Cisco Unified SIP Phone 3905 Administration Guide for Cisco Unified Communications Manager 10.0

First Published: 2013-10-17

Last Modified: 2025-05-09

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

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

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

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

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco 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.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

CONTENTS

Preface

Overview

Cisco Unified SIP Phone 3905 Administration Guide for Cisco Unified Communications Manager provides the information you need to understand, install, configure, manage, and troubleshoot the phones on a Voice-over-IP (VoIP) network.

Because of the complexity of an IP telephony network, this guide does not provide complete and detailed information for procedures that you need to perform in Cisco Unified Communications Manager or other network devices.

Audience

Network engineers, system administrators, and telecom engineers should review this guide to learn the steps that are required to set up Cisco IP Phones. The tasks described in this document involve configuring network settings that are not intended for phone users. The tasks in this manual require a familiarity with Cisco Unified Communications Manager.

Guide Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[]	Elements in square brackets are optional.

Convention	Description
{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 w include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`input` font	Information you must enter is in **`input`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control - for example, the key combination ^D in a s display means hold down the Control key while you press the D key.
<>	Nonprinting characters such as passwords are in angle brackets.

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

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

Warnings use the following convention:

Attention 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

Related Documentation

Use the following sections to obtain related information.

Cisco Unified SIP Phone 3905 Documentation

Refer to publications that are specific to your language, phone model and Cisco Unified Communications Manager release. Navigate from the following documentation URL:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-sip-phone-3900-series/tsd-products-support-series-home.html

Cisco Unified Communications Manager Documentation

See the *Cisco Unified Communications Manager Documentation Guide* and other publications that are specific to your Cisco Unified Communications Manager release on the product support page.

Documentation, Support, and Security Guidelines

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

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

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

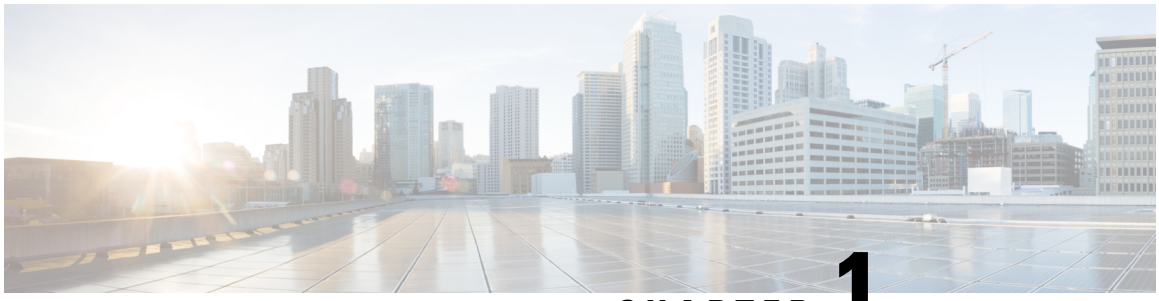
Cisco Product Security Overview

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

Further information regarding U.S. export regulations can be found at https://www.bis.gov/ear.

PART I

About the Cisco Unified IP Phone



CHAPTER 1

Technical Details

Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the Cisco Unified SIP Phone 3905.

Table 1: Physical and Operating Environment Specifications for the Cisco Unified SIP Phone 3905

Specification	Value or Range
Operating temperature	32° to 104°F (0° to 40°C)
Operating relative humidity	10% to 95% (noncondensing)
Storage temperature	14° to 140°F (-10° to 60°C)
Height	8.07 in. (20.5 cm)
Width	5.91 in. (15.0 cm)
Depth	2.11 in. (5.35 cm) - Excluding the handset
Weight	• 0.987 lb (447.8 g) - Phone without handset • 0.347 lb (157.6 g) - Handset weight
Power	• 100-240 VAC, 50-60 Hz, 0.5 A - When using the AC adapter • 48 VDC, 0.2 A - When using the in-line power over the network cable

Specification	Value or Range
Cables	Category 3/5/5e for 10-Mbps cables with 4 pairs Category 5/5e for 100-Mbps cables with 4 pairs **Note** Cables have 4 pairs of wires for a total of 8 conductors.
Distance Requirements	As supported by the Ethernet Specification, it is assumed that the maximum cable length be each CiscoUnified IP Phone and the switch is 100 meters (330feet).

Cable Specifications

- RJ-9 jack (4-conductor) for handset connection.
- RJ-45 jack for the LAN 10/100BaseT connection (labeled 10/100 SW on the Cisco Unified SIP Phone 3905).
- RJ-45 jack for a second 10/100BaseT compliant connection.
- 48-volt power connector.

Network and Computer Port Pinouts

Although both the network and computer (access) ports are used for network connectivity, they serve different purposes and have different port pinouts.

- The network port is labeled `Network` on the phone.
- The computer (access) port is labeled `Computer` on the phone.

Network Port Connector

The following table describes the network port connector pinouts.

Table 2: Network Port Connector Pinouts

Pin Number	Function
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-

Pin Number	Function
6	BI_DB-
7	BI_DD+
8	BI_DD-
Note BI stands for bidirectional, while DA, DB, DC, and DD stand for Data A, Data B, Data C, and Data D respectively.	

Computer Port Connector

The following table describes the computer port connector pinouts.

Table 3: Computer (Access) Port Connector Pinouts

Pin Number	Function
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-
Note BI stands for bidirectional, while DA, DB, DC, and DD stand for Data A, Data B, Data C, and Data D respectively.	

Phone Power Requirements

The Cisco Unified SIP Phone 3905 can be powered with external power or with Power over Ethernet (PoE). External power is provided through a separate power supply. PoE is provided by a switch through the Ethernet cable attached to a phone.

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

The following table provides guidelines for powering the Cisco Unified SIP Phone 3905.

Table 4: Cisco Unified SIP Phone 3905 power guidelines

Power Type	Guidelines
External power: Provided through the Cisco Unified SIP Phone 3905 Power Adapter.	The Cisco Unified SIP Phone 3905 uses the Cisco Unified SIP Phone 3905 Power A
External power: Provided through the Cisco Unified IP Phone Power Injector.	The Cisco Unified IP Phone Power Injector may be used with any Cisco Unified IP I Functioning as a midspan device, the injector delivers inline power to the attached ph Cisco Unified IP Phone Power Injector is connected between a switch port and the IP and supports a maximum cable length of 100m between the unpowered switch and the
PoE power: Provided by a switch through the Ethernet cable attached to the phone.	• The Cisco Unified SIP Phone 3905 supports IEEE 802.3af Class 1 power on sig and spare pairs. • To ensure uninterruptible operation of the phone, make sure that the switch has power supply. • Make sure that the CatOS or IOS version running on your switch supports your phone deployment. Refer to the documentation for your switch for operating syste information.
External power: Provided through inline power patch panel WS-PWR-PANEL	The inline power patch panel WS-PWR-PANEL is compatible with the Cisco Unifie Phone 3905.

Power Outage

Your access to emergency service through the phone requires that the phone receive power. If a power interruption occurs, service or emergency calling service dialing does not function until power is restored. If a power failure or disruption occurs, you may need to reset or reconfigure the equipment before you can use service or emergency calling service dialing.

Cisco Unified Communications Manager Interaction

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

- Firmware for phones

- Certificate Trust List (CTL) and Identity Trust List (ITL) files using the TFTP and HTTP services
- Phone registration
- Call preservation, so that a media session continues if signaling is lost between the primary Communications Manager and a phone

For information about configuring Cisco Unified Communications Manager to work with the phones described in this chapter, see the documentation for your particular Cisco Unified Communications Manager release.

Note If the phone model that you want to configure does not appear in the Phone Type drop-down list in Cisco Unified Communications Manager Administration, install the latest device package for your version of Cisco Unified Communications Manager from Cisco.com.

Network Protocols

CiscoUnifiedIPPhones support several industry-standard and Cisco network protocols required for voice communication. The following table provides an overview of the network protocols that the Cisco Unified SIP Phone 3905 support.

Table 5: Supported Network Protocols

Network Protocol	Purpose	Usage Notes
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.	The phone uses CDP to communicate info as auxiliary VLAN ID, per port power m details, and Quality of Service (QoS) con information with the Cisco Catalyst swit
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect an IP phone into the network and have the phone become operational without your needing to manually assign an IP address or to configure additional network parameters.	DHCP is enabled by default. If disabled, manually configure the IP address, subne gateway, and a TFTP server on each pho Cisco recommends that you use DHCP c 150. With this method, you configure the IP address as the option value. For additio DHCP configurations, go to the "Dynam Configuration Protocol" chapter and the " chapter in the *Cisco Unified Communicat System Guide*. **Note** If you cannot use option 150, you may try option 66.

Network Protocol	Purpose	Usage Notes
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Cisco UnifiedIP Phones use HTTP for troubl purposes.
IEEE 802.1X	The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.	The Cisco Unified IP Phone implements the 802.1X standard by providing support for th authentication method. When 802.1X authentication is enabled on t you should disable the voice VLAN.
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communicate using IP, network devices n an assigned IP address, subnet, and gateway. IP addresses, subnets, and gateways identific automatically assigned if you are using the C UnifiedIPPhone with Dynamic Host Configu Protocol (DHCP). If you are not using DHCP manually assign these properties to each pho
Link Layer Discovery Protocol (LLDP)	LLDP is a standardized network discovery protocol (similar to CDP) that is supported on some Cisco and third-party devices.	The Cisco UnifiedIPPhone supports LLDP on and PC port.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard developed for voice products.	The Cisco UnifiedIPPhone supports LLDP-M the SW port to communicate information suc • Voice VLAN configuration • Device discovery • Power management • Inventory management For more information about LLDP-MED sup the LLDP-MED and "Cisco Discovery Protoc paper: http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	Cisco Unified IP Phones use the RTP protoc and receive real-time voice traffic from othe and gateways.
Real-Time Control Protocol (RTCP)	RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round trip delay) on RTP streams.	RTCP is disabled by default, but you can ena a per phone basis by using CiscoUnified Communications Manager.

Network Protocol	Purpose	Usage Notes
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.	Like other VoIP protocols, SIP is designe the functions of signaling and session ma within a packet telephony network. Signa call information to be carried across netw boundaries. Session management provid to control the attributes of an end-to-end
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Cisco Unified IP Phones use TCP to con Unified Communications Manager.
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the Cisco UnifiedIPPhone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your net can be automatically identified from the I If you want a phone to use a TFTP serve the one specified by the DHCP server, yo manually assign the IP address of the TF using the Network Configuration menu o For more information, go to the "CiscoT in the *Cisco Unified Communications Ma Guide*.
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	Cisco Unified IP Phones transmit and rec streams, which utilize UDP.

Related Topics

Cisco Unified Communications Manager Interaction, on page 4

VLAN Interaction

The Cisco Unified SIP Phone 3905 has an internal Ethernet switch, enabling forwarding of packets to the phone, and to the access port and the network port on the back of the phone.

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

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

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

- Voice traffic to and from the IP phone (auxiliary VLAN on the Cisco Catalyst 6000 series, for example)
- Data traffic to and from the PC connected to the switch through the access port of the IP phone (native VLAN)

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

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

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

External Devices

We recommend that you use good-quality external devices that are shielded against unwanted radio frequency (RF) and audio frequency (AF) signals. External devices include headsets, cables, and connectors.

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

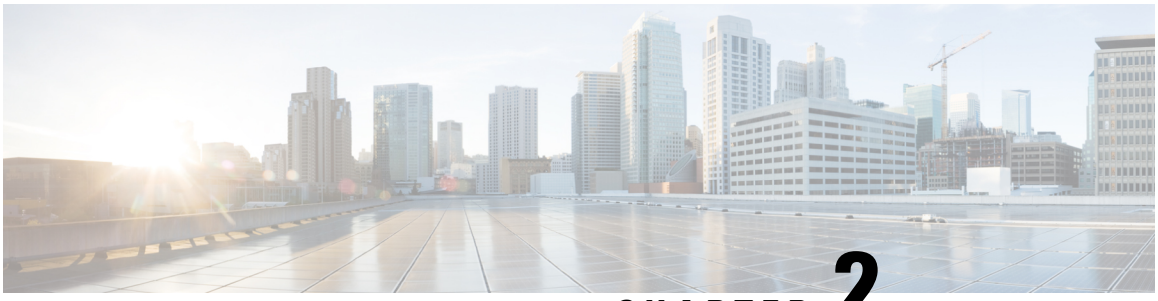
- Move the external device away from the source of the RF or AF signals.
- Route the external device cables away from the source of the RF or AF signals.
- Use shielded cables for the external device, or use cables with a better shield and connector.
- Shorten the length of the external device cable.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

Cisco cannot guarantee the performance of external devices, 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].

Phone Behavior During Times of Network Congestion

- Administrative tasks, such as an internal port scan or security scan.
- Attacks that occur on your network, such as a Denial of Service attack.



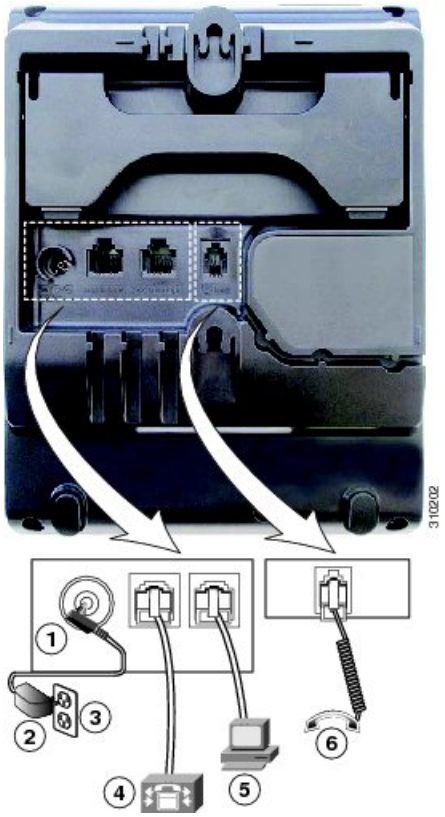
CHAPTER 2

Cisco Unified SIP Phone Hardware

Cisco Unified SIP Phone 3905

Phone Connections

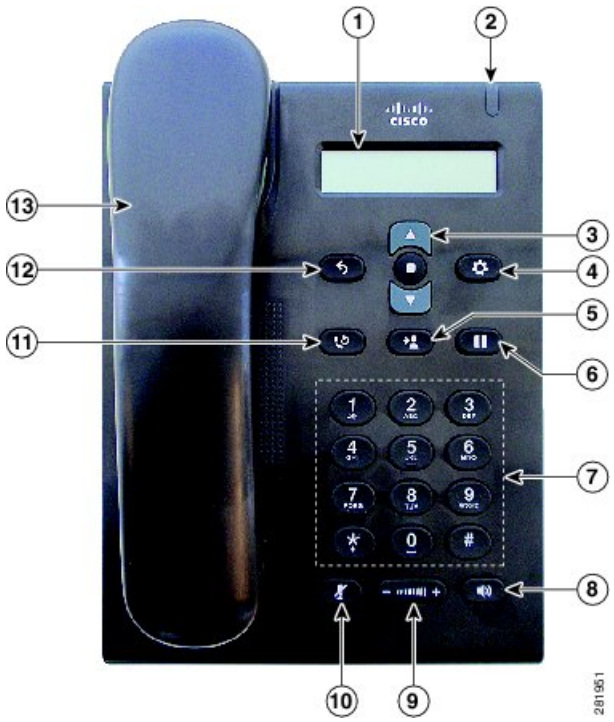
Figure 1: A rough diagram of connecting a phone to the network



1	DC adapter port (DC 4.2V).	4	Network port (10/100 SW) connection. IEEE 802.3af power enabled.
2	AC-to-DC power supply (optional).	5	Access port (10/100 PC) connection.
3	AC power wall connection.	6	Handset connection.

Note In the EU and UK, your phone is shipped with a power switch cable that is required in order to provide power to your phone when using an AC-to-DC power supply. Connect the power cord to the power switch cable and then connect the other end of the power switch cable to the DC adapter port.

Buttons and Hardware



1	Phone screen	Shows information about your phone such as directory number, active call, and phone menu listings.
2	Light strip	Indicates an incoming call (flashing red) or new voice message (steady red).

