Cisco IP Conference Phone 7832 Multiplatform Phones Administration Guide

First Published: 2017-08-14

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

CONTENTS

PART I

About the Cisco IP Conference Phone

CHAPTER 1

Technical Details

Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the conference phone.

Table 1: Physical and Operating Specifications

Specification	Value or Range
Operating temperature	32° to 104°F (0° to 40°C)
Operating relative humidity	10% to 90% (noncondensing)
Storage temperature	14° to 140°F (–10° to 60°C)
Height	8.9 in. (226 mm)
Width	8.9 in. (226 mm)
Depth	2.14 in. (54.4 mm)
Weight	2.0 lb. (0.907 kg)

Specification	Value or Range
Power	• IEEE PoE Class 2. The phone is compatible with both IEEE 802.3af and 802.3at switch blades and supports both Cisco Discovery Protocol and Link Layer Discovery Protocol - Power over Ethernet (LLDP-PoE) • If the connected LAN switches don't support PoE, an additional PoE power injector will be needed to convert AC wall power to provide PoE
Cables	Category 3/5/5e/6 for 10-Mpbs cables with 4 pairs Category 5/5e/6 for 100-Mbps cables with 4 pairs **Note** Cables have 4 pairs of wires for a total of 8 conductors.
Distance Requirements	The Ethernet Specification assumes that the maximum cable length between each conference phone and the switch is 100 meters (330 feet).

For more information, see the *Cisco IP Conference Phone 7832 Data Sheet*: http://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-7800-series/datasheet-listing.html

Cable Specifications

- RJ-45 jack for the LAN 10/100BaseT connection.

Phone Power Requirements

The Cisco IP Conference Phone can use these power sources:

- Power over Ethernet (PoE)
- Cisco IP Conference Phone 7832 PoE Midspan Cable and Cisco Power Cube 3
- Cisco IP Phone Power Injector

Note The midspan cable is not currently available.

Table 2: Guidelines for Cisco IP Conference Phone Power

Power Type	Guidelines
PoE power—Provided by a switch through the Ethernet cable attached to the phone.	To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply. Make sure that the CatOS or IOS version that runs on your switch supports your intended phone deployment. See the documentation for your switch for operating system version information.
External power—Provided through the Cisco IP Conference Phone 7832 PoE Midspan Cable and Cisco Power Cube 3	The midspan cable and power cube provide power to the Ethernet cable. When you install a phone that is powered with the midspan adapter, connect the adapter to power before you connect the Ethernet cable to the phone. When you remove a phone that uses the midspan adapter, disconnect the Ethernet cable from the phone before you remove the power from the adapter.
External power—Provided through the Cisco IP Phone Power Injector	The power injector provides power to the Ethernet cable. When you install a phone that is powered with the power injector, connect the injector to power before you connect the Ethernet cable to the phone. When you remove a phone that uses the injector, disconnect the Ethernet cable from the phone before you remove the power from the injector.

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.

Supported Network Protocols

Cisco IP Conference Phones support several industry-standard and Cisco network protocols that are required for voice communication. The following table provides an overview of the network protocols that the phones support.

Table 3: Supported Network Protocols on the Cisco IP Conference Phone

Network Protocol	Purpose	Usage Notes
Bootstrap Protocol (BootP)	BootP enables a network device, such as the phone, to discover certain startup information, such as its IP address.	—

Network Protocol	Purpose	Usage Notes
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. A device can use CDP to advertise its existence to other devices and receive information about other devices in the network.	The phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect an IP phone into the network and have the phone become operational without the need to manually assign an IP address or to configure additional network parameters.	DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each phone locally. We recommend that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, see the documentation for your particular Cisco Unified Communications Manager release. **Note** If you cannot use option 150, use DHCP option 66.
Hypertext Transfer Protocol (HTTP)	HTTP is the standard protocol for transfer of information and movement of documents across the Internet and the web.	Phones use HTTP for XML services, provisioning, upgrade and for troubleshooting purposes.
Hypertext Transfer Protocol Secure (HTTPS)	Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of servers.	Web applications with both HTTP and HTTPS support have two URLs configured. phones that support HTTPS choose the HTTPS URL. A lock icon is displayed to the user if the connection to the service is via HTTPS.
IEEE 802.1X	The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connection 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 phone implements the IEEE 802.1X standard through support for the following authentication methods: EAP-FAST and EAP-TLS. When 802.1X authentication is enabled on the phone, you should disable the voice VLAN.

Network Protocol	Purpose	Usage Notes
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communicate with IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnets, and gateways identifications are automatically assigned if you are using the phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally. The phones support IPv6 address. For more information, see the documentation for your particular Cisco Unified Communications Manager release.
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.	
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard developed for voice products.	The phone supports LLDP-MED on the SW port to communicate information such as: • Voice VLAN configuration • Device discovery • Power management • Inventory management For more information about LLDP-MED support, see the *LLDP-MED and Cisco Discovery Protocol* white paper at this URL: http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.
Real-Time Control Protocol (RTCP)	RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round trip delay) on RTP streams.	RTCP is enabled by default.

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 designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.
Secure Real-Time Transfer protocol (SRTP)	SRTP is an extension of the Real-Time Protocol (RTP) Audio/Video Profile and ensures the integrity of RTP and Real-Time Control Protocol (RTCP) packets providing authentication, integrity, and encryption of media packets between two endpoints.	Phones use SRTP for media encryption.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	When security is implemented, phones use the TLS protocol when securely registering with the Cisco Unified Communications Manager. For more information, see the documentation for your particular Cisco Unified Communications Manager release.
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the phone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server. If you want a phone to use a TFTP server other than the one specified by the DHCP server, you must manually assign the IP address of the TFTP server by using the Network Setup menu on the phone. For more information, see the documentation for your particular Cisco Unified Communications Manager release.
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	Phones transmit and receive RTP streams, which utilize UDP.

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

Anything that degrades network performance can affect Cisco IP Phone voice and video quality, and in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

- 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 IP Conference Phone Hardware

The Cisco IP Conference Phone 7832

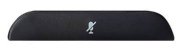
The Cisco IP Conference Phone 7832 enhances people-centric communications, combining superior high-definition (HD) audio performance and 360-degree coverage for all sizes of conference rooms and executive offices. It provides an audiophile sound experience with a full-duplex two-way wideband (G.722) audio hands-free speaker. The Cisco IP Conference Phone 7832 is a simple solution that meets the challenges of the most diverse rooms.

The phone has sensitive microphones with 360-degree coverage. This coverage lets users speak in a normal voice and be heard clearly from up to 7 feet (2.1 m) away. The phone also features technology that resists interference from mobile phones and other wireless devices, assuring delivery of clear communications without distractions.

Cisco IP Phone 7832 Buttons and Hardware

The following figure shows the Cisco IP Conference Phone 7832.

Figure 1: Cisco IP Conference Phone 7832 Buttons and Features

1	**Mute** bar	 Toggle the microphone on or off. When the microphone is muted, the LED bar is lit red.
2	LED bar	Indicates call states: • Green, solid—Active call • Green, flashing—Incoming call • Green, pulsing—Held call • Red, solid—Muted call
3	Softkey buttons	 Access functions and services.
4	Navigation bar and **Select** button	 Scroll through menus, highlight items, and select the highlighted item. When the phone is idle, press **Up** to access the recent calls list and press **Down** to access the favorites list.

5	**Volume** button	 Adjust the speakerphone volume (off hook) and the ringer volume(on hook). When you change the volume, the LED bar lights white to show the volume change.

Conference Phone Softkeys

You can interact with the features on your phone with the softkeys. Softkeys, located below the screen, give you access to the function displayed on the screen above the softkey. The softkeys change depending on what you are doing at the time. The **More ...** softkey shows you that more functions are available.

Related Documentation

Use the following sections to obtain related information.

Cisco IP Conference Phone 7832 Documentation

Refer to publications that are specific to your language and call control system. Navigate from the following documentation URL:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/tsd-products-support-general-information.html

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.doc.gov/policiesandregulations/ear/index.htm.

Terminology Differences

In this document, the term *Cisco IP Phone* includes the Cisco IP Conference Phone 7832.

The following table highlights some of the terminology differences in the *Cisco IP Conference Phone 7832 User Guide*, the *Cisco IP Conference Phone 7832 Administration Guide for Cisco Unified Communications Manager*, and the Cisco Unified Communications Manager documentation.

Table 4: Terminology Differences

User Guide	Administration Guide
Message Indicators	Message Waiting Indicator (MWI)
Voicemail System	Voice Messaging System

PART II

Phone Installation

CHAPTER 3

Cisco IP Conference Phone Installation

Verify the Network Setup

Upon deployment of a new IP telephony system, system administrators and network administrators must complete several initial configuration tasks to prepare the network for IP telephony service.

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

Note The phone displays the date and time from Third-Party Call Control. The time displayed on the phone can differ from the Third-Party Call Control 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.

- Third-Party Call Control 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

Install the Conference Phone

After the phone connects to the network, the phone startup process begins, and the phone registers with Third-party Call Control System . You need to configure the network settings on the phone if you disable the DHCP service.

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

After the phone connects, it determines if a new firmware load should be installed on the phone.

Procedure

Step 1 Choose the power source for the phone:

- Power over Ethernet (PoE)
- Cisco Unified IP Phone Power Injector

For more information, see Ways to Provide Power to Your Conference Phone, on page 19.

Step 2 Connect the phone to the switch.

- If you use PoE, plug the Ethernet cable into the LAN port and plug the other end into the phone.
- If you use the Cisco Unified IP Phone Power Injector, plug the injector into the LAN port with one Ethernet cable. Connect the power cord to the injector and plug the cord into the electrical outlet. Use another Ethernet cable to connect the injector to the conference phone.

Each phone ships with one Ethernet cable in the box.

Step 3 Monitor the phone startup process. This step verifies that the phone is configured properly.

