivity Problems, page 9-1](#)
- [Resolving Voice Quality and Roaming Problems, page 9-11](#)
- [Erasing the Local Configuration, page 9-25](#)

Erasing the Local Configuration

You can clear all locally stored configuration options in a phone by using the Phone Settings menu. When you use the restore to factory default option, all user-defined entries in Network Profiles, Phone Settings, and Call History are erased.

To erase the local configuration, follow these steps:

Procedure

- Step 1** Choose **Settings > Phone Settings**.
- Step 2** Press ****2** on the keypad.
The phone briefly displays “Start factory reset now?”
- Step 3** Press the **Yes** softkey. All settings are deleted.
The phone cycles through normal startup procedures.
Or press **No** to cancel the reset.
- Step 4** Press **Settings > Network Profiles** to reconfigure the network settings for your WLAN.
-



Caution

Erasing the local configuration removes network profiles that are set up for the Cisco Unified Wireless IP Phone to access the WLAN. You must reconfigure the network settings after performing the reset to enable the phone to access the WLAN.

Related Topics

- [Resolving Startup and Connectivity Problems, page 9-1](#)
- [Resolving Voice Quality and Roaming Problems, page 9-11](#)
- [General Troubleshooting Information, page 9-20](#)

Erasing the Local Configuration



CHAPTER **A**

Providing Information to Users By Using a Website

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

To successfully use some features on the Cisco Unified Wireless IP Phone 7921G (such as speed dial numbers and voice messaging system options), users must receive information from you or your network team or be able to contact you for assistance.

Cisco recommends that you create a web page on your internal support site that provides end users with important information about their new Cisco Unified Wireless IP Phone 7921G.

Consider adding the following types of information to this site:

- [How the Cisco Unified Wireless IP Phone Operates, page A-2](#)
- [How Users Access the Help System on the Phone, page A-4](#)
- [How Users Get Copies of Cisco Unified IP Phone Manuals, page A-5](#)
- [How Users Configure Phone Features and Services, page A-6](#)
- [How Users Access Voice Messages, page A-7](#)

How the Cisco Unified Wireless IP Phone Operates

Users need to know that their Cisco Unified Wireless IP Phone 7921G operates more like a cell phone than like their desktop phone. Small wireless phones with an antenna allow users to move around a facility while staying connected to a call. These phones, like cell phones, can approach the edge of the RF signal range and experience static or poor voice quality. At times, the user might encounter areas where there is no signal and lose the call entirely. The following is a list of calling locations and situations in which wireless phones might experience audio problems:

- Stairwells, elevators, rooms with metal equipment such as file cabinets, or heavy machinery
- Break rooms with microwave ovens, or labs with equipment that emits RF signals within the same ranges.
- Conference rooms or other congested areas where many people are using wireless devices
- Parking garages and outdoor areas where access points are not located or out of range.

**Caution**

This product is not a medical device and may use an unlicensed frequency band that is susceptible to interference from other devices or equipment.

The Cisco Unified Wireless IP Phone 7921G has many of the same phone features as the IP phone desktop models, such as Mute, access to voice messaging, and directories. The phone has a limited number of buttons, because of its size. As a consequence, the following are some differences in its operation:

- No line buttons—You must enter the phone number from the key pad and press Send. You can press the Phone icon from the main screen to use other lines on your phone.
- Only two softkeys—You must press the Options softkey to see the list of softkey features.
- You do not hear a dial tone.

Related Topics

- [How to Care for and Clean the Phone, page A-3](#)
- [How Users Get Copies of Cisco Unified IP Phone Manuals, page A-5](#)
- [How Users Configure Phone Features and Services, page A-6](#)
- [How Users Access Voice Messages, page A-7](#)

How to Care for and Clean the Phone

Users need to know how to protect and clean their phone. These guidelines provide information about using accessories and cleaning the Cisco Unified Wireless IP Phone 7921G:

- Use only chargers, batteries, and accessories that are approved by the Cisco Unified Wireless IP Phone 7921G manufacturer. Use of unapproved chargers, batteries, and accessories might be dangerous.
- Do not adhere a clip to the back of the phone or insert a clip between the phone and battery cover because it can damage the battery.
- Use a protective cover case to shield the phone from moisture, dust, hair, grease, and other contaminants that might get on your hands. For example, in Healthcare environments, where phones must be cleaned with sterilizing wipes, you must use a protective cover case to prevent moisture damage to the phone.
- Use a protective cover case in environments where the phone might be bumped or dropped, such as manufacturing or warehouse environments.
- When disconnecting the power cord of any accessory, grasp and pull the plug. Do not pull the cord.
- Keep accessories out of reach of young children.
- Clean the phone only with a soft dry cloth. Do not use moist wipes or cleaning powders that might damage the phone.



Note

Using unapproved accessories, not protecting the phone from moisture, contaminants, and hard impacts can invalidate the one-year hardware warranty.

For a list of available accessories and their descriptions, refer to the *Cisco Unified Wireless IP Phone 7921G Accessory Guide* at this URL:

http://www.cisco.com/en/US/products/hw/phones/ps379/products_user_guide09186a008076b878.html

Related Topics

- [How the Cisco Unified Wireless IP Phone Operates, page A-2](#)
- [How Users Access the Help System on the Phone, page A-4](#)
- [How Users Get Copies of Cisco Unified IP Phone Manuals, page A-5](#)
- [How Users Configure Phone Features and Services, page A-6](#)
- [How Users Access Voice Messages, page A-7](#)

How Users Access the Help System on the Phone

This Cisco Unified Wireless IP Phone 7921G provides access to a comprehensive online help system. To view the main help menu on a phone, from the main screen, press the Select button in the center of the navigation button. Wait for several seconds for this menu to appear.