3	Navigation bar and Select/Feature button 	The Navigation bar allows you to scroll through menus and highlight items. The Select button (in the middle of the Navigation bar) allows you to select a highlighted item. When the phone is off-hook, the Select button functions as the Feature button. You can access these features: • Call Forward All: Allows you to forward a call. • Voice Mail: Allows you access voice mails. • Call Pickup: Allows you to answer a call that is ringing on a co-worker's phone. • Group Call Pickup: Allows you to answer a call that is ringing in another call group.
4	Applications button 	Opens or closes the Applications menu. Use it to access call history, user preferences, phone settings, and phone model information.
5	Transfer button 	Transfers a call.
6	Hold/Resume button 	Places an active call on hold or resumes a held call.
7	Keypad	Allows you to dial phone numbers.
8	Speakerphone button 	Selects the speakerphone as the default audio path and initiates a new call, picks up an incoming call, or ends a call. The speakerphone audio path does not change until a new default audio path is selected (for example, by picking up the handset).
9	Volume button 	Controls the handset and speakerphone volume (off-hook) and the ringer volume (on hook).
10	Mute button 	Toggles the microphone on or off.
11	Redial button 	Dials the last dialed number.
12	Back button 	Returns to the previous screen or menu.
13	Handset	Phone handset.

Terminology Differences

The following table highlights some of the important differences in terminology that is used in these documents:

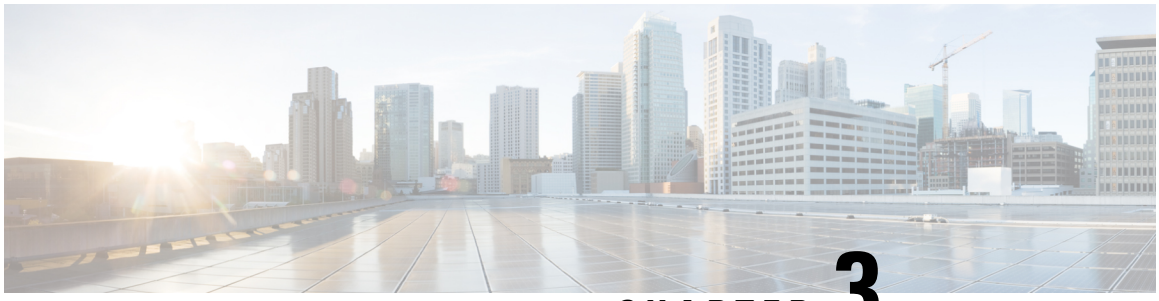
- *Cisco Unified SIP Phone 3905 User Guide for Cisco Unified Communications Manager*
- *Cisco Unified SIP Phone 3905 Administration Guide for Cisco Unified Communications Manager*

- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager System Guide*

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

PART II

Cisco Unified SIP Phone Installation



CHAPTER 3

Cisco Unified SIP Phone Installation

Verify Network Setup

Before you install a phone, you must decide how to configure the phone in your network. Then you can install the phone and verify its functionality.

For the phone to successfully operate as an endpoint in your network, your network must meet specific requirements.

Note The phone displays the date and time from Cisco Unified Communications Manager. The time displayed on the phone can differ from the Cisco Unified Communications Manager time by up to 10 seconds.

Procedure

Step 1 Configure a VoIP Network to meet the following requirements:

- VoIP is configured on your Cisco routers and gateways.
- Cisco Unified Communications Manager is installed in your network and is configured to handle call processing.

Step 2 Set up the network to support one of the following:

- DHCP support

- Manual assignment of IP address, gateway, and subnet mask

Enable Autoregistration for Phones

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

Before you install the Cisco IP Phone, you must choose a method for adding phones to the Cisco Unified Communications Manager database.

By enabling autoregistration before you install the phones, you can:

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

Autoregistration is disabled by default. In some cases, you might not want to use autoregistration; for example, if you want to assign a specific directory number to the phone, or if you want to use a secure connection with Cisco Unified Communications Manager. For information about enabling autoregistration, see the documentation for your particular Cisco Unified Communications Manager release. When you configure the cluster for mixed mode through the Cisco CTL client, autoregistration is automatically disabled, however you can enable it. When you configure the cluster for nonsecure mode through the Cisco CTL client, autoregistration is not enabled automatically.

You can add phones with autoregistration and TAPS, the Tool for AutoRegistered Phones Support, without first gathering MAC addresses from phones.

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

Cisco recommends that you use autoregistration and TAPS to add fewer than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT).

To implement TAPS, you or the end user dials a TAPS directory number and follows voice prompts. After the process is complete, the phone contains the directory number and other settings, and the phone is updated in Cisco Unified Communications Manager Administration with the correct MAC address.

Verify that autoregistration is enabled and is properly configured in Cisco Unified Communications Manager Administration before you connect any Cisco IP Phone to the network. For information about enabling and configuring autoregistration, see the documentation for your particular Cisco Unified Communications Manager release.

Autoregistration must be enabled in Cisco Unified Communications Manager Administration for TAPS to function.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, click **System** > **Cisco Unified CM**.

Step 2 Click **Find** and select the required server.

Step 3 In **Auto-registration Information**, configure these fields.

- **Universal Device Template**
- **Universal Line Template**
- **Starting Directory Number**
- **Ending Directory Number**

Step 4 Uncheck the **Auto-registration Disabled on this Cisco Unified Communications Manager** check box.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Install Cisco Unified SIP Phone

The following steps provide an overview and checklist of installation tasks for the Cisco Unified SIP Phone 3905. 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.

Procedure

Step 1 Choose the power source for the phone:

- Power over Ethernet (PoE)
- External power supply

Determines how the phone receives power. For more information, see Phone Power Requirements, on page 3.

Step 2 Connect the handset to the Handset port.

Step 3 (Optional) Connect the power supply to the Cisco DC Adapter port. See Phone Addition Methods, on page 35 for guidelines.

Step 4 Connect a straight-through Ethernet cable from the switch to the network port labeled Network on the Cisco Unified SIP Phone 3905. Each phone ships with one Ethernet cable in the box.

You can use either Category 3, 5, or 5e cabling for 10-Mbps connections, but you must use Category 5 or 5e for 100 Mbps connections.

Step 5 Connect a straight-through Ethernet cable from another network device, such as a desktop computer, to the access port labeled Computer. You can connect another network device later if you do not connect one now.

You can use either Category 3, 5, or 5e cabling for 10-Mbps connections, but you must use Category 5 or 5e for 100 Mbps connections.

Step 6 Monitor the phone startup process. This step associates directory numbers to the phone and verifies that phone is configured properly.

For more information, see Verify Phone Startup, on page 27.

Step 7 If you are configuring the network settings on the phone, you can set up an IP address for the phone by either using DHCP or manually entering an IP address.

- Using DHCP: Verify that DHCP is enabled. You can set an alternate TFTP by entering the IP address for the TFTP.

  Note
  Consult with the network administrator to determine whether you need to assign an alternative TFTP server instead of using the TFTP server assigned by DHCP.

- Without DHCP: Verify that DHCP is disabled. You must then configure the IP address, subnet mask, TFTP server, and default router locally.

For more information, see Configure Network Settings, on page 20.

Step 8 Set up security on the phone. This step provides protection against data tampering threats and identity theft of phones.

For more information, see Cisco Unified SIP Phone Security, on page 53.

Step 9 Upgrade the phone to the current firmware image.

Step 10 Make calls with the phone. This step verifies that the phone and features work correctly.

For more information, see the *Cisco Unified SIP Phone 3905 User Guide for Cisco Unified Communications Manager*.

Step 11 Provide information to end users about how to use their phones and how to configure their phone options. This step ensures that users have adequate information to successfully use their phones.

For more information, see Cisco IP Phone User Support, on page 57.

Set Up Phone from Setup Menus

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

The phone includes the following setup menus:

- Network Setup: Provides options for viewing and configuring a variety of network settings.
  - IPv4 Setup: This submenu provides additional network options.
- Security Setup: Provides options for viewing and configuring a variety of security settings.

Before you can change option settings on the Network Setup menu, you must unlock options for editing.

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

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

If you cannot access an option on the Administrator Settings menu, check the Settings Access field.

You configure settings that are display-only on the phone in Cisco Unified Communications Manager Administration.

To display a configuration menu, follow these steps:

Procedure

Step 1 Press **Applications** .

Step 2 Select **Admin Settings**.

Step 3 Select **Network** or **Security**.

Note
For information about the Reset Settings menu, see Maintenance, on page 105.

Step 4 Enter your user ID and password, if required, then press **Select**.

Step 5 Perform one of these actions to display the desired menu:

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

Step 6 To display a submenu, repeat step 5.

Step 7 To exit a menu, press **Back**.

Apply a Phone Password

Procedure

Step 1 In Cisco Unified Communications Manager Administration, navigate to the Common Phone Profile Configuration window (**Device** > **Device Settings** > **Common Phone Profile**).

Step 2 Enter a password in the Local Phone Unlock Password option.

Step 3 Apply the password to the common phone profile that the phone uses.

Text and Menu Entry from Phone

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

- Use the arrows on the navigation pad to highlight the field that you wish to edit, then press **Select** in the navigation pad to activate that field. You can also double-tap on an editable field to activate it for editing. After the field is activated, you can enter values.
- Use the keys on the keypad to enter numbers and letters.
- To enter letters by using the keypad, use a corresponding number key. Press the key one or more times to display a particular letter. For example, press the **2** key once for "a," twice quickly for "b," and three times quickly for "c." After you pause, the cursor automatically advances to allow you to enter the next letter.
- To delete a character to the left of the cursor, use the **Hold/Resume** button.
- Press the arrow button to cancel or save your update.
- To enter an IP address, use the star (*) key to input:
  - the period (.) in IPv4 addresses

Note The Cisco IP Phone provides several methods to reset or restore option settings, if necessary.

Related Topics

Apply a Phone Password, on page 20
Basic Reset, on page 105

Configure Network Settings

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

- IP address

- IP subnet information
- Default Router
- TFTP server IP address

The Network Setup menu provides options for viewing and making a variety of network settings. The following table describes these options and, where applicable, explains how to change them.

Table 6: Network Setup Menu Options

Option	Description	To Change
IPv4	In the IPv4 Setup submenu, you can do the following: • Enable or disable the phone to use the IP address that is assigned by the DHCP server. • Manually set the IP Address, Subnet Mask, Default Routers, DNS Server, and Alternate TFTP servers.	Scroll to IPv4 Setup and p
MAC Address	Unique Media Access Control (MAC) address of the phone	Display only - Cannot cor
Host Name	Unique host name that the DHCP server assigned to the phone.	Display only - Cannot cor
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.	See Set Domain Name Fi 23.
Operational VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member. If the phone has not received an auxiliary VLAN, this option indicates the Administrative VLAN. If neither the auxiliary VLAN nor the Administrative VLAN are configured, this option defaults to a VLAN ID of 4095.	Display only - Cannot cor The phone obtains its Ope VLAN ID via Cisco Disco (CDP) from the switch to phone is attached. To assi ID manually, use the Adm option.
Admin. VLAN ID	Auxiliary VLAN in which the phone is a member. Used only if the phone does not receive an auxiliary VLAN from the switch; otherwise it is ignored.	See Set Admin VLAN ID I 24.
PC VLAN	Allows the phone to interoperate with 3rd party switches that do not support a voice VLAN. The Admin VLAN ID option must be set before you can change this option.	See Set PC VLAN Field,

Option	Description	To Change
SW Port Setup	Speed and duplex of the network port. Valid values: • Auto Negotiate • 100 Half: 100-BaseT/half duplex • 100 Full: 100-BaseT/full duplex • 10 Half: 10-BaseT/half duplex • 10 Full: 10-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to auto-negotiate. If you change the setting of this option, you must change the PC Port Configuration option to the same setting.	See Set SW Port Setup Field, 24.
PC Port Setup	Speed and duplex of the access port. Valid values: • Auto Negotiate • 100 Half: 100-BaseT/half duplex • 100 Full: 100-BaseT/full duplex • 10 Half: 10-BaseT/half duplex • 10 Full: 10-BaseT/full duplex If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to auto-negotiate. If you change the setting of this option, you must change the SW Port Configuration option to the same setting.	See Set PC Port Setup Field, 24.

The IPv4 Setup menu is a submenu of the Network Setup menu. To reach the IPv4 Setup menu, select the IPv4 option on the Network Setup menu. The following table describes the IPv4 Setup menu options.

Table 7: IPv4 Setup menu options

Option	Description	To Change
DHCP Enabled	Indicates whether the phone has DHCP enabled or disabled. When DHCP is enabled, the DHCP server assigns the phone an IP address. When DHCP is disabled, the administrator must manually assign an IP address to thephone.	See Set DHCP Enabled Field, 25.
IP Address	Internet Protocol (IP) address of the phone. If you assign an IP address with this option, you must also assign a subnet mask and default router. See the Subnet Mask and Default Router options in this table.	See Set IP Address Field, on p
Subnet Mask	Subnet mask used by the phone.	See Set Subnet Mask Field, or
Default Router 1	Default router used by the phone (Default Router 1).	See Set Default Router Field, 25.

Option	Description	To Change
DNS Server 1	Primary Domain Name System (DNS) server (DNS Server 1) used by the phone.	See Set DNS Server Field
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.	See Set Alternate TFTP Fi 26.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone. If you are not using DHCP in your network and you want to change this server, you must use the TFTP Server 1 option. If you set the Alternate TFTP option to yes, you must enter a non-zero value for the TFTP Server 1 option.	See Set TFTP Server 1 Fi 26.
TFTP Server 2	Optional backup TFTP server that the phone uses if the primary TFTP server is unavailable.	See Set TFTP Server 2 Fi 26.
DHCP Address Released	Releases the IP address assigned by DHCP.	Scroll to the DHCP Addre option and press Select, th to release the DHCP Addr

Procedure

Step 1 On the phone, press **Applications**.
Step 2 Select **Admin Settings** and login if required.
Step 3 Select **Network**.
Step 4 To access the IPv4 setup fields, scroll to IPv4 and press **Select**.

Set Domain Name Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the Domain Name option, press **Select**, and enter a new domain name.
Step 3 Press **Select**.

Set Admin VLAN ID Field

Procedure

Step 1 Scroll to the Admin. VLAN ID option, press **Select**, and enter a new Admin VLAN setting.
Step 2 Press **Select**.

Set PC VLAN Field

Procedure

Step 1 Ensure that the Admin VLAN ID option is set.
Step 2 Scroll to the PC VLAN option, press **Select**, and then enter a new PC VLAN setting.
Step 3 Press **Select**.

Set SW Port Setup Field

Procedure

Step 1 Unlock network configuration options.
Step 2 Scroll to the SW Port Setup option and press **Select**.
Step 3 Scroll to the setting that you want and press **Select**.

Set PC Port Setup Field

Procedure

Step 1 Unlock network configuration options.
Step 2 Scroll to the PC Port Setup option and press **Select**.
Step 3 Scroll to the setting that you want and press **Select**.

Set DHCP Enabled Field

Procedure

Step 1 Scroll to the DHCP Enabled option.
Step 2 Press **No** to disable DHCP, or press **Yes** to enable DHCP.

Set IP Address Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the IP Address option, press **Select**, and enter a new IP address.
Step 3 Press **Select**.

Set Subnet Mask Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the Subnet Mask option, press **Select**, and enter a new subnet mask.
Step 3 Press **Select**.

Set Default Router Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the appropriate Default Router option, press **Select**, and enter a new router IP address.
Step 3 Press **Select**.

Set DNS Server Field

Procedure

Step 1 Set the DHCP Enabled option to **No**.
Step 2 Scroll to the appropriate DNS Server option, press **Select**, and enter a new DNS server IP address.
Step 3 Press **Select**.

Set Alternate TFTP Field

Procedure

Step 1 Scroll to the Alternate TFTP option.
Step 2 Press **Edit**.
Step 3 Press **Yes** if the phone should use an alternative TFTP server.
Step 4 Press **No** if the phone should not use an alternative TFTP server.

Set TFTP Server 1 Field

Procedure

Step 1 If DHCP is enabled, set the Alternate TFTP option to **Yes**.
Step 2 Scroll to the TFTP Server 1 option, press **Select**, and enter a new TFTP server IP address.
Step 3 Press **Select**.

Set TFTP Server 2 Field

Procedure

Step 1 Unlock network configuration options.
Step 2 Enter an IP address for the TFTP Server 1 option.
Step 3 Scroll to the TFTP Server 2 option, press **Select**, and enter a new backup TFTP server IP address. If there is no secondary TFTP Server, you can use **Delete** to clear the field of a previous value.

Step 4 Press **Select**.

Verify Phone Startup

After the Cisco IP Phone has power connected to it, the phone automatically cycles through a startup diagnostic process.

Procedure

Step 1 If you are using Power over Ethernet, plug the LAN cable into the Network port.