Step 4 If you do not use autoregistration, manually configure the network settings on the phone. See Configure the Network from the Phone, on page 19.

Step 5 Make calls with the phone to verify that the phone and features work correctly.

Step 6 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 Cisco phones.

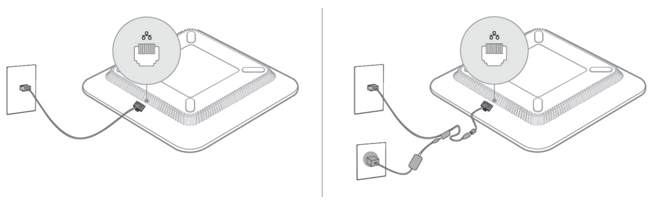
Ways to Provide Power to Your Conference Phone

Your conference phone needs power from one of these sources:

- Power over Ethernet (PoE), which your network supplies.
- Cisco IP Phone Power Injector.

The following figure shows the PoE and midspan cable power options.

Figure 2: Conference Phone Power Options



Configure the Network from the Phone

The phone includes many configurable network settings that you may need to modify before it is functional for your users. You can access these setting through the phone menus.

The Network configuration menu provides you with options to view and configure a variety of network settings.

Note You can control whether a phone has access to the Settings menu or to options on this menu by modifying the value in the Phone-UI-User-Mode field in the **Voice** > **System** > **System Configuration** section of the Phone Configuration Utility page. Also, you must modify the attribute of ua in the Resync file of the phone to control the access. For example, when Phone-UI_User_mode is set to Yes and in the resync file the attribute for Speed_Dial_2 are:

- Speed_Dial_2 ua="rw", you can read and write on web of user model and lcd.
- Speed_Dial_2 ua="na", you can only read on web of user model and lcd.

The Phone-UI-User-Mode field accepts these values:

- Yes: Allows access to the Settings menu. It also allows access to the Phone Configuration Utility page for user-mode.
- No: Prevents access to the Settings menu. It also restricts access to the Phone Configuration Utility page for user-mode.

If you cannot access an option on the Admin Settings menu, check the Phone-UI-User-Mode field.

You can configure settings that are display-only on the phone in your Third-Party Call Control system.

Procedure

Step 1 Press **Settings**.

Step 2 Select **Network configuration**.

Step 3 Use the navigation arrows to select the desired menu and edit.

Step 4 To display a submenu, repeat step 3.

Step 5 To exit a menu, press **Back** .

Network Configuration Fields

Table 5: Ethernet Configuration Submenu

Field	Field Type or Choices	Default	Description
802.1x authentication	Device authentication	Off	Enables you to turn 802.1x authetication on or turn it off. Valid options are: • On • Off
	Transaction status	Disabled	• Transaction status—Indicates different authentication status when you turn on 802.1x in the **Device authentication** field. ◦ Disabled—This is default status. ◦ Connecting—Indicates 802.1x authentication is initiated in the device. ◦ Authenticated—Indicates 802.1x authentication is established in the device. • Protocol—Specifies the protocol of the server.
Switch port config	Auto 10MB half 10MB full 100 MB half 100MB full 100 half 1000 full	Auto	Allows you to select speed and duplex of the network port. 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 autonegotiate.

Field	Field Type or Choices	Default	Description
CDP	On Off	On	Allows you to enable or disable 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.
LLDP-MED	On Off	On	Allows you to enable or disable LLDP-MED. LLDAP-MED enables the phone to advertise itself to device that use discovery protocol.
Startup delay		3 seconds	Allows you to set a value that causes a delay for the switch to get to the forwarding state before the phone will send out the first LLDP-MED packet. The default delay is 3 seconds. For configuration of some switches, you might need to increase this value to a higher value for LLDP-MED to work. Configuring a delay can be important for networks that use Spanning Tree Protocol.
VLAN	On Off	Off	Allows you to enable or disable VLAN. Allows you to enter a VLAN ID when you use VLAN without CDP or LLDP. When you use a VLAN with CDP or LLDP, that associated VLAN takes precedent over the manual entered VLAN ID.
VLAN ID	Text fields in which you need to enter values	1	Allows you to enter a VLAN ID for the IP phone when you use a VLAN without CDP (VLAN enabled and CDP disabled). Note that only voice packets are tagged with the VLAN ID. Do not use 1 for the VLAN ID. If VLAN ID is 1, you cannot tag voice packets with the VLAN ID.

Table 6: IPv4 address settings Submeu

Field	Field Type or Choices	Default	Description
Connection type	DHCP		Indicates whether the phone has DHCP enabled. • DNS1—Identifies the primary Domain Name System (DNS) server that the phone uses. • DNS2—Identifies the secondary Domain Name System (DNS) server that the phone uses. • DHCP address released—Releases the IP address that DHCP assigned. This field is editable if DHCP is enabled. If you wish to remove the phone from the VLAN and release the IP address for reassignment, set this field to Yes and press Set.
	Static IP		When DHCP is disabled, you must set the Internet Protocol (IP) address of the phone. • Static IP address—Identifies the IP that you assign to the phone. The phone uses this IP address instead of acquiring an IP from the DHCP server on the network. • Subnet Mask—Identifies the subnet mask used by the phone. When DHCP is disabled, you must set the subnet mask. • Gateway address—Identifies the default router used by the phone. • DNS1—Identifies the primary Domain Name System (DNS) server that the phone uses. When DHCP is disabled, you must set this field manually. • DNS2—Identifies the primary Domain Name System (DNS) server that the phone uses. When DHCP is disabled, you must set this field manually. If you assign an IP address with this field, you must also assign a subnet mask and a gateway address. See the Subnet Mask and Default Router fields in this table.

Text and Menu Entry From the 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. Press **Select** in the navigation pad to activate the field. 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.
- Press the softkey ⌫ if you make a mistake. This softkey deletes the character to the left of the cursor.
- Press **Revert** before pressing **Apply** to discard any changes that you made.
- To enter a period (for example, in an IP address), press * on the keypad.

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

Related Topics

Basic Reset, on page 185

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.

Note For Cisco IP Phone 8861, if you are using a power cube but there is no Power over Ethernet available, then the wifi will be enabled.

Configure the Voice Codecs

A codec resource is considered allocated if it has been included in the SDP codec list of an active call, even though it eventually might not be chosen for the connection. Negotiation of the optimal voice codec sometimes depends on the ability of the Cisco IP Phone to match a codec name with the far-end device or gateway codec name. The phone allows the network administrator to individually name the various codecs that are supported such that the correct codec successfully negotiates with the far-end equipment.

The Cisco IP Phone supports voice codec priority. You can select up to three preferred codecs. The administrator can select the low-bit-rate codec that is used for each line. G.711a and G.711u are always enabled.

Procedure

Step 1 To configure the voice codecs on each extension, in the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **Ext(n)**, where n is an extension number.

Step 2 In the **Audio Configuration** section, configure the parameters.

Step 3 Click **Submit All Changes**.

VLAN Settings

If you use a virtual LAN (VLAN), your phone voice packets are tagged with the VLAN ID.

In the VLAN Settings section of the **Voice** > **System** window, you can configure these settings:

- Cisco Discovery Protocol (CDP)
- LLDP-MED
- Network Startup Delay
- VLAN ID

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is negotiation-based and determines which virtual LAN (VLAN) the Cisco IP Phone resides in. If you are using a Cisco switch, Cisco Discovery Protocol (CDP) is available and is enabled by default. CDP has these attributes:

- Obtains the protocol addresses of neighboring devices and discovers the platform of those devices.
- Shows information about the interfaces your router uses.
- Is media and protocol-independent.

If you are using a VLAN without CDP, you must enter a VLAN ID for the Cisco IP Phone.

LLDP-MED

The Cisco IP Phone supports Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) for deployment with Cisco or other Third-Party network connectivity devices that use a Layer 2 auto discovery mechanism. Implementation of LLDP-MED is done in accordance with IEEE 802.1AB (LLDP) Specification of May 2005, and ANSI TIA-1057 of April 2006.

The Cisco IP Phone operates as a LLDP-MED Media End Point Class III device with direct LLDP-MED links to Network Connectivity Devices, according to the Media Endpoint Discovery Reference Model and Definition (ANSI TIA-1057 Section 6).

The Cisco IP Phone supports only the following limited set of Type-Length-Values (TLV) as an LLDP-MED Media Endpoint device class III:

- Chassis ID TLV

- Port ID TLV
- Time to live TLV
- Port Description TLV
- System Name TLV
- System Capabilities TLV
- IEEE 802.3 MAC/PHY Configuration/Status TLV (for wired network only)
- LLDP-MED Capabilities TLV
- LLDP-MED Network Policy TLV (for application type=Voice only)
- LLDP-MED Extended Power-Via-MDI TLV (for wired network only)
- LLDP-MED Firmware Revision TLV
- End of LLDPDU TLV

The outgoing LLDPDU contains all the preceding TLVs if applicable. For the incoming LLDPDU, the LLDPDU is discarded if any of the following TLVs are missing. All other TLVs are not validated and ignored.

- Chassis ID TLV
- Port ID TLV
- Time to live TLV
- LLDP-MED Capabilities TLV
- LLDP-MED Network Policy TLV (for application type=Voice only)
- End of LLDPDU TLV

The Cisco IP Phone sends out the shutdown LLDPDU if applicable. The LLDPDU frame contains the following TLVs:

- Chassis ID TLV
- Port ID TLV
- Time to live TLV
- End of LLDPDU TLV

There are some restrictions in the implementation of LLDP-MED on the Cisco IP Phones:

- Storage and retrieval of neighbor information are not supported.
- SNMP and corresponding MIBs are not supported.
- Recording and retrieval of statistical counters are not supported.
- Full validation of all TLVs does not take place; TLVs that do not apply to the phones are ignored.
- Protocol state machines as stated in the standards are used only for reference.