- About Your Cisco Unified IP Phone—Details about your phone
- How do I...?—Procedures for common phone tasks
- Calling Features—Descriptions and procedures for calling features
- Help—Tips on using and accessing Help



Note

Online help for the Cisco Unified Wireless IP Phone 7921G is available only for Cisco Unified CallManager 4.2(3) and Cisco Unified CallManager 5.1. Users who try to access online help on earlier versions of Cisco Unified CallManager will receive a message that this feature is not available.

- [How the Cisco Unified Wireless IP Phone Operates, page A-2](#)
- [How to Care for and Clean the Phone, page A-3](#)
- [How Users Get Copies of Cisco Unified IP Phone Manuals, page A-5](#)

- [How Users Configure Phone Features and Services, page A-6](#)
- [How Users Access Voice Messages, page A-7](#)

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. This documentation includes detailed user instructions for key phone features. See the “[Related Documentation](#)” section on page xvii for more information.

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

For a list of available documentation for Cisco Unified IP Phones, go to this URL:

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

For a list of available documentation for Cisco Unified CallManager, go to this URL:

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

For more information about viewing or ordering documentation, see the “[Obtaining Documentation](#)” section on page xviii.

Related Topics

- [How the Cisco Unified Wireless IP Phone Operates, page A-2](#)
- [How to Care for and Clean the Phone, page A-3](#)
- [How Users Access the Help System on the Phone, page A-4](#)
- [How Users Configure Phone Features and Services, page A-6](#)
- [How Users Access Voice Messages, page A-7](#)

How Users Configure Phone Features and Services

End users can perform a variety of activities using the Cisco Unified CallManager User Options web page. Cisco Unified Wireless IP Phone users can set up speed dial and call forwarding numbers. 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 page.

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

- 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 for accessing 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 6-22).
- A description of a web-based, graphical user interface application and how to access it with a web browser.
- An overview of tasks that users can accomplish by 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/application/pdf/en/us/guest/products/ps1855/c1626/ccmigration_09186a00805f2352.pdf

Related Topics

- [How the Cisco Unified Wireless IP Phone Operates](#), page A-2
- [How to Care for and Clean the Phone](#), page A-3
- [How Users Access the Help System on the Phone](#), page A-4
- [How Users Get Copies of Cisco Unified IP Phone Manuals](#), page A-5
- [How Users Access Voice Messages](#), page A-7

How Users Access Voice Messages

Cisco Unified CallManager provides the flexibility to integrate with many different voice messaging systems, including the Cisco Unity voice messaging system. Because you can integrate with many different systems, you must provide users with detailed information about how to use your specific system.

You should provide this information to each user:

- How to access the voice messaging system account.
- The 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 messages are waiting.

Make sure that you have used Cisco Unified CallManager to set up a message waiting indicator (MWI) method.

For information about setting up the MWI method and the interface to the voice messaging system in Cisco Unified CallManager, refer to the documentation for your system at this URL:

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

If you are using a Cisco Unity voice messaging system, refer to the Cisco Unity documentation for your system for configuring voice messaging and the initial passwords at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html

Refer to the *Cisco Unified Wireless IP Phone 7921G Guide* for information about accessing the voice messaging system from the phone at this URL:

http://www.cisco.com/en/US/products/hw/phones/ps379/products_user_guide_book09186a008076b8af.html

Related Topics

- [How the Cisco Unified Wireless IP Phone Operates, page A-2](#)
- [How to Care for and Clean the Phone, page A-3](#)
- [How Users Access the Help System on the Phone, page A-4](#)

■ How Users Access Voice Messages

- [How Users Get Copies of Cisco Unified IP Phone Manuals, page A-5](#)
- [How Users Configure Phone Features and Services, page A-6](#)



APPENDIX **B**

Supporting International Users

Translated and localized versions of the Cisco Unified Wireless IP Phone 7921G user interface include:

- English
- French
- German
- Japanese

Prior to deploying the wireless IP phones, download the locale installer for the firmware releases and configure the languages in Cisco Unified CallManager. For more information about installing the locale installer, “[Installing the Cisco Unified CallManager Locale Installer](#)” section on page B-1. You can obtain translated documentation for the Cisco Unified IP Phones at this URL:

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

Installing the Cisco Unified CallManager Locale Installer

If you are using Cisco Unified IP Phones in a locale other than English, you must install the locale-specific version of the Cisco Unified CallManager Locale Installer to ensure that you have the latest translated text, user and network locales, and country-specific phone tones available for the Cisco Unified IP Phones.

To provide localized versions of the Cisco Unified Wireless IP Phone 7921G, follow these steps:

Procedure

-
- Step 1** Download the locale-specific version of the Cisco Unified CallManager Locale Installer at this URL:
<http://www.cisco.com/kobayashi/sw-center/telephony/callmgr/locale-installer.shtml>.
- Step 2** Install the locale-specific version of the Cisco Unified CallManager Locale Installer on every Cisco Unified CallManager server in the cluster.
- For Cisco Unified CallManager Release 4.1 and later, refer to *Using the Cisco Unified IP Telephony Locale Installer for Cisco Unified CallManager* for your Cisco Unified CallManager release.
 - For Cisco Unified CallManager Releases 5.0 and later, refer to the “Locale Installation” section in the *Cisco IP Telephony Platform Administration Guide*.
- Step 3** After modifying the user locale on the Cisco Unified Wireless IP Phone 7921G, you must power cycle the phone.
-

**Note**

When deploying Cisco Unified Wireless IP Phone 7921G for the first time, you must install the 7921G Device Pack to add the new phone type to Cisco Unified CallManager. Then you must reinstall the locale specific Cisco Unified CallManager Locale Installer to update the user locale for the Cisco Unified Wireless IP Phone 7921G.