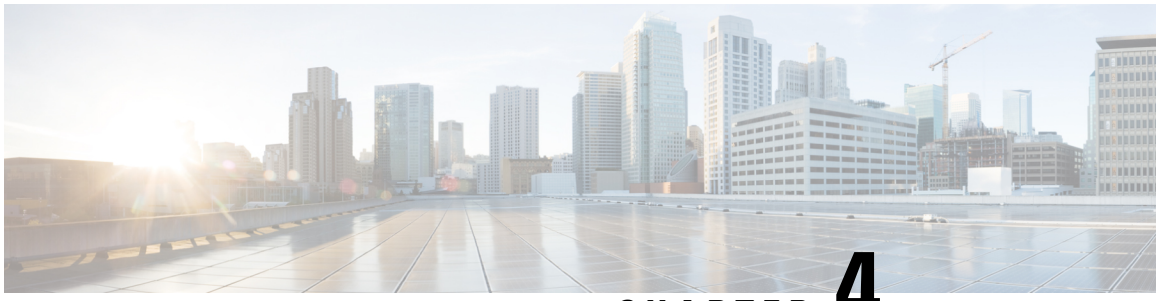
Step 2 If you are using the power cube, connect the cube to the phone and plug the cube into an electrical outlet.

The buttons flash amber and then green in sequence during the various stages of bootup as the phone checks the hardware.

If the phone completes these stages successfully, it has started up properly.

Related Topics

Startup Problems, on page 89
Cisco IP Phone Does Not Go Through the Normal Startup Process, on page 90



CHAPTER 4

Cisco Unified Communications Manager Phone Setup

Phone Configuration Files

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

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

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file will contain sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For more information, see the documentation for your particular Cisco Unified Communications Manager release. A phone requests a configuration file whenever it resets and registers with Cisco Unified Communications Manager.

A phone accesses a default configuration file named XmlDefault.cnf.xml from the TFTP server when the following conditions exist:

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

Set Up Cisco Unified SIP Phone

If autoregistration is not enabled and the phone does not exist in the Cisco Unified Communications Manager database, you must configure the Cisco IP Phone in Cisco Unified Communications Manager manually. Some tasks in this procedure are optional, depending on your system and user needs.

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

Perform the configuration steps in the following procedure using Cisco Unified Communications Manager Administration.

Procedure

Step 1 Gather the following information about the phone:

- Phone model
- MAC address
- Physical location of the phone
- Name or user ID of phone user
- Device pool
- Partition, calling search space, and location information
- Associated directory number (DN) to assign to the phone
- Cisco Unified Communications Manager user to associate with the phone

The information provides a list of configuration requirements for setting up phones and identifies preliminary configuration that you need to perform before configuring individual phones.

For more information, see the "CiscoUnified IP Phones" chapter in the *Cisco Unified Communications Manager System Guide* and Telephony Features, on page 58.

Step 2 Verify that you have sufficient unit licenses for your phone.

For more information, go to the "License Unit Report" chapter in the *Cisco Unified Communications ManagerAdministration Guide*.

Step 3 Define the phone button templates that determine the configuration of buttons on a phone. Select **Device** > **Device Settings** > **Phone Button Template** to create and update the templates.

For more information, see the "Phone button template setup" chapter in the *Cisco Unified Communications ManagerAdministration Guide* .

Step 4 Define the Device Pools. Select **System** > **Device Pool**.

Device Pools define common characteristics for devices, such as region, date/time group, softkey template, and MLPP information. For information on Device Pool setup, see the "Device pool setup" chapter in the *Cisco Unified Communications Manager Administration Guide* .

Step 5 Define the Common Phone Profile. Select **Device** > **Device settings** > **Common Phone Profile**.

Common phone profiles provide data that the Cisco TFTP server requires, as well as common phone settings, such as Do Not Disturb and feature control options. For more information, see the "Common phone profile setup" chapter in the *Cisco Unified Communications ManagerAdministration Guide*.

Step 6 Define a Calling Search Space. In Cisco Unified Communications Manager Administration, click **Call Routing** > **Class of Control** > **Calling Search Space**.

A Calling Search Space is a collection of partitions that are searched to determine how a dialed number is routed. The calling search space for the device and the calling search space for the directory number are used together. The directory number CSS takes precedence over the device CSS. For more information, see the "Calling search space setup" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Step 7 Configure a security profile for the device type and protocol. Select **System** > **Security** > **Phone Security Profile**.

For more information, see the "Phone security profile setup" chapter in the *Cisco Unified Communications Manager Security Guide*.

Step 8 Set up the phone. Select **Device** > **Phone**.

a) Locate the phone you want to modify or add a new phone.

b) Configure the phone by completing the required fields in the Device Information pane of the Phone Configuration window.

- MAC Address (required): Make sure that the value comprises 12 hexadecimal characters.
- Description: Enter a useful description to help you if you need to search on information about this user.
- Device Pool (required)
- Phone Button Template: The phone button template determines the configuration of buttons on a phone.
- Common Phone Profile
- Calling Search Space
- Location
- Owner User ID

The device with its default settings is added to the Cisco Unified Communications Manager database.

For information about Product Specific Configuration fields, see the "?" Button Help in the Phone Configuration window.

Note
If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, see "End user phone addition" chapter in the *Cisco Unified Communications Manager Guide*.

c) In the Protocol Specific Information area of this window, choose a Device Security Profile and set the security mode.

Note

Choose a security profile based on the overall security strategy of the company. If the phone does not support security, choose a nonsecure profile.

d) In the Extension Information area, check the Enable Extension Mobility check box if this phone supports Cisco Extension Mobility.
e) Click **Save**.

Step 9 Select **Device** > **Phone** to configure directory numbers (lines) on the phone by completing the required fields in the Directory Number Configuration window.

a) Find the phone.
b) In the Phone Configuration window, click Line 1 on the left pane of the window.
c) In the Directory Number field, enter a valid number that can be dialed.

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

d) From the Route Partition drop-down list, choose the partition to which the directory number belongs. If you do not want to restrict access to the directory number, choose <None> for the partition.
e) From the Calling Search Space drop-down list, choose the appropriate calling search space. The value that you choose applies to all devices that are using this directory number.
f) In the Call Forward and Call Pickup Settings area, choose the items (for example, Forward All, Forward Busy Internal) and corresponding destinations to which calls should be sent.

Example:

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

g) In the Line 1 on Device pane, configure the following fields:

- Display (Internal Caller ID field): You can enter the first name and last name of the user of this device so that this name displays for all internal calls. Leave this field blank to have the system display the phone extension.
- External Phone Number Mask: Indicate phone number (or mask) that is used to send Caller ID information when a call is placed from this line. You can enter a maximum of 24 numeric and "X" characters. The Xs represent the directory number and must appear at the end of the pattern.

Example:

If you specify a mask of 408902XXXX, an external call from extension 6640 displays a caller ID number of 4089026640.

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

h) Select **Save**.

For more information, see the "Directory number setup" chapter in the *Cisco Unified Communications Manager Administration Guide* and see Telephony Features, on page 58.

Step 10 Associate the user with a phone. Click **Associate End Users** at the bottom of the Phone Configuration window to associate a user to the line that is being configured.

a) Use **Find** in conjunction with the Search fields to locate the user.
b) check the box next to the user name, and click **Add Selected**.

The user name and user ID appears in the Users Associated With Line pane of the Directory Number Configuration window.

c) Select **Save**.
d) Select **Save**.

The user is now associated with Line 1 on the phone.

e) If the phone has a second line, configure Line 2.

Step 11 Associate the user with the device:

a) Choose **User Management** > **End User**.
b) Use the search boxes and **Find** to locate the user you have added.
c) Click on the user ID.
d) In the Directory Number Associations area of the screen, set the Primary Extension from the drop-down list.
e) In the Mobility Information area, check the Enable Mobility box.
f) In the Permissions Information area, use the **Add to Access Control Group** buttons to add this user to any user groups.

For example, you may want to add the user to a group that is defined as a Standard CCM End User Group.

g) To view the details of a group, select the group and click **View Details**.
h) In the Extension Mobility area, check the Enable Extension Mobility Cross Cluster box if the user can use for Extension Mobility Cross Cluster service.
i) In the Device Information area, click **Device Associations**.
j) Use the Search fields and **Find** to locate the device that you want to associate to the user.
k) Select the device, and click **Save Selected/Changes**.
l) Click **Go** next to the "Back to User" Related link in the upper right corner of the screen.
m) Select **Save**.

Step 12 Customize the softkey templates. Select **Device** > **Device Settings** > **Softkey Template**.

Use the page to add, delete, or change the order of softkey features that display on the user's phone to meet feature usage needs.

For more information, see the "Softkey template setup" and "Cisco UnifiedIPPhone setup" chapters in the *Cisco Unified Communications ManagerAdministration Guide*.

Step 13 Configure speed-dial buttons and assign speed-dial numbers. Select **Device** > **Phone**.

Note
Users can change speed-dial settings on their phones using their Self Care Portal.

a) Find the phone you want to set up.
b) In the Association Information area, click **Add a new SD**.
c) Set up the speed dial information.
d) Select **Save**.

Step 14 Configure Cisco IPPhone services and assign services. Select **Device** > **Device Settings** > **Phone Services**.

Provides IP Phone services to the phone.

Note
Users can add or change services on their phones using the Cisco Unified Communications Self Care Portal.

Step 15 (Optional) Assign services to programmable buttons. Select **Device** > **Device Settings** > **Phone Button Profile**.

Provides access to an IP phone service or URL.

Step 16 Add user information to the global directory for Cisco Unified Communications Manager. Select **User Management** > **End User** and configure the required fields. Required fields are indicated by an asterisk (*); for example, User ID and last name.

Note
If your company uses a Lightweight Directory Access Protocol (LDAP) directory to store information on users, you can install and configure Cisco Unified Communications Manager to use your existing LDAP directory, see "Understanding Directory Numbers" in the *Cisco Unified Communications Manager System Guide*. After the Enable Synchronization from the LDAP Server field is enabled, you will not be able to add additional users from Cisco Unified Communications Manager Administration.

Note
If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, see "End user phone addition" in *Cisco Unified Communications ManagerAdministration Guide*.

a) Set the User ID and last name fields.
b) Assign a password (for Self Care Portal).
c) Assign a PIN (for Cisco Extension Mobility and Personal Directory).
d) Associate the user with a phone.

Provides users with control over their phone such a forwarding calls or adding speed-dial numbers or services.

Note
Some phones, such as those in conference rooms, do not have an associated user.

Step 17 Associate a user with a user group. Select **User Management** > **User Settings** > **Access Control Group**.

Assigns users a common list of roles and permissions that apply to all users in a user group. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users. For more information, see Add a User to an End User Group, on page 38.

In order for end users to access the Cisco Unified Communications Self Care Portal, you must add users to the standard Cisco Communications Manager End Users group.

For more information, see "End user setup" and "Access control group setup" in the *Cisco Unified Communications ManagerAdministration Guide*.

Determine the Phone MAC Address

To add phones to Cisco Unified Communications Manager, you must determine the MAC address of a phone.

Procedure

Perform one of the following actions:

- On the phone, press **Applications**, select **Phone Information** and look at the MAC Address field.
- Look at the MAC label on the back of the phone.
- Display the web page for the phone and click **Device Information**.

Phone Addition Methods

After you install the Cisco IP Phone, you can choose one of the following options to add phones to the Cisco Unified Communications Manager database.

- Add phones individually with Cisco Unified Communications Manager Administration
- Add multiple phones with the Bulk Administration Tool (BAT)
- Autoregistration
- BAT and the Tool for Auto-Registered Phones Support (TAPS)

Before you add phones individually or with BAT, you need the MAC address of the phone. For more information, see Determine the Phone MAC Address, on page 34.

For more information about the Bulk Administration Tool, see the documentation for your particular Cisco Unified Communications Manager release.

Add Phones Individually

Collect the MAC address and phone information for the phone that you will add to the Cisco Unified Communications Manager.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 Click **Add New**.

Step 3 Select the phone type.

Step 4 Select **Next**.

Step 5 Complete the information about the phone including the MAC Address.

For complete instructions and conceptual information about Cisco Unified Communications Manager, see the documentation for your particular Cisco Unified Communications Manager release.

Step 6 Select **Save**.

Add Phones with a BAT Phone Template

The Cisco Unified Communications Bulk Administration Tool (BAT) enables you to perform batch operations, including registration of multiple phones.

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

For more information about using BAT, see the documentation for your particular Cisco Unified Communications Manager release.

Procedure

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

Step 2 Click **Add New**.

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

Step 4 Enter the details of phone-specific parameters, such as Device Pool, Phone Button Template, and Device Security Profile.

Step 5 Click **Save**.

Step 6 Select **Device** > **Phone** > **Add New** to add a phone using the BAT phone template.

Add Users to Cisco Unified Communications Manager

You can display and maintain information about the users registered in Cisco Unified Communications Manager. Cisco Unified Communications Manager also allows each user to perform these tasks:

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

Procedure

Step 1 To add users individually, see Add a User Directly to Cisco Unified Communications Manager, on page 37.

Step 2 To add users in batches, use the Bulk Administration Tool. This method also enables you to set an identical default password for all users.

For more information, see the documentation for your particular Cisco Unified Communications Manager release.

Add a User from an External LDAP Directory

If you added a user to an LDAP Directory (a non-Cisco Unified Communications Server directory), you can immediately synchronize the LDAP directory to the Cisco Unified Communications Manager on which you are adding the user and the user phone.

Note If you do not synchronize the LDAP Directory to the Cisco Unified Communications Manager immediately, the LDAP Directory Synchronization Schedule on the LDAP Directory window determines when the next autosynchronization is scheduled. Synchronization must occur before you can associate a new user to a device.

Procedure

Step 1 Sign into Cisco Unified Communications Manager Administration.

Step 2 Select **System** > **LDAP** > **LDAP Directory**.

Step 3 Use **Find** to locate your LDAP directory.

Step 4 Click on the LDAP directory name.

Step 5 Click **Perform Full Sync Now**.

Add a User Directly to Cisco Unified Communications Manager

If you are not using a Lightweight Directory Access Protocol (LDAP) directory, you can add a user directly with Cisco Unified Communications Manager Administration by following these steps.

Note If LDAP is synchronized, you cannot add a user with Cisco Unified Communications Manager Administration.

Procedure

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

Step 2 Click **Add New**.

Step 3 In the User Information pane, enter the following:

- User ID: Enter the end user identification name. Cisco Unified Communications Manager does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #,;, \,, "", and blank spaces. **Example**: johndoe

- Password and Confirm Password: Enter five or more alphanumeric or special characters for the end user password. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces.
- Last Name: Enter the end user last name. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces. **Example**: doe
- Telephone Number: Enter the primary directory number for the end user. End users can have multiple lines on their phones. **Example**: 26640 (John Doe’s internal company telephone number)

Step 4 Click **Save**.

Add a User to an End User Group

To add a user to the Cisco Unified Communications Manager Standard End User group, perform these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **User Management** > **User Settings** > **Access Control Group**.

The Find and List Users window displays.

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

Step 3 Select the **Standard CCM End Users** link. The User Group Configuration window for the Standard CCM End Users appears.

Step 4 Select **Add End Users to Group**. The Find and List Users window appears.

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

A list of users that matches your search criteria appears.

Step 6 In the list of records that appear, click the check box next to the users that you want to add to this user group. If the list is long, use the links at the bottom to see more results.

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

Step 7 Choose **Add Selected**.

Associate Phones with Users

You associate phones with users from the Cisco Unified Communications Manager End User window.

Procedure

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

The Find and List Users window appears.

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

Step 3 In the list of records that appear, select the link for the user.

Step 4 Select **Device Association**.

The User Device Association window appears.

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

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

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

Step 8 From the Related Links drop-down list in the upper, right corner of the window, select **Back to User**, and click **Go**.

The End User Configuration window appears and the associated devices that you chose display in the Controlled Devices pane.

Step 9 Choose **Save Selected/Changes**.