Chassis ID TLV

For the outgoing LLDPDU, the TLV supports subtype=5 (Network Address). When the IP address is known, the value of the Chassis ID is an octet of the INAN address family number followed by the octet string for the IPv4 address used for voice communication. If the IP address is unknown, the value for the Chassis ID is `0.0.0.0`. The only INAN address family supported is IPv4. Currently, the IPv6 address for the Chassis ID is not supported.

For the incoming LLDPDU, the Chassis ID is treated as an opaque value to form the MSAP identifier. The value is not validated against its subtype.

The Chassis ID TLV is mandatory as the first TLV. Only one Chassis ID TLV is allowed for the outgoing and incoming LLDPDUs.

Port ID TLV

For the outgoing LLDPDU, the TLV supports subtype=3 (MAC address). The 6 octet MAC address for the Ethernet port is used for the value of Port ID.

For the incoming LLDPDU, the Port ID TLV is treated as an opaque value to form the MSAP identifier. The value is not validated against its subtype.

The Port ID TLV is mandatory as the second TLV. Only one Port ID TLV is allowed for the outgoing and incoming LLDPDUs.

Time to Live TLV

For the outgoing LLDPDU, the Time to Live TTL value is 180 seconds. This differs from the 120-second value that the standard recommends. For the shutdown LLDPDU, the TTL value is always 0.

The Time to Live TLV is mandatory as the third TLV. Only one Time to Live TLV is allowed for the outgoing and incoming LLDPDUs.

End of LLDPDU TLV

The value is 2-octet, all zero. This TLV is mandatory and only one is allowed for the outgoing and incoming LLDPDUs.

Port Description TLV

For the outgoing LLDPDU, in the Port Description TLV, the value for the port description is the same as “Port ID TLV” for CDP. The incoming LLDPDU, the Port Description TLV, is ignored and not validated. Only one Port Description TLV is allowed for outgoing and incoming LLDPDUs.

System Name TLV

For the Cisco IP Phone, the value is SEP+MAC address.

Example: SEPAC44F211B1D0

The incoming LLDPDU, the System Name TLV, is ignored and not validated. Only one System Name TLV is allowed for the outgoing and incoming LLDPDUs.

System Capabilities TLV

For the outgoing LLDPDU, in the System Capabilities TLV, the bit values for the 2 octet system capabilities fields should be set for Bit 2 (Bridge) and Bit 5 (Phone) for a phone with a PC port. If the phone does not have a PC port, only Bit 5 should be set. The same system capability value should be set for the enabled capability field.

For the incoming LLDPDU, the System Capabilities TLV is ignored. The TLV is not validated semantically against the MED device type.

The System Capabilities TLV is mandatory for outgoing LLDPDUs. Only one System Capabilities TLV is allowed.

Management Address TLV

The TLV identifies an address associated with the local LLDP agent (that may be used to reach higher layer entities) to assist discovery by network management. The TLV allows the inclusion of both the system interface number and an object identifier (OID) that are associated with this management address, if either or both are known.

- TLV information string length—This field contains the length (in octets) of all the fields in the TLV information string.
- Management address string length—This field contains the length (in octets) of the management address subtype + management address fields.

System Description TLV

The TLV allows the network management to advertise the system description.

- TLV information string length—This field indicates the exact length (in octets) of the system description.
- System description—This field contains an alphanumeric string that is the textual description of the network entity. The system description includes the full name and version identification of the system hardware type, software operating system, and networking software. If implementations support IETF RFC 3418, the sysDescr object should be used for this field.

IEEE 802.3 MAC/PHY Configuration/Status TLV

The TLV is not for autonegotiation, but for troubleshooting purposes. For the incoming LLDPDU, the TLV is ignored and not validated. For the outgoing LLDPDU, for the TLV, the octet value autonegotiation support/status should be:

- Bit 0—Set to 1 to indicate that the autonegotiation support feature is supported.
- Bit 1—Set to 1 to indicate that autonegotiation status is enabled.
- Bit 2-7—Set to 0.

The bit values for the 2 octets PMD autonegotiation advertised capability field should be set to:

- Bit 13—10BASE-T half duplex mode
- Bit 14—10BASE-T full duplex mode

- Bit 11—100BASE-TX half duplex mode
- Bit 10—100BASE-TX full duplex mode
- Bit 15—Unknown

Bit 10, 11, 13 and 14 should be set.

The value for 2 octets operational MAU type should be set to reflect the real operational MAU type:

- 16—100BASE-TX full duplex
- 15—100BASE-TX half duplex
- 11—10BASE-T full duplex
- 10—10BASE-T half duplex

For example, usually, the phone is set to 100BASE-TX full duplex. The value 16 should then be set. The TLV is optional for a wired network and not applicable for a wireless network. The phone sends out this TLV only when in wired mode. When the phone is not set for autonegotiation but specific speed/duplexity, for the outgoing LLDPDU TLV, bit 1 for the octet value autonegotiation support/status should be clear (0) to indicate that autonegotiation is disabled. The 2 octets PMD autonegotiation advertised capability field should be set to 0x8000 to indicate unknown.

LLDP-MED Capabilities TLV

For the outgoing LLDPDU, the TLV should have the device type 3 (End Point Class III) with the following bits set for 2-octet Capability field:

Bit Position	Capability
0	LLDP-MED Capabilities
1	Network Policy
4	Extended Power via MDI-PD
5	Inventory

For the incoming TLV, if the LLDP-MED TLV is not present, the LLDPDU is discarded. The LLDP-MED Capabilities TLV is mandatory and only one is allowed for the outgoing and incoming LLDPDUs. Any other LLDP-MED TLVs will be ignored if they present before the LLDP-MED Capabilities TLV.

Network Policy TLV

In the TLV for the outgoing LLDPDU, before the VLAN or DSCP is determined, the Unknown Policy Flag (U) is set to 1. If the VLAN setting or DSCP is known, the value is set to 0. When the policy is unknown, all other values are set to 0. Before the VLAN is determined or used, the Tagged Flag (T) is set to 0. If the tagged VLAN (VLAN ID > 1) is used for the phone, the Tagged Flag (T) is set to 1. Reserved (X) is always set to 0. If the VLAN is used, the corresponding VLAN ID and L2 Priority will be set accordingly. VLAN ID valid value is range from 1-4094. However, VLAN ID=1 will never be used (limitation). If DSCP is used, the value range from 0-63 is set accordingly.

In the TLV for the incoming LLDPDU, Multiple Network Policy TLVs for different application types are allowed.

LLDP-MED Extended Power-Via-MDI TLV

In the TLV for the outgoing LLDPDU, the binary value for Power Type is set to "0 1" to indicate the power type for phone is PD Device. The Power source for the phone is set to "PSE and local" with binary value "1 1". The Power Priority is set to binary "0 0 0 0" to indicate unknown priority while the Power Value is set to maximum power value. The Power Value for the Cisco IP Phone is 12900mW.

For the incoming LLDPDU, the TLV is ignored and not validated. Only one TLV is allowed in the outgoing and incoming LLDPDUs. The phone will send out the TLV for the wired network only.

The LLDP-MED standard was originally drafted in the context of Ethernet. Discussion is ongoing for LLDP-MED for Wireless Networks. Refer to ANSI-TIA 1057, Annex C, C.3 Applicable TLV for VoWLAN, table 24. It is recommended that the TLV is not applicable in the context of the wireless network. This TLV is targeted for use in the context of PoE and Ethernet. The TLV, if added, will not provide any value for network management or power policy adjustment at the switch.

LLDP-MED Inventory Management TLV

This TLV is optional for Device Class III. For the outgoing LLDPDU, we support only Firmware Revision TLV. The value for the Firmware Revision is the version of firmware on the phone. For the incoming LLDPDU, the TLVs are ignored and not validated. Only one Firmware Revision TLV is allowed for the outgoing and incoming LLDPDUs.

Final Network Policy Resolution and QoS

Special VLANs

VLAN=0, VLAN=1, and VLAN=4095 are treated the same way as an untagged VLAN. Because the VLAN is untagged, Class of Service (CoS) is not applicable.

Default QoS for SIP Mode

If there is no network policy from CDP or LLDP-MED, the default network policy is used. CoS is based on configuration for the specific extension. It is applicable only if the manual VLAN is enabled and manual VLAN ID is not equal to 0, 1, or 4095. Type of Service (ToS) is based on configuration for the specific extension.

QoS Resolution for CDP

If there is a valid network policy from CDP:

- If the VLAN=0, 1, or 4095, the VLAN will not be set, or the VLAN is untagged. CoS is not applicable, but DSCP is applicable. ToS is based on the default as previously described.
- If the VLAN > 1 and VLAN< 4095, the VLAN is set accordingly. CoS and ToS are based on the default as previously described. DSCP is applicable.
- The phone reboots and restarts the fast start sequence.

QoS Resolution for LLDP-MED

If CoS is applicable and if CoS=0, the default is used for the specific extension as previously described. But the value shown on L2 Priority for TLV for outgoing LLDPDU is based on the value used for extension 1. If CoS is applicable and if CoS!= 0, CoS is used for all extensions.

If DSCP (mapped to ToS) is applicable and if DSCP=0, the default is used for the specific extension as previously described. But the value show on DSCP for TLV for outgoing LLDPDU is based on value used for the extension 1. If DSCP is applicable and if DSCP!= 0, DSCP is used for all extensions.

If the VLAN > 1 and VLAN < 4095, the VLAN is set accordingly. CoS and ToS are based on the default as previously described. DSCP is applicable.

If there is a valid network policy for the voice application from LLDP-MED PDU and if the tagged flag is set, the VLAN, L2 Priority (CoS), and DSCP (mapped to ToS) are all applicable.

If there is a valid network policy for the voice application from LLDP-MED PDU and if the tagged flag is not set, only the DSCP (mapped to ToS) is applicable.

The Cisco IP Phone reboots and restarts the fast start sequence.