**Note**

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



APPENDIX **C**

Physical and Operating Environment Specifications

The following section describes the technical specifications for the Cisco Unified Wireless IP Phone 7921G. [Table C-1](#) shows the physical and operating environment specifications.

Table C-1 *Physical and Operating Environmental Specifications*

Specification	Value or Range
Operating temperature	0° to 40°C (32° to 104°F)
Operating Relative Humidity	10% to 95% (non-condensing)
Storage Temperature	-30° to 60°C (22° to 140°F)
Drop Specification	1.5 m (5 ft) to concrete without carrying case
Thermal Shock	-22°F (-30° C) for 24 hours to up to 158°F (+70°C) for 24 hours
Phone Height	128.9 mm (5.0 in.)
Phone Width	53.4 mm (2.1 in.)
Phone Depth	25.3 mm (1 in.)
Phone Weight (with Standard Battery)	145g (5oz)
Power	AC adapters by geographic region

Table C-1 *Physical and Operating Environmental Specifications*

Specification	Value or Range
Desktop Charger Height	75 mm (3.0 in)
Desktop Charger Width	93 mm (3.7 in)
Desktop Charger Depth	129 mm (5.1 in)



APPENDIX **D**

Checklist for Deploying the Cisco Unified Wireless IP Phone 7921G

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

- [Configuring the Wireless Network, page D-1](#)
- [Configuring QoS Policies, page D-4](#)
- [Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager, page D-6](#)
- [Installing the Cisco Unified Wireless IP Phone 7921G, page D-9](#)

Configuring the Wireless Network

[Table D-1](#) explains and provides references for many of the configuration activities for the Cisco Aironet Access Point, controller, and Ethernet switch.



Note

When deploying the Cisco Unified Wireless IP Phone 7921G with World regulatory domain (CP-7921G-W-K9), you must enable the access points for world mode (802.11d). The world model phone gets the channels and power information from the access point.

Table D-1 **Wireless Network Configuration Tasks**

Activity	Explanation	Reference
Check that the Cisco IOS version is the recommended version	<ul style="list-style-type: none"> • Under System Software, verify that Cisco IOS version 12.3(8)JA or later is running on the AP. • For the controller, use Version 4.0 and Cisco IOS version 12.3(8)JX or later. 	Interacting with Cisco Unified Wireless Access Points, page 2-12
Configure a VLAN for voice	To isolate voice traffic and enable QoS, you need a separate voice VLAN on the access point and network switch.	Voice Quality in a Wireless Network, page 2-16 <i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA</i>
Configure Service Set Identifier (SSID) for each VLAN	Identifier for a set of wireless devices to communicate with each other. Several access points can have the same SSID to support a group of wireless phones.	Interacting with Cisco Unified Wireless Access Points, page 2-12 <i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA</i>
Configure QoS settings for VLANs	<p>Create a QoS policy for the voice VLAN and assign a higher CoS to voice traffic.</p> <p>Enable the QoS element for wireless IP phones to provide channel utilization (QBSS) information to phones.</p>	Voice Quality in a Wireless Network, page 2-16 Configuring QoS Policies, page D-4 <i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA</i>
Enable ARP caching	Enable this option to ensure two-way audio. The access point has ARP caching disabled by default.	Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA

Table D-1 Wireless Network Configuration Tasks (continued)

Activity	Explanation	Reference
Configure radio (802.11) settings	<p>Data Rate—Set for 11 Mbps or to the rate for the frequency band that you are using.</p> <p>Client Transmit Power—After a site survey, determine the appropriate power requirements and set a specific Client Transmit Power setting. The Cisco Unified Wireless IP Phone 7921G uses the same setting as the access point.</p> <p>Note If set for Max, the access point does not advertise Client Transmit Power setting.</p>	<p>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA</p> <p>Deployment Guidelines for the Cisco Unified Wireless IP Phone 7921G</p>
Configure Security for the voice VLANs	<p>Use one of these authentication and encryption options for the SSID that corresponds to the voice VLAN:</p> <ul style="list-style-type: none"> • Open • Shared Key • EAP • Auto (AKM) 	<p>Choosing Authentication and Encryption Methods, page 2-21</p> <p>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA</p>

Configuration Tip for Cisco Airespace Access Points

If you are using EAP-FAST with Cisco Airespace technology, you must increase the EAP request (802.1x) timeout to at least 20 seconds to ensure that the phone gets the PAC credentials successfully.

To change the request timeout on the controller, follow these steps:

Procedure

- Step 1** Use SSH or Telnet to access the Airespace controller or controllers.
- Step 2** Enter `config advanced eap request-timeout 20`
- Step 3** Enter `save config`
- Step 4** Enter `y` to confirm.
-

Configuring QoS Policies

To ensure that voice traffic receives the highest priority in the WLAN and to place signaling traffic in a higher priority than data traffic, you need to make these changes to QoS policies and device settings.

Access Point Configuration Settings

For detailed information about configuring the Cisco Aironet Access Points, refer to this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1200/accspts/b1238ja/1238jasc/index.htm>

On the IOS access points, add the following Classifications to your IOS Access Point QoS policy:

- DSCP Expedited Forwarding—COS Voice <10ms Latency (6)
Apply this policy to your voice VLAN for both incoming and outgoing traffic.
- DSCP Best Effort—COS Best Effort (0)
Apply this policy to your data or native VLAN for both incoming and outgoing traffic.

Under the Advanced tab, set the following:

- QoS Element for Wireless Phones—**Enable**.
- Dot11e—**Enable**.
- IGMP Snooping—**Enable**.