Perform Final End User Configuration Steps

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

In the End User configuration window, do the following:

Procedure

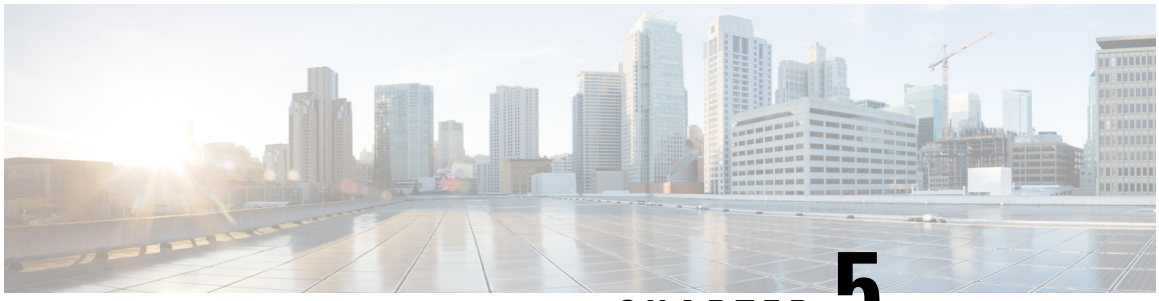
Step 1 In the Directory Number Associations pane of the screen, set the primary extension from the drop-down list.

Step 2 In the Mobility Information pane, check the Enable Mobility box.

Step 3 In the Permissions Information pane, use the User Group buttons to add this user to any user groups. For example, you may want to add the user to a group that has been defined as a Standard CCM End User Group.

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

Step 4 Click **Save**.



CHAPTER 5

Self Care Portal Management

Self Care Portal Overview

From the Cisco Unified Communications Self Care Portal, users can customize and control phone features and settings.

As the administrator, you control access to the Self Care Portal. You must also provide information to your users so that they can access the Self Care Portal.

Before a user can access the Cisco Unified Communications Self Care Portal, you must use Cisco Unified Communications Manager Administration to add the user to a standard Cisco Unified Communications Manager End User group.

You must provide end users with the following information about the Self Care Portal:

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

  `https://<server_name:portnumber>/ucmuser/`, where server_name is the host on which the web server is installed, and portnumber is the port number on that host.

- A user ID and default password to access the application.

- An overview of the tasks that users can accomplish with the portal.

These settings correspond to the values that you entered when you added the user to Cisco Unified Communications Manager.

For more information, see the documentation for your particular Cisco Unified Communications Manager release.

Set Up User Access to the Self Care Portal

Before a user can access the Self Care Portal, you need to authorize the access.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **User Management** > **End User**.
Step 2 Search for the user.
Step 3 Click the user ID link.
Step 4 Ensure that the user has a password and PIN configured.
Step 5 In the Permission Information section, ensure that the Groups list includes **Standard CCM End Users**.
Step 6 Select **Save**.

Customize the Self Care Portal Display

Most options display on the Self Care Portal. However, you must set the following options by using Enterprise Parameters Configuration settings in Cisco Unified Communications Manager Administration:

- Show Ring Settings
- Show Line Label Settings

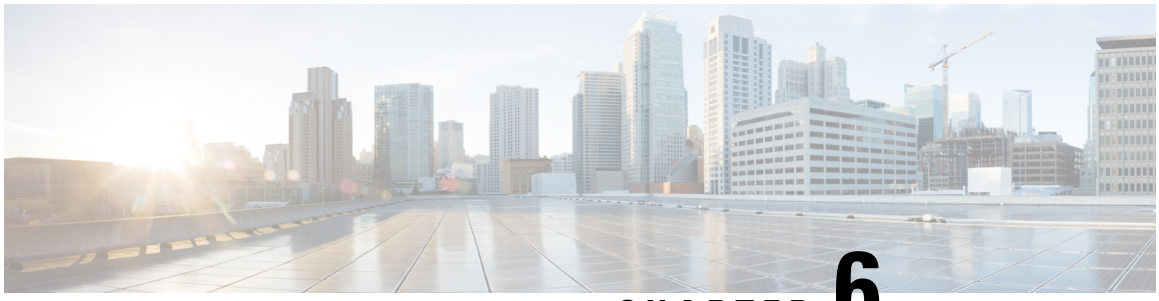
Note The settings apply to all Self Care Portal pages at your site.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **System** > **Enterprise Parameters**.
Step 2 In the Self Care Portal area, set the **Self Care Portal Default Server** field.
Step 3 Enable or disable the parameters that the users can access in the portal.
Step 4 Select **Save**.

PART III

Hardware and Accessory Installation



CHAPTER 6

Cisco Unified SIP Phone Accessories

Adjust footstand

Procedure

The Cisco Unified IP Phone 3905 has a foldable footstand. Unfold the footstand to give the phone an elevated viewing angle.

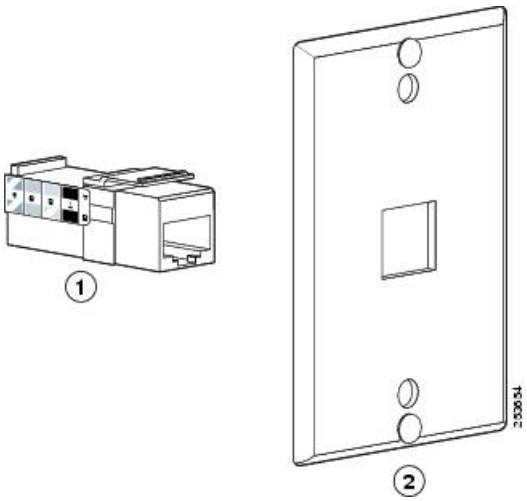
Install Phone on Wall Mount Plate

Before you begin

You can mount the Cisco Unified SIP Phone 3905 on the wall by using a standard telephone wall plate with an opening for an RJ-45 connector. Cisco recommends that you use Leviton Wall Mount plate (Leviton type number: 4108W-0SP) to wall mount the Cisco Unified SIP Phone 3905.

The following figure shows a list of items required to mount the Cisco Unified SIP Phone

Figure 2: Leviton Wall Mount Plate



1	RJ45 Connector	2	Leviton Wall Mount Plate

Procedure

Step 1 Plug the telephone line cord (RJ45 connector) into the phone jack at the base of the phone as shown in the following image:

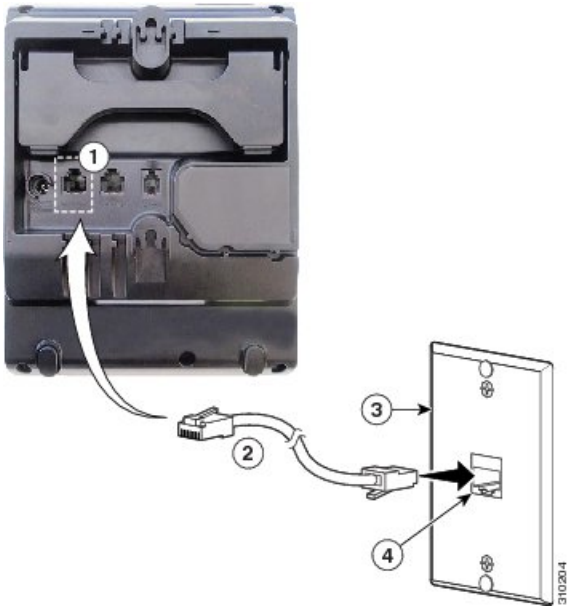
Figure 3: RJ45 Connector in the Phone Jack

1	Network Port on the Phone

2	RJ45 Connector

Step 2 Plug the RJ45 connector into the wall mount phone jack as shown in the following image:

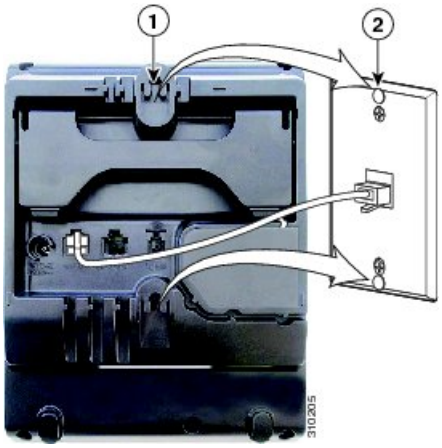
Figure 4: RJ45 Connector in the Wall Mount Jack



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

Step 3 Slip the mounting holes on the base of the wall mount plate and over the wall mount pins as shown in the following image:

Figure 5: Mounting Holes

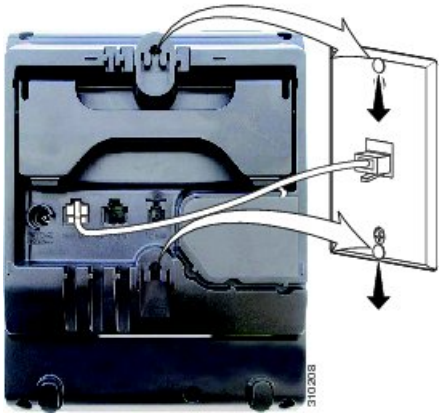


1	Mounting Hole on the Phone

2	Wall Mount Pin on the Wall Mount Plate

Step 4 Firmly slide the IP phone down into place as shown in the following image:

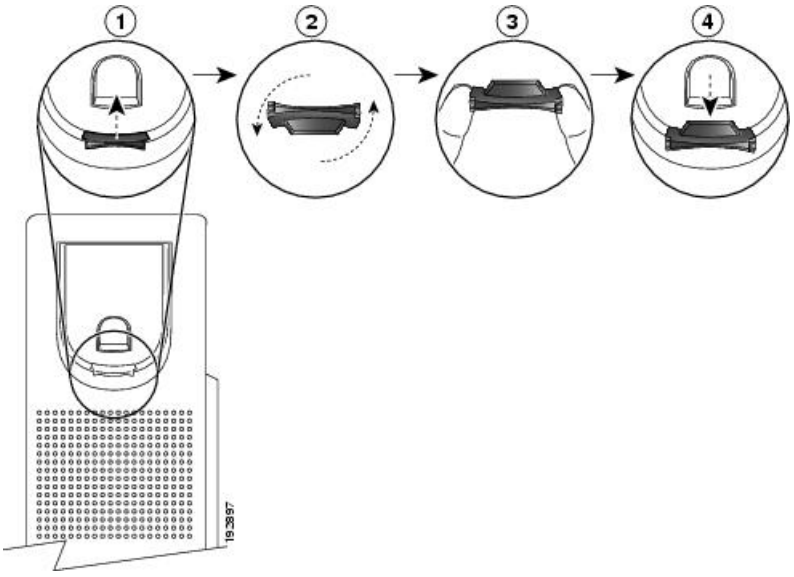
Figure 6: Sliding the IP Phone



Adjust the Handset Rest

If your phone is wall-mounted or if the handset slips out of the cradle too easily, you may need to adjust the handset rest to ensure that the receiver does not slip out of the cradle.

Figure 7: Adjust the Handset Rest



Procedure

Step 1 Remove the handset from the cradle and pull the plastic tab from the handset rest.

Step 2 Rotate the tab 180 degrees.

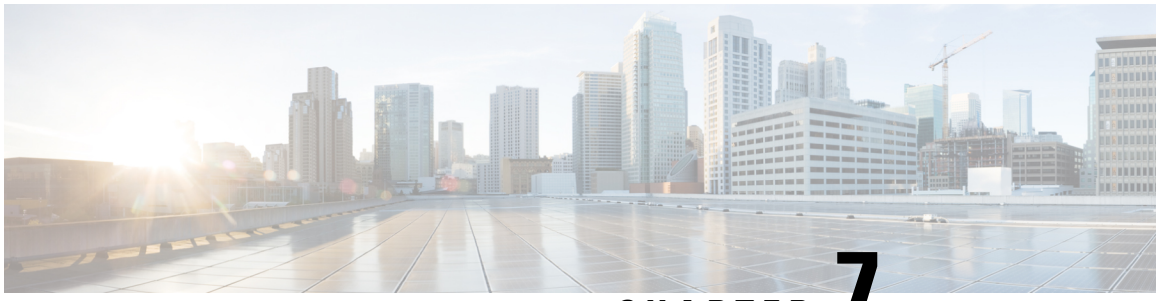
Step 3 Hold the tab between two fingers, with the corner notches facing you.

Step 4 Line up the tab with the slot in the cradle and press the tab evenly into the slot. An extension protrudes from the top of the rotated tab.

Step 5 Return the handset to the handset rest.

PART IV

Cisco Unified SIP Phone Administration



CHAPTER 7

Cisco Unified SIP Phone Security

Cisco Unified SIP Phone Security Features

The following table provides an overview of the security features that the Cisco Unified SIP Phone 3905 supports. For more information about these features and about Cisco Unified Communications Manager and phone security, see the *Cisco Unified Communications Manager Security Guide*.

Table 8: Phone and Cisco Unified Communications Manager Security Topics

Topic	Reference
Detailed explanation of security, including set up, configuration, and troubleshooting information for Cisco Unified Communications Manager and Cisco UnifiedIP Phones	See the *Troubleshooting Guide for Cisco Unified Com Manager*.
Security and the phone startup process	See Verify Phone Startup, on page 27.
Security and phone configuration files	See Phone Addition Methods, on page 35.
Disabling access to a phone web pages	See Control Phone Web Page Access, on page 62.
Troubleshooting	• See Troubleshooting , on page 89 • See the *Troubleshooting Guide for Cisco Unifie Communications Manager*
Resetting or restoring the phone	See Basic Reset, on page 105.
802.1X Authentication for Cisco Unified IP Phones	See these sections: • 802.1X Authentication, on page 54 • Troubleshooting , on page 89

802.1X Authentication

The Cisco IP Phones support 802.1X Authentication.

Cisco IP Phones and Cisco Catalyst switches traditionally use Cisco Discovery Protocol (CDP) to identify each other and determine parameters such as VLAN allocation and inline power requirements. CDP does not identify locally attached workstations. Cisco IP Phones provide an EAPOL pass-through mechanism. This mechanism allows a workstation attached to the Cisco IP Phone to pass EAPOL messages to the 802.1X authenticator at the LAN switch. The pass-through mechanism ensures that the IP phone does not act as the LAN switch to authenticate a data endpoint before accessing the network.

Cisco IP Phones also provide a proxy EAPOL Logoff mechanism. In the event that the locally attached PC disconnects from the IP phone, the LAN switch does not see the physical link fail, because the link between the LAN switch and the IP phone is maintained. To avoid compromising network integrity, the IP phone sends an EAPOL-Logoff message to the switch on behalf of the downstream PC, which triggers the LAN switch to clear the authentication entry for the downstream PC.

Support for 802.1X authentication requires several components:

- Cisco IP Phone: The phone initiates the request to access the network. Cisco IP Phones contain an 802.1X supplicant. This supplicant allows network administrators to control the connectivity of IP phones to the LAN switch ports. The current release of the phone 802.1X supplicant uses the EAP-FAST and EAP-TLS options for network authentication.
- Cisco Secure Access Control Server (ACS) (or other third-party authentication server): The authentication server and the phone must both be configured with a shared secret that authenticates the phone.
- Cisco Catalyst Switch (or other third-party switch): The switch must support 802.1X, so it can act as the authenticator and pass the messages between the phone and the authentication server. After the exchange completes, the switch grants or denies the phone access to the network.

You must perform the following actions to configure 802.1X.

- Configure the other components before you enable 802.1X Authentication on the phone.
- Configure PC Port: The 802.1X standard does not consider VLANs and thus recommends that only a single device should be authenticated to a specific switch port. However, some switches (including Cisco Catalyst switches) support multidomain authentication. The switch configuration determines whether you can connect a PC to the PC port of the phone.
    - Enabled: If you are using a switch that supports multidomain authentication, you can enable the PC port and connect a PC to it. In this case, Cisco IP Phones support proxy EAPOL-Logoff to monitor the authentication exchanges between the switch and the attached PC. For more information about IEEE 802.1X support on the Cisco Catalyst switches, see the Cisco Catalyst switch configuration guides at:

      http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
    - Disabled: If the switch does not support multiple 802.1X-compliant devices on the same port, you should disable the PC Port when 802.1X authentication is enabled. If you do not disable this port and subsequently attempt to attach a PC to it, the switch denies network access to both the phone and the PC.
- Configure Voice VLAN: Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.

- Enabled: If you are using a switch that supports multidomain authentication, you can continue to use the voice VLAN.
- Disabled: If the switch does not support multidomain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN.

Set Device Authentication Field

Procedure

Step 1 Press **Applications**.
Step 2 Choose **Admin Settings** > **Security** > **802.1X Authentication** > **Device Authentication**.
Step 3 Press **Select**.
Step 4 Set the Device Authentication option to Enabled or Disabled.
Step 5 Press **Select** to confirm.