Coexistence with CDP

If both CDP and LLDP-MED are enabled, the network policy for the VLAN determines the last policy set or changed with either one of the discovery modes. If both LLDP-MED and CDP are enabled, during startup the phone sends both CDP and LLDP-MED PDUs at the same time.

Inconsistent configuration and behavior for network connectivity devices for CDP and LLDP-MED modes could result in an oscillating rebooting behavior for the phone due to switching to different VLANs.

If the VLAN is not set by CDP and LLDP-MED, the VLAN ID that is configured manually is used. If the VLAN ID is not configured manually, no VLAN is supported. DSCP is used and the network policy determines LLDP-MED if applicable.

LLDP-MED and Multiple Network Devices

You can use the same application type for network policy. However, phones receive different Layer 2 or Layer 3 QoS Network policies from multiple network connectivity devices. In such a case, the last valid network policy is accepted.

LLDP-MED and IEEE 802.X

The Cisco IP Phone does not support IEEE 802.X and does not work in a 802.1X wired environment. However, IEEE 802.1X or Spanning Tree Protocols on network devices could result in delay of fast start response from switches.

Configure VLAN Settings

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **System**.

Step 2 In the **VLAN Settings** section, configure the fields.

Step 3 Click **Submit All Changes**.

SIP and NAT Configuration

SIP and the Cisco IP Phone

The Cisco IP Phone uses Session Initiation Protocol (SIP), which allows interoperation with all IT service providers that support SIP. SIP is an IETF-defined signaling protocol that controls voice communication sessions in an IP network.

SIP handles signaling and session management within a packet telephony network. *Signaling* allows call information to be carried across network boundaries. *Session management* controls the attributes of an end-to-end call.

In typical commercial IP telephony deployments, all calls go through a SIP Proxy Server. The receiving phone is called the SIP user agent server (UAS), while the requesting phone is called the user agent client (UAC).

SIP message routing is dynamic. If a SIP proxy receives a request from a UAS for a connection but cannot locate the UAC, the proxy forwards the message to another SIP proxy in the network. When the UAC is located, the response routes back to the UAS, and the two UAs connect using a direct peer-to-peer session. Voice traffic transmits between UAs over dynamically assigned ports using Real-time Protocol (RTP).

RTP transmits real-time data such as audio and video; RTP does not guarantee real-time delivery of data. RTP provides mechanisms for the sending and receiving applications to support streaming data. Typically, RTP runs on top of UDP.

SIP Over TCP

To guarantee state-oriented communications, the Cisco IP Phone can use TCP as the transport protocol for SIP. This protocol provides *guaranteed delivery* that assures that lost packets are retransmitted. TCP also guarantees that the SIP packages are received in the same order that they were sent.

TCP overcomes the problem of UDP port-blocking by corporate firewalls. With TCP, new ports do not need to be open or packets dropped, because TCP is already in use for basic activities, such as internet browsing or e-commerce.

SIP Proxy Redundancy

An average SIP Proxy Server can handle tens of thousands of subscribers. A backup server allows an active server to be temporarily switched out for maintenance. Cisco phones support the use of backup SIP Proxy Servers to minimize or eliminate service disruption.

A static list of proxy servers is not always adequate. If your user agent serves different domains, for example, you do not want to configure a static list of proxy servers for each domain into every Cisco IP Phone.

A simple way to support proxy redundancy is to configure a SIP Proxy Server in the Cisco IP Phone configuration profile. The DNS SRV records instruct the phones to contact a SIP Proxy Server in a domain named in SIP messages. The phone consults the DNS server. If configured, the DNS server returns an SRV record that contains a list of SIP Proxy Servers for the domain, with their hostnames, priority, listening ports, and so forth. The Cisco IP Phone tries to contact the hosts in the order of their priority.

If the Cisco IP Phone currently uses a lower-priority proxy server, the phone periodically probes the higher-priority proxy and switches to the higher-priority proxy when available.

Dual Registration

The phone always registers to both primary (or primary outbound) and alternate (or alternate outbound) proxies. After registration, the phone sends out Invite and Non-Invite SIP messages through primary proxy first. If there is no response for the new INVITE from the primary proxy, after timeout, the phone attempts to connect with the alternate proxy. If the phone fails to register to the primary proxy, it sends an INVITE to the alternate proxy without trying the primary proxy.

Dual registration is supported on a per-line basis. Three added parameters can be configured through web user interface and remote provisioning:

- Alternate Proxy—Default is empty.
- Alternate Outbound Proxy—Default is empty.
- Dual Registration—Default is NO (turned off).

After you configure the parameters, reboot the phone for the feature to take effect.

Note Specify a value for primary proxy (or primary outbound proxy) and alternate proxy (or alternate outbound proxy) for the feature to function properly.

Dual Registration and DNS SRV Limitations

- When Dual Registration is enabled, DNS SRV Proxy Fallback or Recovery must be disabled.
- Do not use Dual Registration along with other Fallback or Recovery mechanisms. For example: Broadsoft mechanism.
- There is no recovery mechanism for feature request. However, the administrator can adjust the reregistration time for a prompt update of the registration state for primary and alternate proxy.

Dual Registration and Alternate Proxy

When the Dual Register parameter is set to **No**, Alternate Proxy is ignored.

Failover and Recovery Registration

- Failover—The phone performs a failover when transport timeout/failure or TCP connection failures; if Try Backup RSC and Retry Reg RSC values are datafilled.

- Recovery—The phone attempts to reregister with the primary proxy while registered or actively connected to the secondary proxy.

  Auto register when failover parameter controls the failover behavior when there is an error. When this parameter is set to yes, the phone re-registers upon failover or recovery.

Fallback Behavior

The fallback occurs when the current registration expires or Proxy Fallback Intvl fires.

If the Proxy Fallback Intvl is exceeded, all the new SIP messages go to primary proxy.

For example, when the value for Register Expires is 3600 seconds and Proxy Fallback Intvl is 600 seconds, the fallback triggers 600 seconds later.

When the value for Register Expires is 800 seconds and Proxy Fallback Intvl is 1000 seconds, the fallback triggers at 800 seconds.

After successful registration back to the primary server, all SIP messages go to the primary server.

RFC3311

The Cisco IP Phone supports RFC-3311, the SIP UPDATE Method.

SIP NOTIFY XML-Service

The Cisco IP Phone supports the SIP NOTIFY XML-Service event. On receipt of a SIP NOTIFY message with an XML-Service event, the phone challenges the NOTIFY with a 401 response if the message does not contain correct credentials. The client must furnish the correct credentials using MD5 digest with the SIP account password for the corresponding line of the IP phone.

The body of the message can contain the XML event Message. For example:

```
<CiscoIPPhoneExecute>
  <ExecuteItem Priority="0" URL="http://xmlserver.com/event.xml"/>
</CiscoIPPhoneExecute>
```

Authentication:

```
challenge  = MD5( MD5(A1) ":" nonce ":" nc-value ":" cnonce ":" qop-value
":" MD5(A2) )
where A1 = username ":" realm ":" passwd
and A2 = Method ":" digest-uri
```

SIP Configuration

SIP settings for the Cisco IP Phone are configured for the phone in general and for the extensions.

Configure the Basic SIP Parameters

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **SIP**.

Step 2 In the **SIP Parameters** section, set the SIP parameters as described in the SIP Parameters, on page 127 table.

Step 3 Click **Submit All Changes**.

Configure the SIP Timer Values

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **SIP**.

Step 2 In the **SIP Timer Values** section, set the SIP timer values in seconds as described in the SIP Timer Values, on page 130 table.

Step 3 Click **Submit All Changes**.

Configure the Response Status Code Handling

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **SIP**.

Step 2 In the **Response Status Code Handling** section, set the values as specified:

- **Try Backup RSC**—SIP response code that retries a backup server for the current request. Defaults to blank. For example, you can enter numeric values 500 or a combination of numeric values plus wild cards if multiple values are possible. For the later, you can use 5?? to represent all SIP Response messages within the 500 range. If you want to use multiple ranges, you can add a comma "," to delimit values of 5?? and 6??.

- **Retry Reg RSC**—SIP response code that the phone retries registration after failing during the last registration. Defaults to blank. For example, you can enter numeric values 500 or a combination of numeric values plus wild cards if multiple values are possible. For the later, you can use 5?? to represent all SIP Response messages within the 500 range. If you want to use multiple ranges, you can add a comma "," to delimit values of 5?? and 6??.

Step 3 Click **Submit All Changes**.

Configure the RTP Parameters

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **SIP**.

Step 2 In the **RTP Parameters** section, set the Real-Time Transport Protocol (RTP) parameter values as described in the RTP Parameters, on page 132 table.

Step 3 Click **Submit All Changes**.

Configure the SDP Payload Types

Configured dynamic payloads are used for outbound calls only when the Cisco IP Phone presents a Session Description Protocol (SDP) offer. For inbound calls with an SDP offer, the phone follows the caller's assigned dynamic payload type.

The Cisco IP Phone uses the configured codec names in outbound SDP. For incoming SDP with standard payload types of 0-95, the phone ignores the codec names. For dynamic payload types, the phone identifies the codec by the configured codec names (comparison is case-sensitive).

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **SIP**.

Step 2 In the **SDP Payload Types** section, set the value as specified in the SDP Payload Types, on page 133 table.

- **AVT Dynamic Payload—**Any nonstandard data. Both sender and receiver must agree on a number. Ranges from 96 to 127. Default: 101.

Step 3 Click **Submit All Changes.**

Configure the SIP Settings for Extensions

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **Ext(n)**, where n is an extension number.

Step 2 In the **SIP Settings** section, set the parameter values as described in the SIP Settings, on page 160 table.

Step 3 Click **Submit All Changes**.

Configure the SIP Proxy Server

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **Ext(n)**, where n is an extension number.

Step 2 In the **Proxy and Registration** section, set the parameter values as described in the Proxy and Registration, on page 164 table.