- AVVID Priority Mapping—**Yes**.
- WiFi Multimedia (WMM) on radio interfaces—**Enabled**

Controller Settings

For detailed information about configuring QoS policies for the controller, refer to these URLs:

- <http://www.cisco.com/univercd/cc/td/doc/product/wireless/control/index.htm>
- <http://www.cisco.com/univercd/cc/td/doc/product/wireless/control/c44/ccfig40/index.htm>

When using a controller, add the following QoS policies:

- Platinum (voice)—Apply this policy to your voice WLAN SSID/VLAN for both incoming and outgoing traffic.
- Silver (best effort)—Apply this policy to your data WLAN SSID/VLAN for both incoming and outgoing traffic.
- WLAN configuration screen for the voice WLAN SSID/VLAN—For the 7921G Phone Support field, check the AP CAC Limit checkbox to enable QoS Element for Wireless Phones (QBSS).
- General Controller configuration screen—Set Aggressive Load Balancing to **Disabled**.

Switch Configuration

To implement QoS in the connected Ethernet switch individual configurations will vary; however, you can use this example of QoS commands as a guide.

```
mls qos
mls qos map cos-dscp 0 8 16 24 34 46 48 56
mls qos map ip-prec-dscp 0 8 16 24 34 46 48 56

interface FastEthernet0/00
switchport access vlan 11
switchport mode access
switchport voice vlan 111
no ip address
mls qos trust dscp
wrr-queue cos-map 1 1
```

```
wrr-queue cos-map 2
wrr-queue cos-map 3 2 3 4 6 7
wrr-queue cos-map 4 5
priority queue out
spanning-tree portfast
```

**Note**

When you are using U-APSD for power save, you must implement proper QoS policies on the access points and Ethernet switch.

Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager

[Table D-2](#) provides an overview and checklist of configuration tasks for the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager Administration. The list presents a suggested order to guide you through the phone configuration process. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, refer to the sources in the list.

Table D-2 Checklist for Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager

Task	For More Information
<p>1. Gather the following information about the phone:</p> <ul style="list-style-type: none"> • MAC address • 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 softkey template, phone features, IP Phone services, or phone applications 	<p>Refer to the <i>Cisco Unified CallManager System Guide</i>, Cisco Unified IP Phone chapter.</p> <p>See Telephony Features Available for the Phone, page 6-2.</p>
<p>2. Customize phone button templates (if required).</p>	<p>Refer to <i>Cisco Unified CallManager Administration Guide</i>, “Phone Button Template Configuration” chapter.</p> <p>See Modifying Phone Button Templates, page 6-18.</p>

Table D-2 **Checklist for Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager (continued)**

Task	For More Information
<p>3. Add and configure the phone by completing these required fields in the Phone Configuration window:</p> <ul style="list-style-type: none"> • Phone type • Description (user name or ID) • MAC address • Device pool • Partition • Calling Search Space • Security mode or profile (if applicable) • Product Specific Configuration • Softkey template (if customized) 	<p>Refer to the <i>Cisco Unified CallManager Administration Guide</i>, Cisco Unified IP Phone Configuration chapter.</p> <p>For information about Product Specific Configuration fields, refer to “I” Button Help in the Phone Configuration window.</p>
<p>4. Add and configure directory numbers (lines) on the phone by completing these required fields in the Directory Number Configuration window.</p> <ul style="list-style-type: none"> • Directory number(s) • Partition • Multiple Calls and Call Waiting • Call Forwarding and Pickup (if used) • Voice Messaging (if used) 	<p>Refer to the <i>Cisco Unified CallManager Administration Guide</i>, Cisco Unified IP Phone Configuration chapter: “Adding a Directory Number” section “Creating a Cisco Unity Voice Mailbox” section.</p> <p>See Telephony Features Available for the Phone, page 6-2.</p>
<p>5. Customize softkey templates (optional).</p>	<p>Refer to the <i>Cisco Unified CallManager Administration Guide</i>, “Softkey Template Configuration” chapter.</p> <p>See Configuring Softkey Templates, page 6-16.</p>

Table D-2 Checklist for Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified CallManager (continued)

Task	For More Information
6. Configure speed-dial numbers (optional).	Refer to the <i>Cisco Unified CallManager Administration Guide</i> , Cisco Unified IP Phone Configuration chapter, “Configuring Speed-Dial Buttons” section.
7. Configure Cisco Unified IP Phone services and assign services (optional).	Refer to the <i>Cisco Unified CallManager Administration Guide</i> , Cisco Unified IP Phone Services Configuration chapter. See Setting Up Services, page 6-19 .
8. Add user information by configuring required fields: (optional). <ul style="list-style-type: none"> • Name (last) • User ID • Password (for User Options web pages) • PIN (for use with Extension Mobility and Personal Directory) 	Refer to the <i>Cisco Unified CallManager Administration Guide</i> , Adding a New User chapter. See Adding Users to Cisco Unified CallManager, page 6-22 .
9. Associate a user with a phone (optional).	Refer to the <i>Cisco Unified CallManager Administration Guide</i> , Adding a New User chapter, “Associating Devices to a User” section.

Installing the Cisco Unified Wireless IP Phone 7921G

[Table D-3](#) provides an overview and checklist of installation tasks for the Cisco Unified Wireless IP Phone 7921G. The list presents a suggested order to guide you through the phone installation. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, refer to the sources in the list.

Table D-3 **Checklist for Installing the Cisco Unified Wireless IP Phone 7921G**

Task	For More Information
1. Assemble the phone components and charge the battery.	See Providing Power to the Phone , page 3-10.
2. Configure the network profile by using the USB cable and the Cisco Unified Wireless IP Phone 7921G web pages.	See Using the Cisco Unified Wireless IP Phone 7921G Web Pages , page 4-1.
3. Configure the phone settings by using the Settings menu on the phone.	See Configuring Settings on the Cisco Unified Wireless IP Phone 7921G , page 5-1.
4. Power on the phone and monitor the phone startup process.	See Understanding the Phone Startup Process , page 3-26. See Resolving Startup and Connectivity Problems , page 9-1
5. Make calls with the wireless IP phone.	Refer to the <i>Cisco Unified Wireless IP Phone 7921Guide</i> . See Resolving Voice Quality and Roaming Problems , page 9-11
6. Provide information to end users about how to use their phones and how to configure their phone options.	See Appendix A, “Providing Information to Users By Using a Website.”