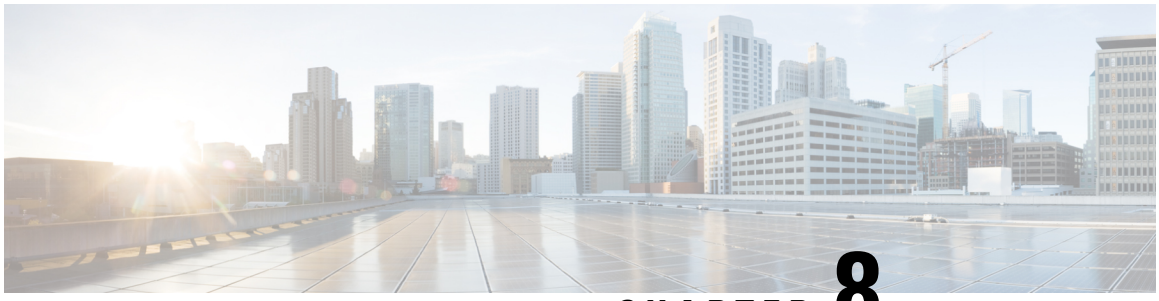
Set Shared Secret Field

Choose a password to use on the phone and on the authentication server. The password must be between 6 and 32 characters, consisting of any combination of numbers or letters.

Note If you disable 802.1X authentication or perform a factory reset of the phone, the shared secret is deleted.

Procedure

Step 1 Press **Applications**.
Step 2 Choose **Admin Settings** > **Security** > **802.1X Authentication** > **EAP-MD5** > **Shared Secret**.
Step 3 Press **Select**.
Step 4 Enter the shared secret.
Step 5 Press **Select** to confirm.



CHAPTER 8

Phone Features and Setup

Phone Features and Setup Overview

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

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

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

For suggestions about how to provide users with information about features, and what information to provide, see Cisco IP Phone User Support, on page 57.

For information about setting up phones in non-English environments, see International User Support, on page 109.

Cisco IP Phone User Support

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

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

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

Consider including the following types of information on this site:

- User guides for all Cisco IP Phone models that you support
- Information on how to access the Cisco Unified Communications Self Care Portal
- List of features supported
- User guide or quick reference for your voicemail system

Telephony Features

CiscoUnified IP Phones provide traditional telephony functionality, such as call forwarding and transferring, redialing, conference calling, and voice messaging system access. CiscoUnified IP phones also provide a variety of other features.

As with other network devices, you must configure CiscoUnified IP Phones to prepare them to access CiscoUnifiedCommunications Manager and the rest of the IP network. By using DHCP, you have fewer settings to configure on a phone, but if your network requires it, you can manually configure an IP address, TFTP server, subnet information, and so on.

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

You can modify additional settings for the CiscoUnified IP Phone from Cisco Unified Communications Manager Administration. Use Cisco Unified Communications Manager Administration to set up phone registration criteria and calling search spaces, among other tasks. See the “Telephony Features” section in this document and the CiscoUnifiedCommunications Manager documentation for additional information.

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

After you add CiscoUnified IP Phones to CiscoUnifiedCommunications Manager, you can add functionality to the phones. The following table includes a list of supported telephony features, many of which you can configure using CiscoUnifiedCommunications Manager Administration.

For information about using most of these features on the phone, see the *Cisco Unified SIP Phone 3905 User Guide for Cisco Unified Communications Manager*.

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

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

Table 9: Telephony Features

Feature	Description
Audible Message Waiting Indicator (AMWI)	A stutter tone from the handset or speakerphone indicates that a user has one or more new voice a line. See the *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chap
Auto Answer	Connects incoming calls automatically after a ring or two. Auto Answer works with the speakerphone. See the *Cisco Unified Communications Manager Administration Guide*, "Directory Number Co chapter.
Block External to External Transfer	Prevents users from transferring an external call to another external number. See the *Cisco Unified Communications Manager Features and Services Guide*, "External Call T Restrictions" chapter.
Call Forward	Allows users to redirect incoming calls to another number. The Call Forward All option is supp hear a stutter tone after going off-hook if the Call Forward All feature is configured on the phor See: • *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configu • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter • Customize the Self Care Portal Display, on page 42
Call Forward All Loop Breakout	Detects and prevents Call Forward All loops. When a Call Forward All loop is detected, the Ca configuration is ignored and the call rings through. See the *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chap
Call Forward All Loop Prevention	Prevents a user from configuring a Call Forward All destination directly on the phone that creates All loop or that creates a Call Forward All chain with more hops than the existing Forward Max Count service parameter allows. See the *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chap
Call Forward Destination Override	Allows you to override Call Forward All (CFA) in cases where the CFA target places a call to the This feature allows the CFA target to reach the CFA initiator for important calls. The override w the CFA target phone number is internal or external. See the *Cisco Unified Communications Manager System Guide*, "Understanding Directory Num
Call Pickup	Allows users to answer a call that is ringing on a co-worker's phone by redirecting the call to th You can configure an audio alert for the primary line on the phone. This alert notifies the users ringing in their pickup group. See the *Cisco Unified Communications Manager Features and Services Guide*, "Call Pickup" c
Call Waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. The phone sounds the call waiting tone (single beep) and the phone screen displays the second See *Cisco Unified Communications Manager System Guide*, "Understanding Directory Number

Feature	Description
cBarge	Allows a user to join a non-private call on a shared phone line. cBarge adds a user to a call and con a conference, allowing the user and other parties to access conference features. For more information, see the *Cisco UnifiedCommunications Manager Features and Services Guid* and Privacy" chapter.
Conference	• Allows a user to talk simultaneously with multiple parties by calling each participant individu • Allows a non-initiator in a standard (adhoc) conference to add participants; also allows any co participant to join together two standard conferences on the same line. The service parameter, Advance Adhoc Conference, (disabled by default in Cisco Unified Commu Manager Administration) allows you to enable these features. See: • CiscoUnified Communications Manager System Guide, "Conference Bridges" chapter. • *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phone" chapter. **Note** Be sure to inform your users whether these features are activated.
Forced Authorization Codes (FAC)	Controls the types of calls that certain users can place. For more information, see the *Cisco UnifiedCommunications Manager Features and Services Guid* Matter Codes" and "Forced Authorization Codes" chapters.
Group Call Pickup	Allows a user to answer a call that is ringing on a directory number in another group. For more information, see the *Cisco Unified Communications Manager Features and Services Gui* Pickup" chapter.
Hold/Resume	Allows the user to move a connected call from an active state to a held state by using the Hold/Resu The user resumes a held call by pressing the Hold/Resume button, speaker button, or going off-hoo No configuration required unless you want to use music on hold. See "Music-On-Hold" in this tabl information.
Hookflash Timer	Controls the length of time before the hookflash indicates a timeout (or call disconnect). See *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Con chapter.
Line Text Label	Sets a text label for a phone line instead of the directory number. See Set the Label for a Line, on page 63.
Message Waiting	Defines directory numbers for message-waiting on and message-waiting off indicator. A directly co voice-messaging system uses the specified directory number to set or to clear a message-waiting in a particular Cisco Unified IP Phone. See: • *Cisco Unified Communications Manager Administration Guide*, "Message Waiting Configurati • *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco U Communications Manager" chapter.

Feature	Description
Message Waiting Indicator	A light on the phone that indicates that a user has one or more new voice messages. See: • *Cisco Unified Communications Manager Administration Guide*, "Message Waiting Configu • *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisc Communications Manager" chapter
Music On Hold	Plays music while callers are on hold. See the *Cisco Unified Communications Manager Features and Services Guide*, "Music On Hol
Mute	Mutes the microphone from the handset or speakerphone. No configuration required.
On-hook Call Transfer	Allows a user to press the Transfer button and then go on-hook to complete a call transfer. See the *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" cha
Plus Dialing	Allows the user to dial E.164 numbers prefixed with a **+** sign. To dial the + sign, the user needs to press and hold the ***** key for at least 1 second. This applies t first digit for both on-hook or off-hook calls. Requires no configuration.
Private Line Automated Ringdown (PLAR)	The Cisco UnifiedCommunications Manager administrator can configure a phone number that t UnifiedIPPhone dials as soon as the handset goes off-hook. This can be useful for phones that a for calling emergency or *hotline* numbers. See the *Cisco Unified Communications Manager Administration Guide*, "Directory Number Co chapter.
Redial	Allows users to call the most recently dialed phone number by pressing the Redial button. No configuration required.
Shared Line	Allows a user to have multiple phones that share the same phone number or allows a user to sha number with a coworker. See the *Cisco Unified Communications Manager System Guide*, "Understanding Directory Nun
Telnet	You can use Telnet to connect to your Cisco Unified IP Phone for use in troubleshooting and phon See: • *Cisco Unified Communications Manager Administration Guide*, " Cisco Unified IP Phone chapter • *Cisco Unified Communications Manager Administration Guide*, "SIP Profile Configuratio chapter
Time-of-Day Routing	Restricts access to specified telephony features by time period. See: • *Cisco Unified Communications Manager Administration Guide*, "Time Period Configurati • *Cisco Unified Communications Manager System Guide*, "Time-of-Day Routing" chapter

Feature	Description
Time Zone Update	Updates the Cisco Unified IP Phone with time zone changes. See the *Cisco Unified Communications Manager Administration Guide*, "Time Group Configuratio
Transfer	Allows users to redirect connected calls from their phones to another number. No configuration required.
Voice Messaging System	Enables callers to leave messages if calls are unanswered. See: • *Cisco Unified Communications Manager Administration Guide*, " Cisco Voice-Mail Port Conf chapter • *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Un Communications Manager" chapter

Disable Speakerphone

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

You can disable the speakerphone by using Cisco Unified Communications Manager Administration. When the speakerphone is disabled, the Redial, New Call, and Forward All softkeys are not displayed on the phones when the user presses the speakerphone button. The softkey labels are dimmed or removed.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **Device** > **Phone**.

Step 2 Select the phone you want to modify.

Step 3 In the Phone Configuration window for the phone, check the **Disable Speakerphone** check box.

Step 4 Select **Save**.

Control Phone Web Page Access

For security purposes, access to the phone web pages is disabled by default. This practice prevents access to the phone web pages and the Cisco Unified Communications Self Care Portal.

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

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.
Step 2 Specify the criteria to find the phone and select **Find**, or select **Find** to display a list of all phones.
Step 3 Select the device name to open the Phone Configuration window for the device.
Step 4 Scroll to the Product Specific Configuration area.
Step 5 To enable access, from the Web Access drop-down list, choose **Enabled**.
Step 6 To disable access, from the Web Access drop-down list, choose **Disabled**.
Step 7 Select **Save**.

Set the Label for a Line

You can set up a phone to display a text label instead of the directory number. Use this label to identify the line by name or function. For example, if your user shares lines on the phone, you could identify the line with the name of the person that shares the line.

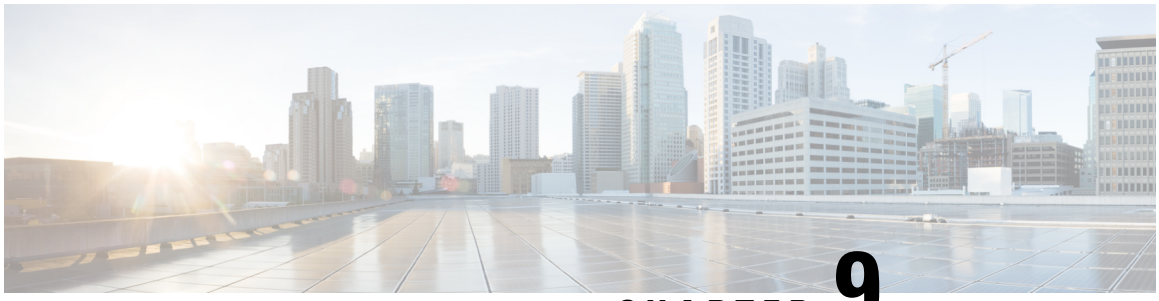
When adding a label to a key expansion module, only the first 25 characters are displayed on a line.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select **Device** > **Phone**.
Step 2 Locate the phone to be configured.
Step 3 Locate the line instance and set the Line Text Label field.
Step 4 (Optional) If the label needs to be applied to other devices that share the line, check the Update Shared Device Settings check box and click **Propagate Selected**.
Step 5 Select **Save**.

PART V

Cisco Unified IP Phone Troubleshooting



CHAPTER 9

Monitoring Phone Systems

Cisco Unified SIP Phone status

This section describes how to use the following menus on the Cisco Unified SIP Phone 3905 to view model information, status messages, and network statistics for the phone:

- Model Information screen: Displays hardware and software information about the phone.
- Status menu: Provides access to screens that display the status messages, network statistics, 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, and obtain other related information, remotely through the phone web page.

For more information about troubleshooting the Cisco Unified SIP Phone 3905, see Troubleshooting , on page 89

Display Model Information Window

To display the Model Information screen, follow these steps.

Procedure

Step 1 Press **Applications**.

Step 2 Select **Phone Information**.

If the user is connected to a secure or authenticated server, a corresponding icon (lock or certificate) displays in the Phone Information Screen to the right of the server option. If the user is not connected to a secure or authenticated server, no icon appears.

Step 3 To exit the Model Information screen, press **Back**.

Related Topics

Cisco IP Phone Web Page, on page 75

Model Information Fields

The following table describes the Model Information Settings fields.

Table 10: Model Information Settings fields

Option	Description	To Change
Model Number	Model number of the phone.	Display only - cannot configure.
MAC Address	MAC address of the phone.	Display only - cannot configure.
Active Load ID	Version of firmware currently installed on the phone.	Display only - cannot configure.
Boot Load ID	Identifier of the factory-installed load running on the phone.	Display only - cannot configure.
IP Address	IP address of the phone.	Display only - cannot configure.
Active Server	IP address or name of the server to which the phone is registered.	Display only - cannot configure.
Stand-by Server	IP address or name of the standby server.	Display only - cannot configure.

Display Status Menu

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

- Network Statistics: Displays the Network Statistics screen, which shows Ethernet traffic statistics
- Call Statistics: Displays counters and statistics for the current call.

Procedure

Step 1 Press **Applications**.

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

Step 3 To exit the Status menu, press **Back** .

Display Status Messages Window

To display the Status Messages screen,

Procedure

Step 1 Press **Applications**.

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

For information on the messages, see Status Messages, on page 69.

Step 3 To exit the Status Messages screen, press **Back**.

Related Topics

Phone Displays Error Messages, on page 91

Status Messages

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

Table 11: Status Messages on the Cisco Unified SIP Phone 3905

Message	Description	Possible Explanation and Action
CFG file not found	The name-based and default configuration file was not found on the TFTP Server.	The configuration file for a phone is create phone is added to the Cisco UnifiedCommu Manager database. If the phone has not beer Cisco UnifiedCommunications Manager da TFTP server generates a **`CFG File Not`** response. • Phone is not registered with Cisco Un Communications Manager. You must manually add the phone to C UnifiedCommunications Manager if y allowing phones to auto-register. See Addition Methods, on page 35 for deta • If you are using DHCP, verify that the is pointing to the correct TFTP server. • If you are using static IP addresses, che server configuration.
CFG TFTP Size Error	The configuration file is too large for the file system on the phone.	Power cycle the phone.
Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firmware a the TFTPPath directory. You should only c this directory when the TFTP server softwa down, otherwise the files may be corrupted

Message	Description	Possible Explanation and Action
DHCP timeout	DHCP server did not respond.	• Network is busy. The errors should resolv themselves when the network load reduce • No network connectivity between the DH and the phone. Verify the network connec • DHCP server is down. Check the DHCP s configuration. • Errors persist. Consider assigning a static I
DNS timeout	DNS server did not respond.	• Network is busy. The errors should resolv themselves when the network load reduce • No network connectivity between the DN and the phone. Verify the network connec • DNS server is down. Check the DNS serv configuration.
DNS unknown host	DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	• Verify that the host names of the TFTP se Cisco UnifiedCommunications Manager a configured properly in DNS. • Consider using IP addresses rather than ho
Duplicate IP	Another device is using the IP address assigned to the phone.	• If the phone has a static IP address, verify have not assigned a duplicate IP address. • If you are using DHCP, check the DHCP configuration.
File not found	The phone cannot locate, on the TFTP server, the phone load file that is specified in the phone configuration file.	From Cisco Unified Operating System Admini make sure that the phone load file is on the TFT and that the entry in the configuration file is co
IP address released	The phone has been configured to release its IP address.	The phone remains idle until it is power cycled reset the DHCP address.
Load ID incorrect	Load ID of the software file is of the wrong type.	Check the load ID assigned to the phone (from UnifiedCommunications Manager, choose **Dev Phone**). Verify that the load ID is entered corre
Load rejected HC	The application that was downloaded is not compatible with the phone's hardware.	Occurs if you were attempting to install a versi software on this phone that did not support har changes on this newer phone. Check the load ID assigned to the phone (from UnifiedCommunications Manager, choose **Dev Phone**). Re-enter the load displayed on the ph
No default router	DHCP or static configuration did not specify a default router.	• If the phone has a static IP address, verify default router has been configured. • If you are using DHCP, the DHCP server provided a default router. Check the DHC configuration.