Step 3 Click **Submit All Changes**.

Configure the Subscriber Information Parameters

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **Ext(n)**, where n is an extension number.

Step 2 In the **Subscriber Information** section, set the parameter values as described in the Subscriber Information, on page 166 table.

Step 3 Click **Submit All Changes**.

Managing NAT Transversal with Phones

Network Address Translation (NAT) allows multiple devices to share a single, public, routable, IP address to establish connections over the Internet. NAT is present in many broadband access devices to translate public and private IP addresses. For VoIP to coexist with NAT, NAT traversal is required.

Not all service providers provide NAT traversal. If your service provider does not provide NAT traversal, you have several options:

- NAT Mapping with Session Border Controller
- NAT Mapping with SIP-ALG Router
- NAT Mapping with a Static IP Address
- NAT Mapping with STUN

Enable NAT Mapping

You must enable NAT mapping to set NAT parameters.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **advanced** > **Voice** > **Ext(n)**.

Step 2 Set up the fields as described in the NAT Settings, on page 160 table.

Step 3 Click **Submit All Changes** .

NAT Mapping with Session Border Controller

We recommend that you choose an service provider that supports NAT mapping through a Session Border Controller. With NAT mapping provided by the service provider, you have more choices in selecting a router.

NAT Mapping with SIP-ALG Router

NAT mapping can be achieved by using a router that has a SIP Application Layer Gateway (ALG). By using a SIP-ALG router, you have more choices in selecting an service provider.

NAT Mapping with the Static IP Address

You can configure NAT mapping on the phone to ensure interoperability with the service provider.

- You must have an external (public) IP address that is static .
- The NAT mechanism used in the router must be symmetric. See Determining Symmetric or Asymmetric NAT, on page 38

Use NAT mapping only if the service provider network does not provide a Session Border Controller functionality. To configure NAT mapping on the phone:

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **SIP**.

Step 2 In the **NAT Support Parameters** section, set **Handle VIA received**, **Insert VIA received**, **Substitute VIA Addr**, **Handle VIA rport**, **Insert VIA rport**, **Send Resp To Src Port** fields to **Yes**.

Step 3 In the **NAT Support Parameters** section, set a value for the **NAT Keep Alive Intvl** field.

Step 4 Enter the public IP address for your router in the **EXT IP** field.

Step 5 Click the **Ext(n)** tab.

Step 6 In the **NAT Settings** section, set **NAT Mapping Enable** to **Yes**.

Step 7 (Optional) Set **NAT Keep Alive Enable** to **Yes**.
The service provider might require the phone to send NAT keep alive messages to keep the NAT ports open. Check with your service provider to determine the requirements.

Step 8 Click **Submit All Changes**.

What to Do Next

Configure the firewall settings on your router to allow SIP traffic.

Configure NAT mapping with STUN

If the service provider network does not provide a Session Border Controller functionality and if the other requirements are met, it is possible to use Session Traversal Utilities for NAT (STUN) to discover the NAT mapping. The STUN protocol allows applications operating behind a network address translator (NAT) to discover the presence of the network address translator and to obtain the mapped (public) IP address (NAT addresses) and the port number that the NAT has allocated for the User Datagram Protocol (UDP) connections to remote hosts. The protocol requires assistance from a third-party network server (STUN server) located on the opposing (public) side of the NAT, usually the public Internet. This option is considered a last resort and should be used only if the other methods are not available. To use STUN:

- The router must use asymmetric NAT . See Determining Symmetric or Asymmetric NAT, on page 38
- A computer running STUN server software is available on the network. You can also use a public STUN server or set up your own STUN server.

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **SIP**.

Step 2 In the **NAT Support Parameters** section, set **Handle VIA received**, **Insert VIA received**, **Substitute VIA Addr**, **Handle VIA rport**, **Insert VIA rport**, **Send Resp To Src Port** fields to **Yes**.

Step 3 In the **NAT Support Parameters** section, set **STUN Enable** field to **Yes**.

Step 4 Enter the IP address for your STUN server in the **STUN Server** field.

Step 5 Click the **Ext(n)** tab.

Step 6 In the **NAT Settings** section, set **NAT Mapping Enable** to **Yes**.

Step 7 (Optional) Set **NAT Keep Alive Enable** to **Yes**.
The service provider might require the phone to send NAT keep alive messages to keep the NAT ports open. Check with your service provider to determine the requirements.

Step 8 Click **Submit All Changes**.

What to Do Next

Configure the firewall settings on your router to allow SIP traffic.

Determining Symmetric or Asymmetric NAT

STUN does not work on routers with symmetric NAT. With symmetric NAT, IP addresses are mapped from one internal IP address and port to one external, routable destination IP address and port. If another packet is sent from the same source IP address and port to a different destination, a different IP address and port number combination is used. This method is restrictive because an external host can send a packet to a particular port on the internal host only if the internal host first sent a packet from that port to the external host.

This procedure assumes that a syslog server is configured and is ready to receive syslog messages.

To Determine Whether the Router Uses Symmetric or Asymmetric NAT:

Procedure

Step 1 Verify that the firewall is not running on your PC. (It can block the syslog port.) By default, the syslog port is 514.

Step 2 Click **Voice**>**System** and navigate to **Optional Network Configuration**.

Step 3 Enter the IP address for the **Syslog Server**, if the port number is anything other than the default, 514. It is not necessary to include the port number if it is the default.
The address and port number must be reachable from the Cisco IP phone. The port number appears on the output log file name. The default output file is `syslog.514.log` (if port number was not specified).

Step 4 Set the **Debug Level** to **Error**, **Notice**, or **Debug**.

Step 5 To capture SIP signaling messages, click the **Ext** tab and navigate to **SIP Settings**. Set the **SIP Debug Option** to **Full**.

Step 6 To collect information about what type of NAT your router uses click the **SIP** tab and navigate to **NAT Support Parameters**.

Step 7 Click **Voice**>**SIP** and navigate to **NAT Support Parameters**.

Step 8 Set **STUN Test Enable** to **Yes**.

Step 9 Determine the type of NAT by viewing the debug messages in the log file. If the messages indicate that the device is using symmetric NAT, you cannot use STUN.

Step 10 Click **Submit All Changes**.

Dial Plan

Dial Plan Overview

Dial plans determine how digits are interpreted and transmitted. They also determine whether the dialed number is accepted or rejected. You can use a dial plan to facilitate dialing or to block certain types of calls such as long distance or international.

Use the phone web user interface to configure dial plans on the IP phone.

This section includes information that you must understand about dial plans, and procedures to configure your own dial plans.

The Cisco IP Phone has various levels of dial plans and processes the digits sequence.

When a user presses the speaker button on the phone, the following sequence of events begins:

1. The phone begins to collect the dialed digits. The interdigit timer starts to track the time that elapses between digits.
2. If the interdigit timer value is reached, or if another terminating event occurs, the phone compares the dialed digits with the IP phone dial plan. This dial plan is configured in the phone web user interface in **Voice** > **Ext(n)** under the **Dial Plan** section.

Digit Sequences

A dial plan contains a series of digit sequences, separated by the | character. The entire collection of sequences is enclosed within parentheses. Each digit sequence within the dial plan consists of a series of elements that are individually matched to the keys that the user presses.

White space is ignored, but can be used for readability.

Digit Sequence	Function
0 1 2 3 4 5 6 7 8 9 0 * #	Characters that represent a key that the user must press the phone keypad.
x	Any character on the phone keypad.
[sequence]	Characters within square brackets create a list of accepted key presses. The user can press any one of the keys in the list. A numeric range, for example, `[2-9]` allows a user to press any one digit from `2` through `9`. A numeric range can include other characters. For example, `[35-8*]` allows a user to press 3, 5, 6, 7, 8, or *.
. (period)	A period indicates element repetition. The dial plan accepts `0` or more entries of the digit. For example, `01.` allows users to enter 0, 01, 011, 0111, and so forth.

<dialed:substituted>	This format indicates that certain *dialed* digits are replaced by the *substituted* characters when the sequence is transmitted. The *dialed* digits can be zero to 9. For example:
	`<8:1650>xxxxxxx`
	When the user presses `8` followed by a seven-digit number, the system automatically replaces the dialed `8` with the sequence `1650`. If the user dials **85550112**, the system transmits **16505550112**.
	If the *dialed* parameter is empty and there is a value in the *substituted* field, no digits are replaced and the *substituted* value is always prepended to the transmitted string. For example:
	`<:1>xxxxxxxxxx`
	When the user dials **9725550112**, the number `1` is added at the beginning of the sequence; the system transmits **19725550112**.

, (comma)	An intersequence tone played (and placed) between digits plays an outside line dial tone. For example: `9, 1xxxxxxxxxx` An outside line dial tone plays after the user presses `9`. The tone continues until the user presses `1`.

Digit Sequence	Function
! (exclamation point)	Prohibits a dial sequence pattern. For example: `1900xxxxxxx!` Rejects any 11-digit sequence that begins with 1900.
*xx	Allows a user to enter a 2-digit star code.
S0 or L0	For Interdigit Timer Master Override, enter `S0` to reduce the short interdigit timer to 0 seconds, or enter `L0` to reduce the long interdigit timer to 0 seconds.
P	To pause, enter `P`, the number of seconds to pause, and a space. This feature is typically used for implementation of a hotline and warm line, with a 0 delay for the hot line, and a nonzero delay for a warm line. For example: `P5` A pause of 5 seconds is introduced.

Digit Sequence Examples

The following examples show digit sequences that you can enter in a dial plan.

In a complete dial plan entry, sequences are separated by a pipe character (|), and the entire set of sequences is enclosed within parentheses:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

- Extensions on your system:

  ```
  ( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx
   | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
  ```

  `[1-8]xx` Allows a user dial any three-digit number that starts with the digits 1 to 8. If your system uses four-digit extensions, enter the following string: `[1-8]xxx`

- Local dialing with seven-digit number:

  ```
  ( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx
   | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]111)
  ```

  `9, xxxxxxx` After a user presses 9, an external dial tone sounds. The user can enter any seven-digit number, as in a local call.