INDEX

Numerics

802.11a standard [2-3](#)

802.11b standard [2-3](#)

802.11g standard [2-3](#)

A

active mode [3-25](#)

adding

 users to Cisco Unified CallManager [6-22](#)

advanced encryption standard, See AES

AES

 description [2-8](#)

 encryption description [2-21](#)

AP

 associating [2-13](#)

 Cisco Aironet Access Point [2-12](#)

 Cisco IOS version for wireless voice [2-27](#)

 description [2-12](#)

 troubleshooting [9-3](#)

AP settings, identifying [9-11](#)

audience, for this document [1-xv](#)

authenticated call [1-15](#)

authentication [1-9, 5-17](#)

 selecting type [4-16, 5-14](#)

 wireless network setting [5-14](#)

auto-pickup [6-3](#)

auto-registration

 using [3-4](#)

 using with TAPS [3-4](#)

auxiliary VLAN, description [2-17](#)

B

barge [1-16, 6-4](#)

BAT (Bulk Administration Tool) [3-5](#)

battery

 charging times with desktop charger [3-19](#)

 charging times with power supply [3-11](#)

 description [3-10](#)

 figure, installing in phone [3-12](#)

 installing and removing [3-10](#)

 types available [3-10](#)

battery caution [3-8](#)

 charging [3-9](#)

 damaged [3-9](#)

 disposal [3-9](#)

- replacement re [3-9](#)
 - temperature [3-9](#)
 - battery safety notices [3-8](#)
 - battery warning
 - disposal [3-8](#)
 - explosion [3-8](#)
 - block external to external transfer [6-4](#)
- ## C
-
- call
 - authenticated [1-15](#)
 - encrypted [1-15](#)
 - call display restrictions [6-4](#)
 - caller ID [6-6](#)
 - call forward [6-5](#)
 - call forward display, configuring [6-7](#)
 - call park [6-5](#)
 - call pickup [6-5](#)
 - call statistics screen [7-1, 7-18](#)
 - call waiting [6-6](#)
 - CAPF (Certificate Authority Proxy Function) [1-13, 5-17](#)
 - cautions
 - for battery pack [3-8](#)
 - for charging battery pack [3-9](#)
 - for damaged battery [3-9](#)
 - for disposing of battery pack [3-9](#)
 - for exposing battery pack to high temperatures [3-9](#)
 - for replacing battery pack [3-9](#)
 - for replacing power supply [3-9](#)
 - translations [3-6](#)
 - CCKM
 - description [2-8](#)
 - CDP
 - description [2-9](#)
 - CDP settings [5-10](#)
 - change password web page [4-35](#)
 - Cisco Call Back [6-6](#)
 - Cisco Centralized Key Management, See CCKM
 - Cisco Discovery Protocol, See CDP
 - Cisco IOS version, supporting wireless voice LAN [2-27](#)
 - Cisco Unified CallManager
 - adding phone to database of [3-3](#)
 - configuring DHCP settings [2-26](#)
 - interacting with [2-24](#)
 - restricting phone settings access [5-2, 5-3, 5-15](#)
 - verifying settings [9-8](#)
 - Cisco Unified CallManager Administration
 - adding telephony features [6-2](#)
 - Cisco Unified IP Phone
 - configuration requirements [D-1](#)
 - configuring user services [6-19](#)
 - installation overview [1-16, D-1](#)
 - installation requirements [D-1](#)
 - modifying phone button templates [6-18](#)

- online help for [A-4](#)
 - using LDAP directories [6-21](#)
 - Cisco Unified Wireless IP Phone
 - configuration requirements [1-16](#)
 - installation requirements [1-16](#)
 - overview [1-1](#)
 - web page [4-1, 8-1](#)
 - Cisco Unified Wireless IP Phone, See also wireless IP phone
 - Cisco Unified Wireless IP Phone specifications [C-1](#)
 - client matter codes [6-7](#)
 - conference [6-7](#)
 - configurable call forward display [6-7](#)
 - configuration
 - checklist for [1-17](#)
 - phones in Cisco Unified CallManager [1-17](#)
 - configuration file
 - creating new [9-10](#)
 - encrypted [1-13](#)
 - overview [2-25](#)
 - SEPxxxxxxxxxxxx.cnf.xml [2-25](#)
 - XMLDefault.cnf.xml [2-25](#)
 - configuring
 - AP tasks [2-29, D-2](#)
 - LDAP directories [6-21](#)
 - network features on phone [1-8](#)
 - overview [1-16, D-1](#)
 - personal directories [6-21](#)
 - phone button templates [6-18](#)
 - softkey templates [6-16](#)
 - user features [6-22](#)
 - CTL file
 - unlocking [7-5](#)
 - CTL file screen [7-4](#)
 - current configuration
 - viewing [7-12, 7-15](#)
-
- ## D
- data VLAN [2-17](#)
 - desktop charger
 - description [3-19](#)
 - figure [3-18](#)
 - using [3-19](#)
 - device authentication [1-12](#)
 - device information menu, about [7-1](#)
 - device information web page [8-3, 8-9](#)
 - DHCP
 - description [2-9](#)
 - displaying settings [5-8](#)
 - enable, network setting [5-6](#)
 - gateway [2-26](#)
 - interacting with [2-25](#)
 - IP address [2-26](#)
 - modifying settings [5-8](#)
 - priority for TFTP server [2-26](#)
 - scope settings [2-26](#)
 - subnet mask [2-26](#)