Message	Description	Possible Explanation and Action
No DNS server IP	A name was specified but DHCP or static IP configuration did not specify a DNS server address.	• If the phone has a static IP address, ve DNS server has been configured. • If you are using DHCP, the DHCP ser provided a DNS server. Check the DH configuration.
TFTP access error	TFTP server is pointing to a directory that does not exist.	• If you are using DHCP, verify that the is pointing to the correct TFTP server. • If you are using static IP addresses, che server configuration.
TFTP error	The phone does not recognize an error code provided by the TFTP server.	Contact the Cisco TAC.
TFTP file not found	The requested load file (.bin) was not found in the TFTPPath directory.	Check the load ID assigned to the phone (fi UnifiedCommunications Manager, choose **Phone**). Verify that the TFTPPath directory .bin file with this load ID as the name.
TFTP timeout	TFTP server did not respond.	• Network is busy. The errors should res themselves when the network load red • No network connectivity between the and the phone. Verify the network con • TFTP server is down. Check the TFTI configuration.
Timed Out	Supplicant attempted 802.1X transaction but timed out to due the absence of an authenticator.	Authentication typically times out if 802.1X configured on the switch.
Version error	The name of the phone load file is incorrect.	Make sure that the phone load file has the c
XmlDefault.cnf.xml, or .cnf.xml corresponding to the phone device name	Name of the configuration file.	None. This is an informational message ind name of the configuration file for the phon

Display Network Statistics Screen

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

Procedure

Step 1 Press **Applications**.

Step 2 Select **Admin Settings**.

Step 3 Select **Status**.

Step 4 Select **Network Statistics**. Network Statistics Fields, on page 72 describes the information that appears in this screen.

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

Network Statistics Fields

The following table lists the Network Statistics Message information.

Table 12: Network Statistics Message Information for the Cisco Unified SIP Phone 3905

Item	Description
Rx Frames	Number of packets received by the phone
Tx Frames	Number of packets sent by the phone
Rx Broadcasts	Number of broadcast packets received by the phone
Restart Cause	Cause of the last reset of the phone - One of these values: • Hardware Reset (Power-on reset) • Software Reset (memory controller also reset) • Software Reset (memory controller not reset) • Watchdog Reset • Unknown
Port 1	Link state and connection of the PC port (for example, **`Auto 100 Mb Full-Duplex`** means that the PC port is in a link-up state and has auto-negotiated a full-duplex, 100-Mbps connection)
Port 2	Link state and connection of the Network port

Item	Description
IPv4	Information on the DHCP status. This includes the following states: • CDP BOUND • CDP INIT • DHCP BOUND • DHCP DISABLED • DHCP INIT • DHCP INVALID • DHCP REBINDING • DHCP REBOOT • DHCP RENEWING • DHCP REQUESTING • DHCP RESYNC • DHCP UNRECOGNIZED • DHCP WAITING COLDBOOT TIMEOUT • SET DHCP COLDBOOT • SET DHCP DISABLED • DISABLED DUPLICATE IP • SET DHCP FAST

Display Call Statistics Window

You can access the Call Statistics screen on the phone to display counters, statistics, and voice-quality metrics of the most recent call.

Note You can also remotely view the call statistics information by using a web browser to access the Streaming Statistics web page. This web page contains additional RTCP statistics not available on the phone. For more information about remote monitoring, see Cisco IP Phone Web Page, on page 75.

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 latest voice stream, perform these steps:

Procedure

Step 1 Press **Applications**.

Step 2 Select **Admin Settings**.

Step 3 Select **Status**.

Step 4 Select **Call Statistics**.

Call Statistics Fields, on page 74 describes the information that appears in this window.

Step 5 To exit the Call Statistics window, press **Back** .

Call Statistics Fields

The following table contains the fields in the Call Statistics screen.

Table 13: Call Statistics Items for the Cisco Unified SIP Phone 3905

Item	Description
Rcvr Codec	Type of voice stream received (RTP streaming audio from codec): G.729, G.711 u-law, G.711 A-law.
Sender Codec	Type of voice stream transmitted (RTP streaming audio from codec): G.729, G.711 u-law, G.711 A-law.
Avg Jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network) observed since the receiving voice stream was opened.
Max Jitter	Maximum jitter observed since the receiving voice stream was opened.
Voice Quality Metrics	
MOS LQK	Objective estimate of the Mean Opinion Score (MOS) for Listening Quality (LQK) that ranks audio quality from 5 (excellent) to 1 (bad). This score is based on audible-concealment events due to a frame loss in the preceding 8 seconds of the voice stream. **Note** The MOS LQK score can vary based on the type of codec that the CiscoUnifiedIPPhone uses.
Avg MOS LQK	Average MOS LQK score for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score from the start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score from the start of the voice stream. The following codecs provide the corresponding maximum MOS LQK scores under normal conditions with no frame loss: • G.711: 4.5 • G729A/AB: 3.7
MOS LQK Version	Version of the Cisco-proprietary algorithm used to calculate the MOS LQK scores.
Latency	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.

Cisco IP Phone Web Page

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

- Device information: Displays device settings and related information for the phone.
- Network setup information: Displays network setup information and information about other phone settings.
- Network statistics: Displays hyperlinks that provide information about network traffic.
- Device logs: Displays hyperlinks that provide information that you can use for troubleshooting.
- Streaming statistic: Includes the Audio and Video statistics, Stream 1, Stream 2, Stream 3, Stream 4, Stream 5 and Stream 6 hyperlinks, which display a variety of streaming statistics.

This section describes the information that you can obtain from the phone 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.

Related Topics

Display Model Information Window, on page 67

Access Web Page for Phone

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

Note If you cannot access the web page, it may be disabled. See Control Phone Web Page Access, on page 62 for more information.

Procedure

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

- Search for the phone in Cisco Unified Communications Manager by choosing **Device** > **Phone**. Phones registered with Cisco Unified Communications Manager display the IP address on the **Find and List Phones** window and at the top of the **Phone Configuration** window.
- On the Cisco Unified IP Phone, press **Applications**, choose **Network** > **IPv4**, and then scroll to the IP Address option.

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

http://*IP_address*

Device Information

The Device Information area on a phone web page displays device settings and related information for the phone. The following table describes these items.

To display the Device Information area, access the web page for the phone as described in Access Web Page for Phone, on page 75, and click the **Device Information** hyperlink.

Table 14: Device Information Area Items

Item	Description
MAC Address	Media Access Control (MAC) address of the phone
Host Name	Unique, fixed name that is automatically assigned to the phone based on its MAC address
Phone DN	Directory number assigned to the phone
App Load ID	Identifier of the firmware running on the phone
Boot Load ID	Identifier of the factory-installed load running on the phone
Hardware Revision	Revision value of the phone hardware
Serial Number	Unique serial number of the phone
Model Number	Model number of the phone
Message Waiting	Indicates if there is a voice message waiting on the primary line for this phone
UDI	Displays the following Cisco Unique Device Identifier (UDI) information about the phone: • Device Type: Indicates hardware type. For example, phone displays for all phone model • Device Description: Displays the name of the phone associated with the indicated mode • Product Identifier: Specifies the phone model • Version Identifier: Represents the hardware version of the phone • Serial Number: Displays the unique serial number of the phone
Time	Time obtained from the Date/Time Group in CiscoUnified Communications Manager to whi phone belongs
Time Zone	Time zone obtained from the Date/Time Group in CiscoUnified Communications Manager t the phone belongs
Date	Date obtained from the Date/Time Group in CiscoUnified Communications Manager to whic phone belongs

Network Setup Page

The Network Setup page on a phone web page displays network setup information and information about other phone settings. The following table describes these items.

You can view and set many of these items from the Network Setup Menu and the Phone Information Menu on the CiscoUnified IP Phone. For more information, see Cisco Unified SIP Phone Installation, on page 15

To display the Network Setup area, access the web page for the phone as described in the Access Web Page for Phone, on page 75, and click the Network Configuration hyperlink.

Table 15: Network Setup Area items

Item	Description
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which t obtains its IP address.
MAC Address	Media Access Control (MAC) address of the phone.
Host Name	Host name that the DHCP server assigned to the phone.
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.
IP Address	Internet Protocol (IP) address of the phone.
Subnet Mask	Subnet mask used by the phone.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone.
TFTP Server 2	Backup Trivial File Transfer Protocol (TFTP) server used by the phone.
Default Router 1	Default router used by the phone.
DNS Server 1–5	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup D (DNS Server 2 - 5) used by the phone.
Operational VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switc the phone is a member.
Admin VLAN ID	Auxiliary VLAN in which the phone is a member.
CallManager 1–5	Host names or IP addresses, in prioritized order, of the CiscoUnifiedCommunication servers with which the phone can register. An item can also show the IP address of an that is capable of providing limited CiscoUnifiedCommunications Manager function a router is available. For an available server, an item will show the CiscoUnifiedCommunications Manag address and one of the following states: • Active: CiscoUnifiedCommunications Manager server from which the phone is receiving call-processing services. • Standby: CiscoUnifiedCommunications Manager server to which the phone sw current server becomes unavailable. • Blank: No current connection to this CiscoUnifiedCommunications Manager se An item may also include the Survivable Remote Site Telephony (SRST) designation identifies an SRST router capable of providing CiscoUnifiedCommunications Manager with a limited feature set. This router assumes control of call processing if all other CiscoUnifiedCommunications Manager servers become unreachable. The SRST CiscoUnifiedCommunications Manager always appears last in the list of servers, even You configure the SRST router address in the Device Pool section in CiscoUnifiedCom Manager Configuration window.

Item	Description
DHCP Enabled	Indicates if DHCP is being used by the phone.
DHCP Address Released	Indicates the setting of the DHCP Address Released option on the phone's Network Conf menu.
Alternate TFTP	Indicates if the phone is using an alternative TFTP server.
SW Port Setup Auto Negotiate	Indicates if switch port is set to auto negotiate.
PC Port Setup Auto Negotiate	Indicates if PC port is set to auto negotiate.
User Locale	User locale associated with the phone user. Identifies a set of detailed information to supp including language, font, date and time formatting, and alphanumeric keyboard text info
Network Locale	Network locale associated with the phone user. Identifies a set of detailed information to the phone in a specific location, including definitions of the tones and cadences used by t
User Locale Version	Version of the user locale loaded on the phone.
Network Locale Version	Version of the network locale loaded on the phone.
PC Port Disabled	Indicates if the PC port on the phone is enabled or disabled.
Speaker Enabled	Indicates if the speakerphone is enabled on the phone.
GARP Enabled	Indicates if the phone learns MAC addresses from Gratuitous ARP responses.
Voice VLAN Enabled	Indicates if the phone allows a device attached to the PC port to access the Voice VLAN
DSCP for Call Control	DSCP IP classification for call control signaling.
DSCP for Configuration	DSCP IP classification for any phone configuration transfer.
DSCP for Services	DSCP IP classification for phone-based services.
Web Access Enabled	Indicates if web access is enabled (Yes) or disabled (No) for the phone.
Span to PC Port	Indicates if the phone forwards packets transmitted and received on the network port to t port.
PC VLAN	VLAN used to identify and remove 802.1P/Q tags from packets sent to the PC.
CDP: PC Port	Indicates if CDP is supported on the PC port (default is enabled). Enable CDP on the PC port when Cisco VT Advantage/Unified Video Advantage (CVT connected to the PC port. CVTA does not work without CDP interaction with the phone When CDP is disabled in Cisco Unified Communications Manager, a warning is displayed, i that disabling CDP on the PC port prevents CVTA from working. The current PC and switch port CDP values are shown on the Settings menu.

Item	Description
CDP: SW Port	Indicates if CDP is supported on the switch port (default is enabled). Enable CDP on the switch port for VLAN assignment for the phone, power negotiat management, and 802.1x security. Enable CDP on the switch port when the phone is connected to a Cisco switch. When CDP is disabled in Cisco Unified Communications Manager, a warning is present that CDP should be disabled on the switch port only if the phone is connected to a non- The current PC and switch port CDP values are shown on the Settings menu.

Network Statistics

The following table lists the Network Statistics information.

Table 16: Network Statistics information

Item	Description
Rx Frames	Number of packets received by the phone
Tx Frames	Number of packets sent by the phone
Rx Broadcasts	Number of broadcast packets received by the phone
Restart Cause	Cause of the last reset of the phone - One of these values: • Hardware Reset (Power-on reset) • Software Reset (memory controller also reset) • Software Reset (memory controller not reset) • Watchdog Reset • Unknown
Port 1	Link state and connection of the Network port
Port 2	Link state and connection of the PC port (for example, **`Auto 100 Mb Full-Duplex`** means that the PC port is in a link-up state and has auto-negotiated a full-duplex, 100-Mbps connection)

Item	Description
IPv4	Information on the DHCP status. This includes the following states: • CDP BOUND • CDP INIT • DHCP BOUND • DHCP DISABLED • DHCP INIT • DHCP INVALID • DHCP REBINDING • DHCP REBOOT • DHCP RENEWING • DHCP REQUESTING • DHCP RESYNC • DHCP UNRECOGNIZED • DHCP WAITING COLDBOOT TIMEOUT • SET DHCP COLDBOOT • SET DHCP DISABLED • DISABLED DUPLICATE IP • SET DHCP FAST

Ethernet Information Web Page

The following table describes the contents of the Ethernet Information web page.

Table 17: Ethernet Information Items

Item	Description
Tx Frames	Total number of packets that the phone transmits.
Tx broadcast	Total number of broadcast packets that the phone transmits.
Tx multicast	Total number of multicast packets that the phone transmits.
Tx unicast	Total number of unicast packets that the phone transmits.
Rx Frames	Total number of packets received by the phone.
Rx broadcast	Total number of broadcast packets that the phone receives..
Rx multicast	Total number of multicast packets that the phone receives.
Rx unicast	Total number of unicast packets that the phone receives.
Rx PacketNoDes	Total number of shed packets that the no Direct Memory Access (DMA) descriptor causes.

Network Information Fields

The following table describes the information in the Network Area web page.

Table 18: Network Items on the Cisco Unified SIP Phone 3905

Item	Description
Tx Frames	Total number of packets transmitted by the phone
Tx broadcast	Total number of broadcast packets transmitted by the phone
Tx unicast	Total number of unicast packets transmitted by the phone
Rx Frames	Total number of packets received by the phone
Rx broadcast	Total number of broadcast packets received by the phone
Rx unicast	Total number of unicast packets received by the phone
Neighbor Device ID	Identifier of a device connected to this port discovered by CDP protocol or LLDP
Neighbor IP Address	IP address of the neighbor device discovered by CDP protocol
Neighbor Port	Neighbor device port to which the phone is connected discovered by CDP protoc
LLDP AgeoutsTotal	Total number of LLDP frames that have been time out in cache
LLDP FramesDiscardedTotal	Total number of LLDP frames that are discarded when any of the mandatory TLV or out of order or contains out of range string length
LLDP FramesInErrorsTotal	Total number of LLDP frames that received with one or more detectable errors
LLDP FramesInTotal	Total number of LLDP frames received on the phone
LLDP TLVDiscardedTotal	Total number of LLDP TLVs that are discarded
LLDP TLVUnrecognizedTotal	Total number of LLDP TLVs that are not recognized on the phone
Restart Cause	Reason for the last restart
Port 1-2	Speed and duplex information
IPv4	IPv4 Address
IPv6	IPv6 Address

Device Logs

The following device logs hyperlinks on a phone web page provide information you can use to help monitor and troubleshoot the phone.

- Console Logs: Includes hyperlinks to individual log files. The console log files include debug and error messages received on the phone.

- Core Dumps: Includes hyperlinks to individual dump files. The core dump files include data from a phone crash.
- Status Messages: Displays up to the 30 most recent status messages that the phone has generated since it was last powered up. You can also see this information from the Status Messages screen on the Web page of the phone. The following table describes the status messages that may be displayed.
- Debug Display: Displays debug messages that might be useful to the Cisco Technical Assistance Center (TAC) if you require assistance with troubleshooting.