- Local dialing with 3-digit area code and a 7-digit local number:

  ```
  ( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx
   | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
  ```

  `9, <:1>[2-9]xxxxxxxxx` This example is useful where a local area code is required. After a user presses 9, an external dial tone sounds. The user must enter a 10-digit number that begins with a digit 2 through 9. The system automatically inserts the 1 prefix before it transmits the number to the carrier.

- Local dialing with an automatically inserted 3-digit area code:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9]
xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

`8, <:1212>xxxxxxx` This example is useful where a local area code is required by the carrier but most calls go to one area code. After the user presses 8, an external dial tone sounds. The user can enter any seven-digit number. The system automatically inserts the 1 prefix and the 212 area code before it transmits the number to the carrier.

- U.S. long-distance dialing:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9]
xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

`9, 1 [2-9] xxxxxxxxx` After the user presses 9, an external dial tone sounds. The user can enter any 11-digit number that starts with 1 and is followed by a digit 2 through 9.

- Blocked number:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9]
xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

`9, 1 900 xxxxxxx !` This digit sequence is useful if you want to prevent users from dialing numbers that are associated with high tolls or inappropriate content, such as 1-900 numbers in the U.S. After the user press 9, an external dial tone sounds. If the user enters an 11-digit number that starts with the digits 1900, the call is rejected.

- U.S. international dialing:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9]
xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

`9, 011xxxxxx` After the user presses 9, an external dial tone sounds. The user can enter any number that starts with 011, as in an international call from the U.S.

- Informational numbers:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9]
xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

`0 | [49]11` This example includes two-digit sequences, separated by the pipe character. The first sequence allows a user to dial 0 for an operator. The second sequence allows the user to enter 411 for local information or 911 for emergency services.

Acceptance and Transmission of the Dialed Digits

When a user dials a series of digits, each sequence in the dial plan is tested as a possible match. The matching sequences form a set of candidate digit sequences. As the user enters more digits, the set of candidates diminishes until only one or none is valid. When a terminating event occurs, the IP PBX either accepts the user-dialed sequence and initiates a call, or else rejects the sequence as invalid. The user hears the reorder (fast busy) tone if the dialed sequence is invalid.

The following table explains how terminating events are processed.

Terminating Event	Processing
Dialed digits have not matched any sequence in the dial plan.	The number is rejected.

Terminating Event	Processing
Dialed digits exactly match one sequence in the dial plan.	If the dial plan allows the sequence, the number is accepted and is transmitted according to the dial plan. If the dial plan blocks the sequence, the number is rejected.
A timeout occurs.	The number is rejected if the dialed digits are not matched to a digit sequence in the dial plan within the time that the applicable interdigit timer specifies. The Interdigit Long Timer applies when the dialed digits do not match any digit sequence in the dial plan. Default: 10 seconds. The Interdigit Short Timer applies when the dialed digits match one or more candidate sequences in the dial plan. Default: 3 seconds.
A user presses the # key or the dial softkey on the IP phone screen.	If the sequence is complete and is allowed by the dial plan, the number is accepted and is transmitted according to the dial plan. If the sequence is incomplete or is blocked by the dial plan, the number is rejected.

Dial Plan Timer (Off-Hook Timer)

You can think of the Dial Plan Timer as the off-hook timer. This timer starts when the phone goes off hook. If no digits are dialed within the specified number of seconds, the timer expires and the null entry is evaluated. Unless you have a special dial plan string to allow a null entry, the call is rejected. The default length of the Dial Plan Timer is 5 seconds.

Syntax for the Dial Plan Timer

SYNTAX: (P*s*<:n> | dial plan)

- **s:** The number of seconds; if no number is entered after P, the default timer of 5 seconds applies. With the timer set to 0 seconds, the call transmits automatically to the specified extension when the phone goes off hook.
- **n:** (optional): The number to transmit automatically when the timer expires; you can enter an extension number or a DID number. No wildcard characters are allowed because the number is transmitted as shown. If you omit the number substitution, <:n>, the user hears a reorder (fast busy) tone after the specified number of seconds.

Examples for the Dial Plan Timer

Allow more time for users to start dialing after taking a phone off hook:

```
(P9 | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

P9 means that after taking a phone off hook, a user has 9 seconds to begin dialing. If no digits are pressed within 9 seconds, the user hears a reorder (fast busy) tone. By setting a longer timer, you allow more time for users to enter digits.

To create a hotline for all sequences on the System Dial Plan:

```
(P9<:23> | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

P9<:23> means that after taking the phone off hook, a user has 9 seconds to begin dialing. If no digits are pressed within 9 seconds, the call is transmitted automatically to extension 23.

To create a hotline on a line button for an extension:

```
( P0 <:1000>)
```

With the timer set to 0 seconds, the call is transmitted automatically to the specified extension when the phone goes off hook. Enter this sequence in the Phone Dial Plan for Ext 2 or higher on a client phone.

Interdigit Long Timer (Incomplete Entry Timer)

You can think of this timer as the incomplete entry timer. This timer measures the interval between dialed digits. It applies as long as the dialed digits do not match any digit sequences in the dial plan. Unless the user enters another digit within the specified number of seconds, the entry is evaluated as incomplete, and the call is rejected. The default value is 10 seconds.

This section explains how to edit a timer as part of a dial plan. Alternatively, you can modify the Control Timer that controls the default interdigit timers for all calls.

Syntax for the Interdigit Long Timer

SYNTAX: L:s, (dial plan)

- **s:** The number of seconds; if no number is entered after L:, the default timer is 5 seconds. With the timer set to 0 seconds, the call is transmitted automatically to the specified extension when the phone goes off hook.
- Note that the timer sequence appears to the left of the initial parenthesis for the dial plan.

Example for the Interdigit Long Timer

```
L:15, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

L:15 means that this dial plan allows the user to pause for up to 15 seconds between digits before the Interdigit Long Timer expires. This setting is especially helpful to users such as sales people, who are reading the numbers from business cards and other printed materials while dialing.

Interdigit Short Timer (Complete Entry Timer)

You can think of this timer as the complete entry timer. This timer measures the interval between dialed digits. The timer applies when the dialed digits match at least one digit sequence in the dial plan. Unless the user enters another digit within the specified number of seconds, the entry is evaluated. If the entry is valid, the call proceeds. If the entry is invalid, the call is rejected.

Default: 3 seconds.

Syntax for the Interdigit Short Timer

SYNTAX 1: S:s, (dial plan)

Use this syntax to apply the new setting to the entire dial plan within the parentheses.

SYNTAX 2: *sequence* Ss

Use this syntax to apply the new setting to a particular dialing sequence.

s: The number of seconds; if no number is entered after S, the default timer of 5 seconds applies.

Examples for the Interdigit Short Timer

To set the timer for the entire dial plan:

```
S:6, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

S:6 means that while the user enters a number with the phone off hook, the user can pause for up to 15 seconds between digits before the Interdigit Short Timer expires. This setting is especially helpful to users such as sales people, who are reading the numbers from business cards and other printed materials while dialing.

Set an instant timer for a particular sequence within the dial plan:

```
(9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxS0 | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

9,8,1[2-9]xxxxxxxxxS0 means that with the timer set to 0, the call is transmitted automatically when the user dials the final digit in the sequence.

Edit the Dial Plan on the IP Phone

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **Ext(n)**, where n is an extension number.

Step 2 Scroll to the **Dial Plan** section.

Step 3 Enter the digit sequences in the **Dial Plan** field.
The default (US-based) systemwide dial plan appears automatically in the field.

Step 4 You can delete digit sequences, add digit sequences, or replace the entire dial plan with a new dial plan. Separate each digit sequence with a pipe character, and enclose the entire set of digit sequences within parentheses. Example:

```
(9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

Step 5 Click **Submit All Changes**.
The phone reboots.

Step 6 Verify that you can successfully complete a call with each digit sequence that you entered in the dial plan.

Note If you hear a reorder (fast busy) tone, review your entries and modify the dial plan appropriately.

Reset the Control Timers

If you need to edit a timer setting only for a particular digit sequence or type of call, you can edit the dial plan.

Procedure

Step 1 Log in to the phone web user interface.

Step 2 Click **Admin Login** > **advanced** > **Voice** > **Regional**.

Step 3 Scroll to the **Control Timer Values (sec)** section.

Step 4 Enter the desired values in the **Interdigit Long Timer** field and the **Interdigit Short Timer** field.

Step 5 Click **Submit All Changes**.

Regional Parameters and Supplementary Services

Regional Parameters

In the phone web user interface, use the **Regional** tab to configure regional and local settings, such as control timer values, dictionary server script, language selection, and locale to change localization. The Regional tab includes these sections:

- Call Progress Tones—Displays values of all ringtones.
- Distinctive Ring Patterns—Ring cadence defines the ringing pattern that announces a telephone call.
- Control Timer Values—Displays all values in seconds.
- Vertical Service Activation Codes—Includes Call Back Act Code and Call Back Deact Code.
- Outbound Call Codec Selection Codes—Defines the voice quality.
- Time—Includes local date, local time, time zone, and Daylight Saving Time.
- Language—Includes Dictionary Server Script, Language Selection, and Locale.

Set the Control Timer Values

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **Regional**.

Step 2 Configure the values in the fields in the **Control Timer Values (sec)** section.

Step 3 Click **Submit All Changes**.

Localize Your Cisco IP Phone

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **Regional**.

Step 2 Configure the values in the fields in the **Time** and **Language** sections.

Step 3 Click **Submit All Changes**.

Time and Date Settings

The Cisco IP Phone obtains the time settings in one of three ways:

- NTP Server—When the phone boots up, it tries to contact the first Network Time Protocol (NTP) server to get the time. The phone periodically synchronizes its time with the NTP server. The synchronization period is fixed at 1 hour. Between updates, the phone tracks time with its internal clock.