- troubleshooting [9-12](#)
- directory numbers, assigning manually [3-6](#)
- direct-sequence spread spectrum (DSSS) [2-4](#)
- direct transfer [6-7](#)
- displaying, network statistics [7-16](#)
- disposal warning [3-8](#)
- DNS server
 - settings for TFTP server [2-26](#)
 - troubleshooting [9-13](#)
 - verifying settings [9-8](#)
- documentation
 - additional [1-xvii](#)
 - for users [A-5](#)
 - localized versions [B-1](#)
- dynamic host configuration protocol, See DHCP

E

- EAP, description [2-9](#)
- EAP-FAST, description [2-9](#)
- EAP username
 - length [4-18](#)
 - setting [4-18](#)
- editing configuration values, guidelines [5-5](#)
- encrypted call [1-15](#)
- encrypted configuration file [1-13](#)
- encryption
 - media [1-9, 1-13](#)
 - signaling [1-9, 1-13](#)

- WEP key [4-20](#)

- erase configuration, procedure [9-25](#)

- explosive gas warning [3-7](#)

- Extensible Authentication Protocol, See EAP

- extensible authentication protocol-flexible authentication via secure tunneling, See EAP-FAST

F

- features

- configuring with Cisco Unified CallManager [1-6](#)

- informing users about [1-8](#)

- See also telephony features

- file

- creating new configuration [9-10](#)

- file authentication [1-12](#)

- firmware

- verifying version [7-22](#)

- forced authorization codes [6-8](#)

G

- group call pickup [6-8](#)

H

- help, using [A-4](#)

- hold [6-8](#)

I

image authentication [1-12](#)

installation

AP configuration tasks [2-29, D-2](#)

checklist for [1-22](#)

network requirements [3-1](#)

preparing [3-3](#)

installation warning [3-7](#)

installing

requirements, overview [1-16, D-1](#)

Internet Protocol (IP) [2-10](#)

IP, description [2-10](#)

IP address [2-26, 4-23, 5-9](#)

troubleshooting [9-7](#)

J

join [6-9](#)

L

LDAP directories, using with Cisco Unified IP Phone [6-21](#)

LEAP

description [2-10](#)

light extensible authentication protocol, See LEAP

local configuration, erasing [9-25](#)

Locale Installer [B-1](#)

localization

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

Locally Significant Certificate (LSC) [5-17](#)

M

MAC address

determining [3-3, 3-5](#)

malicious caller identification (MCID) [6-9](#)

manufacturing installed certificate (MIC) [1-12](#)

media encryption [1-13](#)

meet-me conference [6-10](#)

menu

phone settings [5-15](#)

message waiting [6-10](#)

metrics, voice quality [7-21, 8-18](#)

MIC [1-12](#)

model information screen [7-1](#)

music-on-hold [6-10](#)

N

native VLAN [2-17](#)

network configuration menu

displaying [5-3](#)

displaying WLAN configuration menu [5-12](#)

editing options [5-5](#)

network configuration web page [8-3, 8-4](#)

network connectivity, verifying [9-6](#)

network features, configuring overview [1-8](#)

networking protocol

- AES [2-8](#)
- CCKM [2-8](#)
- CDP [2-9](#)
- DHCP [2-9](#)
- IP [2-10](#)
- RTP [2-10](#)
- SCCP [2-10](#)
- supported [2-8](#)
- TCP [2-11](#)
- TFTP [2-11](#)
- TKIP [2-10](#)
- TLS [2-11](#)
- U-APSD [2-11](#)
- UDP [2-11](#)
- WEP [2-12](#)
- WiFi (802.11) [2-11](#)
- WPA [2-12](#)

network outages, identifying [9-12](#)

network protocol

- EAP [2-9](#)
- EAP-FAST [2-9](#)
- LEAP [2-10](#)
- PS-Poll [2-10](#)
- RTCP [2-10](#)

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

network settings

accessing on phone [5-2](#)

configuring [5-1](#)

DHCP enable [5-6](#)

network statistics [8-13](#)

network statistics, viewing [7-16](#)

network statistics web page [8-3](#)

O

on hook call transfer [6-10](#)

online help, using [A-4](#)

open authentication, description [2-19](#)

orthogonal frequency division multiplexing (OFDM) [2-3, 2-4](#)

other group pickup [6-11](#)

P

personal directories, configuring [6-21](#)

phone audio, troubleshooting [9-14](#)

phone button templates, modifying [6-18](#)

phone mode

- active [3-25](#)
- standby [3-25](#)

phone operation for users [A-2](#)

phone resets, resolving problems [9-11](#)

phone roaming, troubleshooting [9-15](#)

phones

- configuration checklist (table) [1-17](#)
- installation checklist (table) [1-22](#)

- installing [1-22](#)
- phone settings [5-15](#)
 - access restrictions [5-2, 5-3, 5-15](#)
- phone upgrade web page [4-34](#)
- phone web page
 - about [4-1, 8-1](#)
 - accessing [4-7, 8-2](#)
 - change password [4-35](#)
 - device information [8-3, 8-9](#)
 - installing drivers [4-2](#)
 - network configuration [8-4](#)
 - network configuration web page [8-3](#)
 - network statistics [8-3, 8-13](#)
 - phone upgrade [4-34](#)
 - profile settings [4-10](#)
 - summary information [4-9, 8-3](#)
 - system settings [4-29](#)
 - trace logs [4-30](#)
 - trace settings [4-27](#)
 - USB settings [4-25](#)
- plug-socket warning [3-7](#)
- powering on phone [3-20, 3-23](#)
- power outage warning [3-7](#)
- power save poll, See PS-Poll
- power supply
 - connecting [3-14](#)
 - figure, connected [3-15, 3-16](#)
- power supply replacement caution [3-9](#)
- power supply warning [3-7](#)