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

Table 19: Status Messages

Message	Description	Possible explanation and action
CFG file not found	The name-based and default configuration file was not found on the TFTP Server.	The configuration file for a phone is created w phone is added to the Cisco UnifiedCommunic Manager database. If the phone has not been ad Cisco UnifiedCommunications Manager datab TFTP server generates a `CFG File Not Fo` response. • Phone is not registered with Cisco Unifie Communications Manager. You must manually add the phone to Cisc UnifiedCommunications Manager if you allowing phones to autoregister. See Phone Methods, on page 35 for details. • If you are using DHCP, verify that the DH is pointing to the correct TFTP server. • If you are using static IP addresses, check server configuration.
CFG TFTP Size Error	The configuration file is too large for the file system on the phone.	Power cycle the phone.
Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firmware and p the TFTPPath directory. You should only copy this directory when the TFTP server software i down, otherwise the files may be corrupted.
DHCP timeout	DHCP server did not respond.	• Network is busy. The errors should resolv themselves when the network load reduce • No network connectivity between the DH and the phone. Verify the network connec • DHCP server is down. Check the DHCP s configuration. • Errors persist. Consider assigning a static IP

Message	Description	Possible explanation and action
DNS timeout	DNS server did not respond.	• Network is busy. The errors should res themselves when the network load red • No network connectivity between the and the phone. Verify the network con • DNS server is down. Check the DNS configuration.
DNS unknown host	DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	• Verify that the host names of the TFTI Cisco UnifiedCommunications Manag configured properly in DNS. • Consider using IP addresses rather thar
Duplicate IP	Another device is using the IP address assigned to the phone.	• If the phone has a static IP address, ve have not assigned a duplicate IP addre • If you are using DHCP, check the DH configuration.
File not found	The phone cannot locate, on the TFTP server, the phone load file that is specified in the phone configuration file.	From Cisco Unified Operating System Adr make sure that the phone load file is on the and that the entry in the configuration file i
IP address released	The phone has been configured to release its IP address.	The phone remains idle until it is power cy reset the DHCP address.
Load ID incorrect	Load ID of the software file is of the wrong type.	Check the load ID assigned to the phone (fi UnifiedCommunications Manager, choose **Phone**). Verify that the load ID is entered c
Load rejected HC	The application that was downloaded is not compatible with the phone's hardware.	Occurs if you were attempting to install a v software on this phone that did not support changes on this newer phone. Check the load ID assigned to the phone (fi UnifiedCommunications Manager, choose **Phone**). Re-enter the load displayed on the
No default router	DHCP or static configuration did not specify a default router.	• If the phone has a static IP address, ve default router has been configured. • If you are using DHCP, the DHCP ser provided a default router. Check the D configuration.
No DNS server IP	A name was specified but DHCP or static IP configuration did not specify a DNS server address.	• If the phone has a static IP address, ve DNS server has been configured. • If you are using DHCP, the DHCP ser provided a DNS server. Check the DH configuration.

Message	Description	Possible explanation and action
TFTP access error	TFTP server is pointing to a directory that does not exist.	• If you are using DHCP, verify that the DH is pointing to the correct TFTP server. • If you are using static IP addresses, check server configuration.
TFTP error	The phone does not recognize an error code provided by the TFTP server.	Contact the Cisco TAC.
TFTP file not found	The requested load file (.bin) was not found in the TFTPPath directory.	Check the load ID assigned to the phone (from UnifiedCommunications Manager, choose **Dev Phone**). Verify that the TFTPPath directory co .bin file with this load ID as the name.
TFTP timeout	TFTP server did not respond.	• Network is busy. The errors should resolv themselves when the network load reduce • No network connectivity between the TF and the phone. Verify the network connec • TFTP server is down. Check the TFTP se configuration.
Timed Out	Supplicant attempted 802.1X transaction but timed out to due the absence of an authenticator.	Authentication typically times out if 802.1X is configured on the switch.
Version error	The name of the phone load file is incorrect.	Make sure that the phone load file has the corr
XmlDefault.cnf.xml, or .cnf.xml corresponding to the phone device name	Name of the configuration file.	None. This is an informational message indica name of the configuration file for the phone.

Streaming Statistics

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

The streaming statistics areas on a phone web page provide information about the streams. Cisco Unified SIP Phone 3905 use only Stream 1.

To display a Streaming Statistics area, access the web page for the phone as described in Access Web Page for Phone, on page 75 and click the Stream 1 hyperlink.

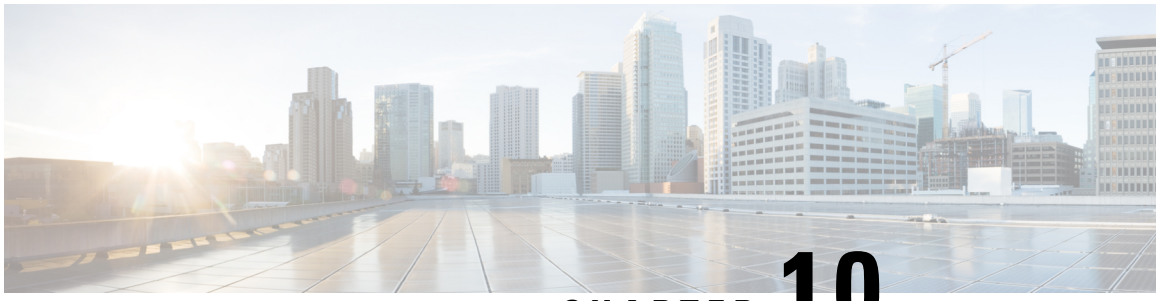
Table 20: Streaming Statistics Area Items

Item	Description
Remote Address	IP address and UDP port of the destination of the stream.
Local Address	IP address and UDP port of the phone.
Start Time	Internal time stamp indicating when Cisco Unified Communications Manager requeste the phone start transmitting packets.

Item	Description
Stream Status	Indication of whether streaming is active or not.
Host Name	Unique, fixed name that is automatically assigned to the phone based on its MAC a
Sender Packets	Total number of RTP data packets transmitted by the phone since starting this conne value is 0 if the connection is set to receive only mode.
Sender Octets	Total number of payload octets transmitted in RTP data packets by the phone since s connection. The value is 0 if the connection is set to receive only mode.
Sender Codec	Type of audio encoding used for the transmitted stream.
Sender Reports Sent	Number of times the RTCP Sender Report have been sent. When the RTCP Control Protocol is disabled, no data generates for this field and thu as 0.
Sender Report Time Sent	Internal time stamp indication when the last RTCP Sender Report was sent. When the RTCP Control Protocol is disabled, no data generates for this field and thu as 0.
Rcvr Lost Packets	Total number of RTP data packets that have been lost since starting receiving data c connection. Defined as the number of expected packets less the number of packets a received, where the number of received packets includes any that are late or duplica value displays as 0 if the connection was set to send-only mode.
Avg Jitter	Estimate of mean deviation of the RTP data packet inter-arrival time, measured in mi The value displays as 0 if the connection was set to send-only mode.
Rcvr Codec	Type of audio encoding used for the received stream.
Rcvr Reports Sent	Number of times the RTCP Receiver Reports have been sent. When the RTCP Control Protocol is disabled, no data generates for this field and thu as 0.
Rcvr Report Time Sent	Internal time stamp indication when a RTCP Receiver Report was sent. When the RTCP Control Protocol is disabled, no data generates for this field and thu as 0.
Rcvr Packets	Total number of RTP data packets received by the phone since starting receiving da connection. Includes packets received from different sources if this is a multicast call. displays as 0 if the connection was set to send-only mode.
Rcvr Octets	Total number of payload octets received in RTP data packets by the device since sta reception on the connection. Includes packets received from different sources if this is call. The value displays as 0 if the connection was set to send-only mode.

Item	Description
MOS LQK	Objective estimate of the Mean Opinion Score (MOS) for Listening Quality (LQK) tha audio quality from 5 (excellent) to 1 (bad). This score is based on audible-concealment due to a frame loss in the preceding 8 seconds of the voice stream. **Note** The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Ph uses.
Avg MOS LQK	Average MOS LQK score for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score from the start of the voice stream.
Max MOS LQK	Baseline or highest MOS LQK score from the start of the voice stream. The following codecs provide the corresponding maximum MOS LQK scores under nc conditions with no frame loss: • G.711: 4.5 • G729A/AB: 3.7
MOS LQK Version	Version of the Cisco-proprietary algorithm used to calculate the MOS LQK scores.
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames receive start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active s If using voice activity detection (VAD), a longer interval might be required to accumul 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 (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than 5 percent concealment events (lost frames) fro start of the voice stream.
Latency	Estimate of the network latency, expressed in milliseconds. Represents a running avera the round-trip delay, measured when RTCP receiver report blocks are received. When the RTCP Control Protocol is disabled, no data generates for this field and thus d as 0.
Max Jitter	Maximum value of instantaneous jitter, in milliseconds.
Sender Size	RTP packet size, in milliseconds, for the transmitted stream.
Sender Reports Received	Number of times RTCP Sender Reports have been received. When the RTCP Control Protocol is disabled, no data generates for this field and thus d as 0.

Item	Description
Sender Report Time Received	Last time at which an RTCP Sender Report was received. When the RTCP Control Protocol is disabled, no data generates for this field and thu as 0.
Rcvr Size	RTP packet size, in milliseconds, for the received stream.
Rcvr Discarded	RTP packets received from network but discarded from jitter buffers.
Rcvr Reports Received	Number of times RTCP Receiver Reports have been received. When the RTCP Control Protocol is disabled, no data generates for this field and thu as 0.
Rcvr Report Time Received	Last time at which an RTCP Receiver Report was received. When the RTCP Control Protocol is disabled, no data generates for this field and thu as 0.



CHAPTER 10

Troubleshooting

Troubleshooting Overview

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

If you need additional assistance to resolve an issue, see Documentation, Support, and Security Guidelines, on page xi.

This chapter includes these topics:

Startup Problems

After you install a phone into your network and add it to Cisco Unified Communications Manager, the phone should start up as described in the related topic below.

If the phone does not start up properly, see the following sections for troubleshooting information.

Related Topics

Verify Phone Startup, on page 27

Cisco IP Phone Does Not Go Through the Normal Startup Process

Problem

When you connect a Cisco IP Phone to the network port, the phone does not go through the normal startup process as described in the related topic and the phone screen does not display information.

Cause

If the phone does not go through the startup process, the cause may be faulty cables, bad connections, network outages, lack of power, or the phone may not be functional.

Solution

To determine whether the phone is functional, use the following suggestions to eliminate other potential problems.

- Verify that the network port is functional:
  - Exchange the Ethernet cables with cables that you know are functional.
  - Disconnect a functioning Cisco IP Phone from another port and connect it to this network port to verify that the port is active.
  - Connect the Cisco IP Phone that does not start up to a different network port that is known to be good.
  - Connect the Cisco IP Phone that does not start up directly to the port on the switch, eliminating the patch panel connection in the office.
- Verify that the phone is receiving power:
  - If you are using external power, verify that the electrical outlet is functional.
  - If you are using in-line power, use the external power supply instead.
  - If you are using the external power supply, switch with a unit that you know to be functional.
- If the phone still does not start up properly, power up the phone from the backup software image.
- If the phone still does not start up properly, perform a factory reset of the phone.
- After you attempt these solutions, if the phone screen on the Cisco IP Phone does not display any characters after at least five minutes, contact a Cisco technical support representative for additional assistance.

Related Topics

Verify Phone Startup, on page 27

Cisco IP Phone Does Not Register with Cisco Unified Communications Manager

If the phone proceeds past the first stage of the startup process (LED buttons flashing on and off) but continues to cycle through the messages that displays on the phone screen, the phone is not starting up properly. The phone cannot successfully start up unless it connects to the Ethernet network and it registers with a Cisco Unified Communications Manager server.

In addition, problems with security may prevent the phone from starting up properly. See Troubleshooting Procedures, on page 100 for more information.

Phone Displays Error Messages

Problem

Status messages display errors during startup.

Solution

While the phone cycles through the startup process, you can access status messages that might provide you with information about the cause of a problem. See the "Display Status Messages Window" section for instructions about accessing status messages and for a list of potential errors, their explanations, and their solutions.

Related Topics

Display Status Messages Window, on page 68

Phone Cannot Connect to TFTP Server or to Cisco Unified Communications Manager

Problem

If the network is down between the phone and either the TFTP server or Cisco Unified Communications Manager, the phone cannot start up properly.

Solution

Ensure that the network is currently running.

Phone Cannot Connect to TFTP Server

Problem

The TFTP server settings may not be correct.

Solution

Check the TFTP settings.

Related Topics

Check TFTP Settings, on page 100

Phone Cannot Connect to Server

Problem

The IP addressing and routing fields may not be configured correctly.

Solution

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

Related Topics

Check DHCP Settings, on page 100

Cisco Unified Communications Manager and TFTP Services Are Not Running

Problem

If the Cisco Unified Communications Manager or TFTP services are not running, phones may not be able to start up properly. In such a situation, it is likely that you are experiencing a systemwide failure, and other phones and devices are unable to start up properly.

Solution

If the Cisco Unified Communications Manager service is not running, all devices on the network that rely on it to make phone calls are affected. If the TFTP service is not running, many devices cannot start up successfully. For more information, see Start Service, on page 101.

Configuration File Corruption

Problem

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

Solution

Create a new phone configuration file.

Cisco Unified Communications Manager Phone Registration

Problem

The phone is not registered with the Cisco Unified Communications Manager

Solution

A Cisco IP Phone can register with a Cisco Unified Communications Manager server only if the phone is added to the server or if autoregistration is enabled. Review the information and procedures in Phone Addition Methods, on page 35 to ensure that the phone is added to the Cisco Unified Communications Manager database.

To verify that the phone is in the Cisco Unified Communications Manager database, choose **Device** > **Phone** from Cisco Unified Communications Manager Administration. Click **Find** to search for the phone based on the MAC Address. For information about determining a MAC address, see Determine the Phone MAC Address, on page 34.

If the phone is already in the Cisco Unified Communications Manager database, the configuration file may be damaged. See Configuration File Corruption, on page 92 for assistance.

Cisco IP Phone Cannot Obtain IP Address

Problem

If a phone cannot obtain an IP address when it starts up, the phone may not be on the same network or VLAN as the DHCP server, or the switch port to which the phone connects may be disabled.

Solution

Ensure that the network or VLAN to which the phone connects has access to the DHCP server, and ensure that the switch port is enabled.

Phone Reset Problems

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

Typically, a phone resets if it has problems in connecting to the network or to Cisco Unified Communications Manager.

Phone Cannot Connect to LAN

Problem

The physical connection to the LAN may be broken.

Solution

Verify that the Ethernet connection to which the Cisco IP Phone connects is up. For example, check whether the particular port or switch to which the phone connects is down and that the switch is not rebooting. Also ensure that no cable breaks exist.

Phone Resets Due to Intermittent Network Outages

Problem

Your network may be experiencing intermittent outages.

Solution

Intermittent network outages affect data and voice traffic differently. Your network might be experiencing intermittent outages without detection. If so, data traffic can resend lost packets and verify that packets are received and transmitted. However, voice traffic cannot recapture lost packets. Rather than retransmitting a lost network connection, the phone resets and attempts to reconnect to the network. Contact the system administrator for information on known problems in the voice network.

Phone Resets Due to DHCP Setting Errors

Problem

The DHCP settings may be incorrect.

Solution

Verify that you have properly configured the phone to use DHCP. Verify that the DHCP server is set up properly. Verify the DHCP lease duration. We recommend that you set the lease duration to 8 days.

Related Topics

Check DHCP Settings, on page 100

Phone Resets Due to Incorrect Static IP Address

Problem

The static IP address assigned to the phone may be incorrect.

Solution

If the phone is assigned a static IP address, verify that you have entered the correct settings.

Phone Resets During Heavy Network Usage

Problem

If the phone appears to reset during heavy network usage, it is likely that you do not have a voice VLAN configured.

Solution

Isolating the phones on a separate auxiliary VLAN increases the quality of the voice traffic.

Phone Resets Due to Intentional Reset

Problem

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

Solution

You can check if a Cisco IP Phone received a command from Cisco Unified Communications Manager to reset by pressing **Applications** on the phone and choosing **Admin Settings** > **Status** > **Network Statistics**.

- If the Restart Cause field displays `Reset-Reset`, the phone receives a Reset/Reset from Cisco Unified Communications Manager Administration.

- If the Restart Cause field displays `Reset-Restart`, the phone closed because it received a Reset/Restart from Cisco Unified Communications Manager Administration.