  Note NTP time takes priority over the time you set using the menu options on the phone screen. When you manually enter a time, this setting takes effect. On the next NTP synchronization, the time id is corrected so that the NTP time is displayed.

  When you manually enter the phone time, a pop-up is available that alerts you of this behavior.

- SIP Messages—Each SIP message (request or response) sent to the phone can contain a Date header with the current time information. If the header is present, the phone uses it to set its clock.
- Manual Setup—You can use the phone web user interface to enter the time and date manually. However, the NTP time or SIP Message Date overwrites this value when either is available to the phone. Manual setup requires that you enter the time in 24-hour format only.

The time that the NTP Server and the SIP Date Header serve is expressed in GMT time. The local time is obtained by offsetting the GMT according to the time zone of the region.

You can configure the Time Zone parameter with the phone web user interface or through provisioning. This time can be further offset by the Time Offset (HH/mm) parameter. This parameter must be entered in 24-hour format and can also be configured from the IP phone screen.

The Time Zone and Time Offset (HH/mm) offset values are not applied to manual time and date setup

Note The time of the log messages and status messages are in UTC time and are not affected by the time zone setting.

Configure Daylight Saving Time

The phone supports automatic adjustment for daylight saving time.

Note The time of the log messages and status messages are in UTC time. The time zone setting does not affect them.

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **Regional**.

Step 2 Set the **Daylight Saving Time Enable** drop-down list box to **Yes**.

Step 3 In the **Daylight Saving Time Rule** field, enter the DST rule. This value affects the time stamp on the CallerID.

Step 4 Click **Submit All Changes**.

Daylight Saving Time Examples

The following example configures daylight saving time for the U.S, adding one hour starting at midnight on the first Sunday in April and ending at midnight on the last Sunday of October; add 1 hour (USA, North America):

```
start=4/1/7/0:0:0;end=10/31/7/0:0:0;save=1
start=4/1/7;end=10/-1/7;save=1
start=4/1/7/0;end=10/-1/7/0;save=1
```

The following example configures daylight saving time for Egypt, starting at midnight on the last Sunday in April and ending at midnight on the last Sunday of September:

```
start=4/-1/7;end=9/-1/7;save=1 (Egypt)
```

The following example configures daylight saving time for New Zealand (in version 7.5.1 and higher), starting at midnight on the first Sunday of October and ending at midnight on the third Sunday of March.

```
start=10/1/7;end=3/22/7;save=1 (New Zealand)
```

The following example reflects the new change starting in March. DST starts on the second Sunday in March and ends on the first Sunday in November:

```
start=3/8/7/02:0:0;end=11/1/7/02:0:0;save=1
```

The following example configures the daylight saving time starting on the last Monday (before April 8) and ending on the first Wednesday (after May 8.)

```
start=4/-8/1;end=5/8/3;save=1
```

Select a Display Language on the Phone

You can define up to nineteen languages, in addition to English, to be available and host the dictionaries for each of the languages on the HTTP or TFTP provisioning server. Language support follows Cisco dictionary principles.

Use the Language Selection parameter to select the phone default display language. The value must match one of the languages that the dictionary server supports. The script (dx value) is as follows:

- <Language_Selection ua =“na”>

- </Language_Selection>

The Language Selection parameter defaults to blank; the maximum number of characters is 512. For example:

```
<Language_Selection ua=”na”> Spanish
</Language_Selection>
```

During startup, the phone checks the selected language and downloads the dictionary from the TFTP/ HTTP provisioning server that the phone configuration indicates. The dictionaries are available at the support website.

Procedure

Step 1 Press **Settings**.

Step 2 Select **Device administration**.

Step 3 Scroll to **Language**.

Step 4 Select the desired language , then press **Set**.

Dictionary Server Script

The Dictionary Server Script defines the location of the dictionary server, the available languages, and the associated dictionary. The script recognizes up to 19 language entries. The syntax is:

```
Dictionary_Server_Script
serv=tftp://192.168.1.119/
;d0=English;x0=enS_v101.xml;d1=Spanish;x1=esS_v101.xml
```

Note TFTP, HTTP, and HTTPS support exists for the dictionary download.

Default to blank; the maximum number of characters is 512. The detailed format is as follows:

```
serv={server ip port and root path};
d0=language0;x0=dictionary0 filename;
d1=language1;x1=dictionary1 filename;
d2=language2;x2=dictionary2 filename;
d3=language3;x3=dictionary3 filename;
d4=language4;x4=dictionary4 filename;
d5=language5;x5=dictionary5 filename;
d6=language6;x6=dictionary6 filename;
d7=language7;;x7=dictionary7 filename;
d8=language8;x8=dictionary8 filename;
d9=language9;x9=dictionary9 filename;
```

The following languages locales are supported on the Cisco IP Phone:

- None: English-US
- bg-BG: Bulgarian
- cs-CZ: Czech
- da-DK: Danish
- fi-FI: Finnish
- fr-FR: French

- de-DE: German
- es-ES: Spanish-ES
- hr-HR: Croatian
- hu-HU: Hungarian
- it-IT: Italian
- nl-NL: Dutch
- no-NO: Norwegian
- pl-PL: Polish
- pt-PT: Portuguese
- sk-SK: Slovak
- sv-SE: Swedish
- tr-TR: Turkish

Localization Configuration Example

Language Selection: French

(Entry dx must match one of the languages that the dictionary server supports.)

Locale: fr-FR

(Entry lx must be within the Locale option list.)

Cisco IP Phone 7800 Series Documentation

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

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/tsd-products-support-series-home.html

CHAPTER 4

Third-Party Call Control Setup

Determine the Phone MAC Address

To add phones to the Third-Party Call Control system, determine the MAC address of a Cisco IP Phone.

Procedure

Perform one of the following actions:

- On the phone, press **Settings** > **Status** > **Product 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 select **Info** > **Status** > **Product Information**.

Network Configuration

The Cisco IP Phone is used as a part of a SIP network, because the phone supports Session Initiation Protocol (SIP). The Cisco IP Phone is compatible with other SIP IP PBX call control systems, such as BroadSoft, MetaSwitch, and Asterisk.

Configuration of these systems is not described in this document. For more information, see the documentation for the SIP PBX system to which you are connecting the Cisco IP Phone.

This document describes some common network configurations; however, your configuration can vary, depending on the type of equipment that your service provider uses.

Provisioning

Phones can be provisioned to download configuration profiles or updated firmware from a remote server when they are connected to a network, when they are powered up, and at set intervals. Provisioning is typically part of high-volume, Voice-over-IP (VoIP) deployments and is limited to service providers. Configuration profiles or updated firmware are transferred to the device through use of TFTP, HTTP, or HTTPS.

The *Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series Multiplatform Phones Provisioning Guide* describes provisioning in detail.

Web-Based Configuration Utility

Your phone system administrator can allow you to view the phone statistics and modify some or all the parameters. This section describes the features of the Cisco IP Phone that you can modify with the phone web user interface.

Access the Web-Based Configuration Utility

Access the Cisco IP Phone configuration utility from a web browser on a computer that can reach the phone on the subnetwork.

Procedure

Step 1 If the computer is connected to a VPN, exit the VPN.

Step 2 Launch a web browser.

Step 3 Enter the IP address of the phone in your web browser address bar.
For example, `http://10.64.84.147`

Note If your service provider disables access to the configuration utility, contact the service provider to proceed.

Determine the IP Address of the Phone

A DHCP server assigns the IP address, so the phone must be booted up and connected to the subnetwork.

Procedure

Step 1 Click **Admin Login** > **advanced** > **Info** > **Status**.

Step 2 Scroll to **IPv4 Information**. Current IP displays the IP address.

Allow Web Access to the Cisco IP Phone

To view the phone parameters, enable the configuration profile. To make changes to any of the parameters, you must be able to change the configuration profile. Your system administrator might have disabled the phone option to make the phone web user interface viewable or writable.

For more information, see the *Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series Multiplatform Phones Provisioning Guide*.

Procedure

Step 1 Click **Admin Login** > **Voice** > **System**.

Step 2 In the **System Configuration** section, set **Enable Web Server** to **Yes**.

Step 3 To update the configuration profile, click **Submit All Changes** after you modify the fields in the phone web user interface.
The phone reboots and the changes are applied.

Step 4 To clear all changes that you made during the current session (or after you last clicked **Submit All Changes**), click **Undo All Changes**. Values return to their previous settings.

Web Administration Tabs

Each tab contains parameters that are related to a particular feature. Some tasks require that you set multiple parameters in different tabs.

Info, on page 111 briefly describes each parameter that is available on the phone web user interface.

Administrator and User Accounts

The Cisco IP Phone firmware provides specific administrator and user accounts. These accounts provide specific login privileges. The administrator account name is **admin**; the user account name is **user**. These account names cannot be changed.

The **admin** account gives the service provider or Value-added Reseller (VAR) configuration access to the Cisco IP phone. The **user** account gives limited and configurable control to the device end user.

The **user** and **admin** accounts can be password protected independently. If the service provider sets an administrator account password, you are prompted for it when you click **Admin Login**. If the password does not yet exist, the screen refreshes and displays the administration parameters. No default passwords are assigned to either the administrator or the user account. Only the administrator account can assign or change passwords.

The administrator account can view and modify all web profile parameters, including web parameters, that are available to the user login. The Cisco IP Phone system administrator can further restrict the parameters that a user account can view and modify through use of a provisioning profile.

Configuration parameters that are available to the user account are configurable on the Cisco IP Phone. User access to the phone web user interface can be disabled.

Enable User Access to the Phone Interface Menus

Use the **admin** account to enable or disable access to the phone web user interface by the **user** account. If the user account has access, users can set parameters, such as speed-dial numbers and caller ID blocking, through the phone web user interface.