- primary DNS server [2-27, 4-23, 5-9](#)
- primary gateway [2-26, 4-23, 5-9](#)
- primary TFTP server [5-9](#)
- Privacy [6-11](#)
- profile settings web page [4-10](#)
- provides [2-32](#)
- PS-Poll, description [2-10](#)
- Push to Talk service [6-11](#)

Q

- QBSS, description [2-13](#)
- QoS basis service set, See QBSS
- QRT softkey [6-12](#)
- Quality of Service (QoS) [2-16](#)
- Quality Reporting Tool (QRT) [6-12](#)

R

- RADIUS server authentication, description [2-20](#)
- real-time control protocol, See RTCP
- real-time transport protocol, See RTP
- received signal strength indicator, See RSSI
- redial [6-12](#)
- registering, resolving problems with Cisco Unified CallManager [9-5](#)
- resetting, phones [9-13](#)
- resolving startup problems [9-1 to 9-10](#)
- resolving voice quality problems [9-11 to 9-17](#)

- ring activity [6-12](#)
 - ringlist.xml [6-25](#)
 - ring tone, creating custom [6-25](#)
 - roaming [2-15](#)
 - description [2-14](#)
 - fast and secure with CCKM [2-15](#)
 - layer 3 [2-15](#)
 - Layer 3 with WLSM [2-15](#)
 - mid-call [2-15](#)
 - pre-call [2-14](#)
 - resolving problems [9-11](#)
 - RSSI, description [2-13](#)
 - RTCP, description [2-10](#)
 - RTP description [2-10](#)
- S**
-
- SCCP description [2-10](#)
 - secure SRST reference [1-13](#)
 - security
 - AES encryption [2-21](#)
 - CAPF (Certificate Authority Proxy Function) [1-13, 5-17](#)
 - device authentication [1-12](#)
 - encrypted configuration file [1-13](#)
 - file authentication [1-12](#)
 - image authentication [1-12](#)
 - manufacturing installed certificate (MIC) [1-12](#)
 - media encryption [1-13](#)
 - open authentication [2-19](#)
 - RADIUS server authentication [2-20](#)
 - secure SRST reference [1-13](#)
 - security profiles [1-13, 1-14](#)
 - shared key authentication [2-19](#)
 - signaling authentication [1-12](#)
 - signaling encryption [1-13](#)
 - static WEP encryption [2-21](#)
 - TKIP encryption [2-21](#)
 - WLAN overview [2-6](#)
 - WPA authentication [2-20](#)
 - WPA-Pre-shared key authentication [2-19](#)
 - security configuration menu, about [7-1](#)
 - security profiles [1-13, 1-14](#)
 - SEPxxxxxxxxxxxxx.cnf.xml configuration file [2-25](#)
 - services
 - configuring for users [6-19](#)
 - description [6-13](#)
 - subscribing to [6-19](#)
 - service set identifier, See SSID
 - shared key authentication, description [2-19](#)
 - shared lines [6-13](#)
 - short circuit protection warning [3-7](#)
 - signaling authentication [1-12](#)
 - signaling encryption [1-13](#)
 - site survey
 - performing [2-31](#)
 - verification steps [2-31](#)
 - site survey utility

- accessing with phone menu [2-32](#)
 - display values [2-32](#)
 - skinny client control protocol, See SCCP
 - softkey templates, configuring [6-16](#)
 - specifications
 - operating environment [C-1](#)
 - physical [C-1](#)
 - speed dial
 - default buttons for [6-19](#)
 - speed dialing [6-3, 6-13](#)
 - SRST [8-7](#)
 - secure reference [1-13](#)
 - SSID
 - associating to an AP [2-13](#)
 - description [5-12](#)
 - wireless network setting [5-12](#)
 - standby mode [3-25](#)
 - startup
 - failure [9-2](#)
 - resolving problems with [9-1](#)
 - startup process
 - contacting Cisco Unified CallManager [3-29](#)
 - DHCP disabled [2-26](#)
 - steps and description [3-26](#)
 - static settings
 - IP address [2-26, 4-23, 5-9](#)
 - primary DNS server [2-27, 4-23, 5-9](#)
 - primary gateway [2-26, 4-23, 5-9](#)
 - primary TFTP server [5-9](#)
 - subnet mask [2-26, 4-23, 5-9](#)
 - statistics
 - call [7-18, 8-16](#)
 - network [8-13](#)
 - statistics, network [7-16](#)
 - status information [7-12, 7-15](#)
 - status menu [7-1, 7-12](#)
 - streaming statistics [8-16](#)
 - subnet mask [2-26, 4-23, 5-9](#)
 - summary information web page [4-9](#)
 - survivable remote site telephony (SRST)
 - IP address of router [7-5](#)
 - symptom
 - phone does not associate with AP [9-3](#)
 - phone does not register [9-5](#)
 - phone does not start [9-2](#)
 - phone has audio problems [9-14](#)
 - phone has roaming problems [9-15](#)
 - phone resets [9-11](#)
 - phone screen does not display [9-2](#)
 - system log server [9-24](#)
-
- T**
- TAPS (Tool for Auto-Registered Phones Support) [3-4](#)
 - TCP
 - description [2-11](#)
 - telephone receiver warning [3-8](#)
 - telephony features