Phone Resets Due to DNS or Other Connectivity Issues

Problem

The phone reset continues and you suspect DNS or other connectivity issues.

Solution

If the phone continues to reset, eliminate DNS or other connectivity errors by following the procedure in Determine DNS or Connectivity Issues, on page 102.

Phone Does Not Power Up

Problem

The phone does not appear to be powered up.

Solution

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

Cisco IP Phone Security Problems

802.1X Authentication Problems

801.1X authentication problems can be broken into the categories that are described in the following table.

Table 21: 802.1X Authentication Problem Identification

If all the following conditions apply,	See
• Phone cannot obtain a DHCP-assigned IP address. • Phone does not register with Cisco Unified Communications Manager. • Phone status displays `Configuring IP` or `Registering`. • 802.1X Authentication Status displays `Held`. • Status menu 802.1X status displays `Failed`.	802.1X Enabled on Phone but Phone Does Not Authenticate, on page 96

If all the following conditions apply,	See
• Phone cannot obtain a DHCP-assigned IP address. • Phone does not register with Cisco Unified Communications Manager. • Phone status displays `Configuring IP` or `Registering`. • 802.1X Authentication Status displays `Disabled`. • Status menu displays that the DHCP status has timed out.	802.1X Not Enabled, on page 96
• Phone cannot obtain a DHCP-assigned IP address. • Phone does not register with Cisco Unified Communications Manager. • Phone status display as `Configuring IP` or `Registering`. • You are unable to access phone menus to verify 802.1X status.	Factory Reset of Phone Has Deleted 802.1X Shared Secret, on page 97

802.1X Enabled on Phone but Phone Does Not Authenticate

Problem

The phone cannot authenticate.

Cause

These errors typically indicate that 802.1X authentication is enabled on the phone, but the phone is unable to authenticate.

Solution

To resolve this problem, check the 802.1X and shared secret configuration. See Identify 802.1X Authentication Problems, on page 102.

802.1X Not Enabled

Problem

The phone does not have 802.1X configured.

Cause

These errors typically indicate that 802.1X authentication is not enabled on the phone.

Solution

If 802.1X is not enabled on the phone, see 802.1X Authentication section.

Factory Reset of Phone Has Deleted 802.1X Shared Secret

Problem

After a reset, the phone does not authenticate.

Cause

These errors typically indicate that the phone has completed a factory reset while 802.1X was enabled. A factory reset deletes the shared secret, which is required for 802.1X authentication and network access.

Solution

To resolve this situation, temporarily move the phone to a network environment that is not using 802.1X authentication. After the phone starts up normally, access the 802.1X configuration menus to enable device authentication and to reenter the shared secret. See 802.1X Authentication section for details.

Related Topics

Basic Reset

Audio and Video Problems

The following sections describe how to resolve audio and video problems.

No Speech Path

Problem

One or more people on a call do not hear any audio.

Solution

When at least one person in a call does not receive audio, IP connectivity between phones is not established. Check the configuration of routers and switches to ensure that IP connectivity is properly configured.

Choppy Speech

Problem

A user complains of choppy speech on a call.

Cause

There may be a mismatch in the jitter configuration.

Solution

Check the AvgJtr and the MaxJtr statistics. A large variance between these statistics might indicate a problem with jitter on the network or periodic high rates of network activity.

Poor Audio Quality with Calls that Route Outside Cisco Unified Communications Manager

Problem

Poor quality occurs with tandem audio encoding. Tandem encoding can occur when calls are made between an IP Phone and a digital cellular phone, when a conference bridge is used, or in situations where IP-to-IP calls are partially routed across the PSTN.

Cause

In these cases, use of voice codecs such as G.729 and iLBC may result in poor voice quality.

Solution

Use the G.729 and iLBC codecs only when absolutely necessary.

Phone Display Is Wavy

Problem

The display appears to have rolling lines or a wavy pattern.

Cause

The phone might be interacting with certain types of older fluorescent lights in the building.

Solution

Move the phone away from the lights or replace the lights to resolve the problem.

General Telephone Call Problems

The following sections help troubleshoot general telephone call problems.

Phone Call Cannot Be Established

Problem

A user complains about not being able to make a call.

Cause

The phone does not have a DHCP IP address, is unable to register to Cisco Unified Communications Manager. Phones with an LCD display show the message `Configuring IP` or `Registering`. Phones without an LCD display play the reorder tone (instead of dial tone) in the handset when the user attempts to make a call.

Solution

1. Verify the following:
   a. The Ethernet cable is attached.
   b. The Cisco CallManager service is running on the Cisco Unified Communications Manager server.
   c. Both phones are registered to the same Cisco Unified Communications Manager.
2. Audio server debug and capture logs are enabled for both phones. If needed, enable Java debug.

Phone Does Not Recognize DTMF Digits or Digits Are Delayed

Problem

The user complains that numbers are missed or delayed when the keypad is used.

Cause

Pressing the keys too quickly can result in missed or delayed digits.

Solution

Keys should not be pressed rapidly.

Phone Bandwidth Restrictions

Problem

Users report frequent `Not enough bandwidth` messages on their phones.

Cause

The Cisco Unified Communications Manager does not have adequate bandwidth to place the call or there are policy restrictions.

Solution

For information on changing the Cisco Unified Communications Manager bandwidth, see the documentation for your particular version of Cisco Unified Communications Manager.

Troubleshooting Procedures

These procedures can be used to identify and correct problems.

Check TFTP Settings

Procedure

Step 1 Check the TFTP Server 1 field.

If you have assigned a static IP address to the phone, you must manually enter a setting for the TFTP Server 1 option.

If you are using DHCP, the phone obtains the address for the TFTP server from the DHCP server. Check that the IP address is configured in Option 150.

Step 2 You can also enable the phone to use an alternate TFTP server. Such a setting is particularly useful if the phone recently moved from one location to another.

Step 3 If the local DHCP does not offer the correct TFTP address, enable the phone to use an alternate TFTP server.

This is often necessary in VPN scenarios.

Related Topics

Phone Cannot Connect to TFTP Server, on page 91

Check DHCP Settings

Procedure

Step 1 Check the DHCP server field.

Step 2 Check the IP Address, Subnet Mask, and Default Router fields.

If you assign a static IP address to the phone, you must manually enter settings for these options.

Step 3 If you are using DHCP, check the IP addresses that your DHCP server distributes.

See the *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* document, available at this URL:

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

Related Topics

Phone Cannot Connect to Server, on page 91
Phone Resets Due to DHCP Setting Errors, on page 94

Start Service

A service must be activated before it can be started or stopped.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Cisco Unified Serviceability** from the Navigation drop-down list and click **Go**.

Step 2 Choose **Tools** > **Control Center - Feature Services**.

Step 3 Choose the primary Cisco Unified Communications Manager server from the Server drop-down list.

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

Step 4 If a service has stopped, click the corresponding radio button and then click **Start**.

The Service Status symbol changes from a square to an arrow.

Create a New Phone Configuration File

When you remove a phone from the Cisco Unified Communications Manager database, the configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone directory number or numbers remain in the Cisco Unified Communications Manager database. They are called unassigned DNs and can be used for other devices. If unassigned DNs are not used by other devices, delete these DNs from the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers. For more information, see the documentation for your particular Cisco Unified Communications Manager release.

Changing the buttons on a phone button template, or assigning a different phone button template to a phone, may result in directory numbers that are no longer accessible from the phone. The directory numbers are still assigned to the phone in the Cisco Unified Communications Manager database, but the phone has no button on the phone with which calls can be answered. These directory numbers should be removed from the phone and deleted if necessary.

Procedure

Step 1 From Cisco Unified Communications Manager, choose **Device** > **Phone** and click **Find** to locate the phone that is experiencing problems.

Step 2 Choose **Delete** to remove the phone from the Cisco Unified Communications Manager database.

Note
When you remove a phone from the Cisco Unified Communications Manager database, the configuration file is deleted from the Cisco Unified Communications Manager TFTP server. The phone directory number or numbers remain in the Cisco Unified Communications Manager database. They are called unassigned DNs and can be used for other devices. If unassigned DNs are not used by other devices, delete these DNs from

the Cisco Unified Communications Manager database. You can use the Route Plan Report to view and delete unassigned reference numbers.

Step 3 Add the phone back to the Cisco Unified Communications Manager database.

Step 4 Power cycle the phone.

Related Topics

Phone Addition Methods, on page 35

Determine DNS or Connectivity Issues

Procedure

Step 1 Use the Reset Settings menu to reset phone settings to their default values.

Step 2 Modify DHCP and IP settings:

a) Disable DHCP.

b) Assign static IP values to the phone. Use the same default router setting that other functioning phones use.

c) Assign a TFTP server. Use the same TFTP server that other functioning phones use.

Step 3 On the Cisco Unified Communications Manager server, verify that the local host files have the correct Cisco Unified Communications Manager server name mapped to the correct IP address.

Step 4 From Cisco Unified Communications Manager, choose **System** > **Server** and verify that reference to the server is made by the IP address and not by the DNS name.

Step 5 From Cisco Unified Communications Manager, choose **Device** > **Phone**. Click **Find** to search for this phone. Verify that you have assigned the correct MAC address to this Cisco IP Phone.

Step 6 Power cycle the phone.

Related Topics

Basic Reset

Determine the Phone MAC Address, on page 34

Identify 802.1X Authentication Problems

Procedure

Step 1 Verify that you have properly configured the required components.

Step 2 Confirm that the shared secret is configured on the phone.

- If the shared secret is configured, verify that you have the same shared secret on the authentication server.

- If the shared secret is not configured on the phone, enter it, and ensure that it matches the shared secret on the authentication server.

Verify DNS Settings

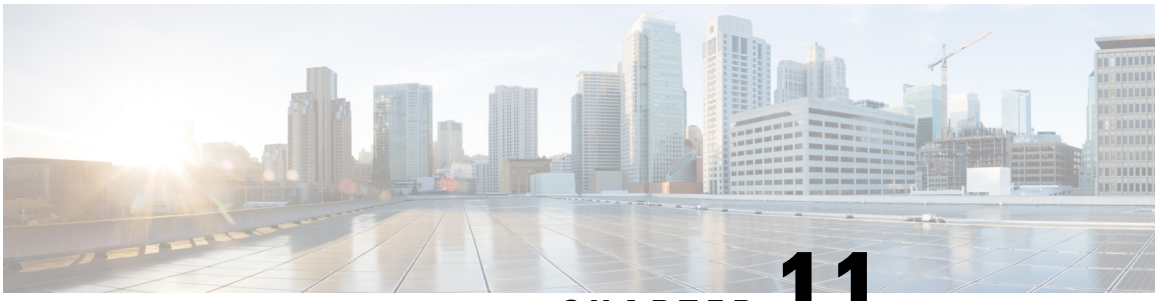
Procedure

Check that the DNS Server 1 field is set correctly.

Additional Troubleshooting Information

If you have additional questions about troubleshooting your phone, go to the following Cisco website and navigate to the desired phone model:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/series.html#Troubleshooting



CHAPTER 11

Maintenance

Basic Reset

Performing a basic reset of a CiscoIP Phone provides a way to recover if the phone experiences an error and provides a way to reset or restore various configuration and security settings.

The following table describes the ways to perform a basic reset. You can reset a phone after the phone has started up. Choose the operation that is appropriate for your situation.

Table 22: Basic Reset Method

Operation	Action	Expla
Restart phone	Press **Services, Applications, or Directories** and then press ****#****.	Reset writte

Reset the Phone to the Factory Settings from the Keypad

You can reset the phone to the factory settings. The reset clears all the phone parameters.

Procedure

	Command or Action	Purpose
Step 1	Remove power from the phone in one of these ways: • Unplug the power adapter. • Unplug the LAN cable.	
Step 2	Press the pound (#) key and plug the phone in.	
Step 3	When prompted, enter the following key sequence:	`123456789*0#`

	Command or Action	Purpose
		The phone resets.

Perform Factory Reset from Phone Menu

To perform a factory reset of a phone,

Procedure

Step 1 Press **Applications**.

Step 2 Choose **Admin Settings** > **Reset All**.

If required, unlock the phone options.

Step 3 Choose **Yes** and press **Select**.

Related Topics

Apply a Phone Password, on page 20

Voice Quality Monitoring

To measure the voice quality of calls that are sent and received within the network, Cisco 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.

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

You can access voice quality metrics from the Cisco IP Phone using the Call Statistics screen or remotely by using Streaming Statistics.

Voice Quality Troubleshooting Tips

When you observe significant and persistent changes to metrics, use the following table for general troubleshooting information.

Table 23: Changes to Voice Quality Metrics

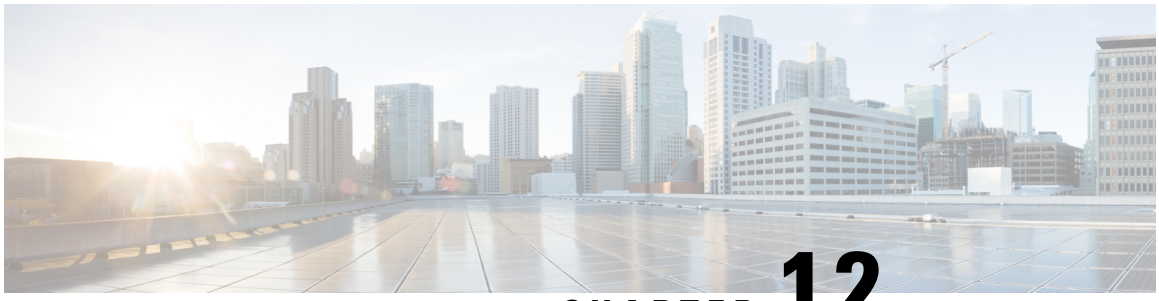
Metric Change	Condition
Conceal Ratio and Conceal Seconds increase significantly	Network impairment from packet loss or high jitter.
Conceal Ratio is near or at zero, but the voice quality is poor.	• Noise or distortion in the audio channel such as echo or audio levels. • Tandem calls that undergo multiple encode/decode such as calls to a cellular network or calling card network. • Acoustic problems coming from a speakerphone, handsfree cellular phone or wireless headset. Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.
MOS LQK scores decrease significantly	Network impairment from packet loss or high jitter levels: • Average MOS LQK decreases may indicate widespread and uniform impairment. • Individual MOS LQK decreases may indicate bursty impairment. Cross-check the conceal ratio and conceal seconds for evidence of packet loss and jitter.
MOS LQK scores increase significantly	• Check to see if the phone is using a different codec than expected (RxType and TxType). • Check to see if the MOS LQK version changed after a firmware upgrade.

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

Cisco IP Phone Cleaning

To clean your Cisco IP Phone, use only a dry soft cloth to gently wipe the phone and the phone screen. Do not apply liquids or powders directly to the phone. As with all non-weatherproof electronics, liquids and powders can damage the components and cause failures.

When the phone is in sleep mode, the screen is blank and the Select button is not lit. When the phone is in this condition, you can clean the screen, as long as you know that the phone will remain asleep until after you finish cleaning.



CHAPTER 12

International User Support

Unified Communications Manager Endpoints Locale Installer

By default, Cisco IP Phones are set up for the English (United States) locale. To use the Cisco IP Phones in other locales, you must install the locale-specific version of the Unified Communications Manager Endpoints Locale Installer on every Cisco Unified Communications Manager server in the cluster. The Locale Installer installs the latest translated text for the phone user interface and country-specific phone tones on your system so that they are available for the Cisco IP Phones.

To access the Locale Installer required for a release, access the Software Download page, navigate to your phone model, and select the Unified Communications Manager Endpoints Locale Installer link.

For more information, see the documentation for your particular Cisco Unified Communications Manager release.

Note The latest Locale Installer may not be immediately available; continue to check the website for updates.

International Call Logging Support

If your phone system is configured for international call logging (calling party normalization), the call logs, redial, or call directory entries may display a plus (+) symbol to represent the international escape code for your location. Depending on the configuration for your phone system, the + may be replaced with the correct international dialing code, or you may need to edit the number before dialing to manually replace the + with the international escape code for your location. In addition, while the call log or directory entry may display the full international number for the received call, the phone display may show the shortened local version of the number, without international or country codes.

Language Limitation

There is no localized Keyboard Alphanumeric Text Entry (KATE) support for the following Asian locales:

- Chinese (China)
- Chinese (Hong Kong)
- Chinese (Taiwan)
- Japanese (Japan)
- Korean (Korea Republic)

The default English (United States) KATE is presented to the user instead.

For example, the phone screen will show text in Korean, but the **2** key on the keypad will display **a b c 2 A B C**.