- auto-pickup [6-3](#)
- barge [1-16](#), [6-4](#)
- block external to external transfer [6-4](#)
- call display restrictions [6-4](#)
- caller ID [6-6](#)
- call forward [6-5](#)
- call park [6-5](#)
- call pickup [6-5](#)
- call waiting [6-6](#)
- Cisco Call Back [6-6](#)
- client matter codes [6-7](#)
- conference [6-7](#)
- configurable call forward display [6-7](#)
- configuration references [6-3](#)
- descriptions [6-3](#)
- direct transfer [6-7](#)
- forced authorization codes [6-8](#)
- group call pickup [6-8](#)
- hold [6-8](#)
- join [6-9](#)
- malicious caller identification (MCID) [6-9](#)
- meet-me conference [6-10](#)
- music-on-hold [6-10](#)
- on hook call transfer [6-10](#)
- other group pickup [6-11](#)
- Push to Talk service (XML application) [6-11](#)
- redial [6-12](#)
- ring activity [6-12](#)
- services [6-13](#)
- shared lines [6-13](#)
- speed dialing [6-13](#)
- supported [6-3](#)
- Time-of-Day Routing [6-13](#)
- transfer [6-14](#)
- voice messaging system [6-14](#)
- template
 - phone button, modifying [6-18](#)
- temporal key integrity protocol, See TKIP
- TFTP
 - description [2-11](#)
 - troubleshooting [9-6](#)
- TFTP server
 - assigning to phone [4-23](#), [5-10](#)
 - options [4-23](#), [5-10](#)
- Time-of-Day Routing [6-13](#)
- TKIP
 - description [2-10](#)
 - encryption description [2-21](#)
- trace logs web page [4-30](#)
- trace route
 - option on phone [9-24](#)
- trace settings web page [4-27](#)
- transfer [6-14](#)
- transmission control protocol, See TCP
- transport layer security
 - See TLS
- trivial file transfer protocol, See TFTP
- troubleshooting

- AP settings [9-3, 9-11](#)
- Cisco Unified CallManager settings [9-8](#)
- DHCP [9-12](#)
- DNS [9-13](#)
- DNS settings [9-8](#)
- general information [9-20](#)
- IP addressing and routing [9-7](#)
- logging information [9-24](#)
- network connectivity [9-6](#)
- network outages [9-12](#)
- phones resetting [9-13](#)
- services on Cisco Unified CallManager [9-9](#)
- TFTP settings [9-6](#)
- VLAN configuration [9-12](#)
- wireless IP phone [9-1](#)

Trust List screen [7-5](#)

U

- U-APSD description [2-11](#)
- UDP description [2-11](#)
- unscheduled asynchronous power save delivery, See U-APSD
- USB configuration [4-2](#)
 - displaying menu [5-19](#)
- USB settings web page [4-25](#)
- user datagram protocol, See UDP
- User Options web page
 - description [6-23](#)
 - giving users access to [6-23](#)

- user options web page
 - specifying options that appear [6-24](#)
- users
 - accessing voice messages [A-7](#)
 - adding to Cisco Unified CallManager [6-22](#)
 - documentation for [A-5](#)
 - international, supporting [B-1](#)
 - required information [A-1](#)
 - wireless IP phone information [A-2](#)

V

- verifying
 - Cisco Unified CallManager settings [9-8](#)
 - firmware version [7-22](#)
 - network settings [9-6](#)
- VLAN
 - assigning separate SSIDs [2-17](#)
 - auxiliary, for voice traffic [2-17](#)
 - native, for data traffic [2-17](#)
 - separate voice for QoS [2-16](#)
 - verifying [9-12](#)
- voice messaging system [6-14](#)
- voice quality, resolving problems [9-11](#)
- voice quality metrics [7-21, 8-18](#)
- voice VLAN [2-17](#)

W

warnings

- definition [3-7](#)
- for battery disposal [3-8](#)
- for battery explosion [3-8](#)
- for disposal [3-8](#)
- for explosive gas [3-7](#)
- for installation [3-7](#)
- for plug socket [3-7](#)
- for power outages [3-7](#)
- for power supply [3-7](#)
- for short circuit protection [3-7](#)
- for telephone receiver [3-8](#)
- translations [3-6](#)

WDS, wireless domain server [2-16](#)

web page

- configuring phone settings [4-1](#)

WEP

- description [2-12](#)

WEP encryption, description [2-21](#)

WEP key

- setting up encryption [4-20](#)

WiFi (802.11)

- description [2-11](#)

Wi-Fi (802.11b) [2-3](#)

wired equivalent privacy, See WEP

wireless domain server (WDS) [2-16](#)

wireless IP phone

adding manually to Cisco Unified CallManager [3-6](#)

adding to Cisco Unified CallManager [3-3](#)

adding using auto-registration [3-4](#)

adding using auto-registration with TAPS [3-4](#)

adding using BAT [3-5](#)

battery [3-10](#)

configuration file [2-25](#)

feature overview [1-5](#)

figure [1-2](#)

keys [1-2](#)

phone modes, active and standby [3-25](#)

powering on [3-20](#), [3-23](#)

registering [3-3](#)

registering with Cisco Unified CallManager [3-4](#), [3-5](#)

supported networking protocols [2-8](#)

troubleshooting [9-1](#)

troubleshooting tips [9-20](#)

wireless IP phone, See also Cisco Unified Wireless IP Phone

wireless local area network, See WLAN

wireless network settings

authentication [5-14](#)

SSID [5-12](#)

wireless protected access, See WPA

Wireless standard, See WiFi (802.11)

WLAN

components [2-8](#)

roaming [2-14](#)

- security [2-6](#)
- security mechanisms [2-19](#)
- voice quality [2-16](#)
- WLAN configuration menu [5-12](#)
- WLAN security mode
 - authentication types [4-16](#)
- WLSM, wireless LAN services module [2-15](#)
- WPA
 - description [2-12](#)
 - encryption with TKIP, description [2-21](#)
- WPA authentication, description [2-20](#)
- WPA-pre-shared key authentication, description [2-19](#)

X

- XMLDefault.cnf.xml configuration file [2-25](#)