Use phone profile provisioning to restrict the ability to configure individual parameters. For more information on provisioning, see the *Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series Multiplatform Phones Provisioning Guide*.

Procedure

Step 1 Click **Admin Login** > **advanced** > **Voice** > **System**.

Step 2 Under **System Configuration** in the **Phone-UI-User-Mode** field, choose **Yes**.

Step 3 Click **Submit All Changes**.

Access Administrative Options by Login

Procedure

Step 1 Log in to the configuration utility.

Step 2 Click **Admin Login.**

Step 3 If prompted, enter the **Admin Password**.

Access Administrative Options by IP Address

Procedure

Enter the IP address of the Cisco IP Phone in a web browser and include the **admin/** extension.
For example: `http://10.64.84.147/admin/`

PART III

Phone Administration

CHAPTER 5

Cisco IP Conference Phone Security

Security Features

Security features ensure that calls are secure and authenticated.

Domain and Internet Setting

Configure Restricted Access Domains

If you enter domains, the Cisco IP Phone responds only to SIP messages only from the identified servers.

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **System**.

Step 2 In the **System Configuration** section, in the **Restricted Access Domains** field, enter fully qualified domain names (FQDNs) for each SIP server that you want the phone to respond to. Separate FQDNs with semicolons.

Example:

```
voiceip.com; voiceip1.com
```

Step 3 Click **Submit All Changes**.

Configure the Internet Connection Type

You can set the connection type to one of the following:

- Dynamic Host Configuration Protocol (DHCP) - Enables the phone to receive an IP address from the network DHCP server. The Cisco IP phone typically operates in a network where a DHCP server assigns

IP addresses to devices. Because IP addresses are a limited resource, the DHCP server periodically renews the device lease on the IP address. If a phone loses the IP address for any reason, or if some other device on the network is assigned the same IP address, the communication between the SIP proxy and the phone is either severed or degraded. Whenever an expected SIP response is not received within a programmable amount of time after the corresponding SIP command is sent, the DHCP Timeout on Renewal parameter causes the device to request a renewal of its IP address. If the DHCP server returns the IP address that it originally assigned to the phone, the DHCP assignment is presumed to be operating correctly. Otherwise, the phone resets to try to fix the issue.

- Static IP - A static IP address for the phone.

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **System**.

Step 2 In the **IPv4 Settings** section, use the **Connection Type** drop-down list box to choose the connection type:

- Dynamic Host Configuration Protocol (DHCP)
- Static IP

Step 3 If you choose Static IP, configure these settings in the **Static IP Settings** section:

- **Static IP—**Static IP address of the phone
- **NetMask—**Netmask of the phone
- **Gateway—**Gateway IP address

Step 4 Click **Submit All Changes**.

DHCP Option Support

The following table lists the DHCP options that are supported on the Cisco IP Phone.

Network Standard	Description
DHCP option 1	Subnet mask
DHCP option 2	Time offset
DHCP option 3	Router
DHCP option 6	Domain name server
DHCP option 15	Domain name
DHCP option 41	IP address lease time
DHCP option 42	NTP server

Network Standard	Description
DHCP option 43	Vendor-specific information Can be used for TR.69 Auto Configurations Server (ACS) discovery.
DHCP option 60	Vendor class identifier
DHCP option 66	TFTP server name
DHCP option 125	Vendor-identifying vendor-specific information Can be used for TR.69 Auto Configurations Server (ACS) discovery.
DHCP option 150	TFTP server
DHCP option 159	Provisioning server IP
DHCP option 160	Provisioning URL

Configure the Challenge for the SIP INVITE Messages

The phone can challenge the SIP INVITE (initial) message in a session. The challenge restricts the SIP servers that are permitted to interact with the devices on a service provider network. This practice significantly increases the security of the VoIP network through prevention of malicious attacks against the device.

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **Ext(n)**, where n is an extension number.

Step 2 In the **SIP Settings** section, choose **Yes** from the **Auth INVITE** drop-down list box.

Step 3 Click **Submit All Changes**.

Transport Layer Security

Transport Layer Security (TLS) is a standard protocol for securing and authenticating communications over the Internet. SIP over TLS encrypts the SIP messages between the service provider SIP proxy and the end user. SIP over TLS encrypts only the signaling messages, not the media.

TLS has two layers:

- TLS Record Protocol—Layered on a reliable transport protocol, such as SIP or TCH, this layer ensures that the connection is private through use of symmetric data encryption and it ensures that the connection is reliable.
- TLS Handshake Protocol—Authenticates the server and client, and negotiates the encryption algorithm and cryptographic keys before the application protocol transmits or receives data.

The Cisco IP Phone uses UDP as the standard for SIP transport, but the phone also supports SIP over TLS for added security.

Configure SIP Over TLS Signaling Encryption

Procedure

Step 1 To enable TLS for the phone, in the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **Ext(n)**, where n is an extension number.

Step 2 In the **SIP Settings** section, select **TLS** from the **SIP Transport** drop-down list box.

Step 3 Click **Submit All Changes**.

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.doc.gov/policiesandregulations/ear/index.htm.

CHAPTER 6

Cisco IP Conference Phone Customization

Phone Information and Display Settings

The phone web user interface allows you to customize settings such as the phone name, background picture, logo, and screen saver.

Configure the Phone Name

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **Phone.**

Step 2 Under **General**, enter the phone name in the **Station Display Name** field.
This name displays on the phone LCD in the top left corner.

Step 3 Click **Submit All Changes**.

Customize the Startup Screen with Text and Picture

You can create a text or 128-by-48 pixel by 1-bit deep image logo to display when the Cisco IP Phone boots up. A logo displays during the boot sequence for a short period after the Cisco logo displays.

Procedure

Step 1 Click **Admin Login** > **advanced** > **Voice** > **User**.

Step 2 In the **Screen** section, select any option from the **Boot Display** field.

- **Default**: Displays a blank screen or existing screen as the startup screen.
- **Download Picture**: Displays a picture as the startup screen. Enter the path in the **Picture Download URL** field.

  For example:

  ```
  http://10.64.84.147/pictures/image04_128x48.png
  ```

  When you enter an incorrect URL to download a new wallpaper, the phone fails to upgrade to the newer wallpaper and displays the existing downloaded wallpaper. If the phone does not have any wallpaper downloaded earlier, it displays a gray screen.

  The supported phone image file attributes are: Bitmap format, one bit-per-pixel color, size 128-by-48 pixels. You can also use a TFTP server.

- **Logo**: Displays a logo as the startup screen. See Add Logo as Boot Display , on page 62.
- **Text**: Displays a text as the startup screen. Enter text in the **Text Display** field. Enter up to two lines of text. Each line must be less than 32 characters. Insert a new line character (\n) and escape code (%0a) between the two lines.

  For example, `Super\n%0aTelecom` displays:

  ```
  Super
  Telecom
  ```

  Use the + character to add spaces for formatting. You can add multiple + characters before and after the text to center it.

Step 3 Click **Submit All Changes.**

The phone reboots, retrieves the .png file, and displays the picture when it next boots.

Add Logo as Boot Display

If you want your user to see a logo icon when the phone restarts, enable this feature from the phone web page.

Procedure

Step 1 On the phone web page, select **Admin Login** > **Advanced** > **Voice** > **User**.

Step 2 In the **Screen** section, select **Logo** from the **Boot Display** field. In the **Logo URL** field, enter a URL or path for the location where the logo image is saved.
You can also download a picture and add as a boot display: select **Download Picture** from the **Boot Display** field. In the **Picture Download URL** field, enter a URL or path for the location where the picture is saved.

The logo must be a .jpg or a .png file. The phone has a fixed display area. So, if the original logo size doesn't fit into the display area scale to fit it. For the Cisco IP Phone 7832, the logo display area is at the mid-center of the phone screen. The display area size of the Cisco IP phone 7832 is 48x48.

Step 3 Click **Submit All Changes**.

Configure the Number of Call Appearances Per Line

Phones that support multiple call appearances on a line can be configured to specify the number of calls to allow on the line.

Procedure

Step 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**.

Step 2 In the **Miscellaneous Line Key Settings** section, use the **Call Appearances Per Line** drop-down list box to specify the number of calls per line to allow.

Step 3 Click **Submit All Changes**.

Call Features Configuration

Enable Call Transfer

Procedure

Step 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**.

Step 2 Under **Supplementary Services,** choose **Yes** for each of the transfer services that you want to enable:

- **Attn Transfer Serv—**Attended call transfer service. The user answers the call before transferring it.
- **Blind Transfer Serv—**Blind call transfer service. The user transfers the call without speaking to the caller.

Step 3 To disable a transfer service, set the field to **No**.

Step 4 Click **Submit All Changes**.

Call Forward

To enable call forwarding, you can enable the feature in two places: on the Voice tab and the User tab of the phone web page.

Enable Call Forwarding on Voice Tab

Perform this task if you want to enable call forward for a user.

Procedure

Step 1 On the Configuration Utility page, click **Admin Login** > **advanced** > **Voice** > **Phone**.

Step 2 Under **Supplementary Services**, choose **Yes** for each of the call forwarding services that you want to enable:

- **Cfwd All Serv—**Forwards all calls.
- **Cfwd Busy Serv—**Forwards calls only if the line is busy.
- **Cfwd No Ans Serv—**Forwards calls only if the line is not answered.

Step 3 Click **Submit All Changes.**

Enable Call Forwarding on User Tab

Perform the following task if you want to give a user the ability to modify the call forward settings from the Configuration Utility page.

Procedure

Step 1 On the Configuration Utility page, click **Admin Login** > **advanced** > **Voice** > **User**.

Step 2 Under **Call Forward**, choose **Yes** for CFWD Setting.

Step 3 Click **Submit All Changes.**

Enable Conferencing

Procedure

Step 1 In the phone web user interface, navigate to **Admin Login** > **advanced** > **Voice** > **Phone**.

Step 2 Under **Supplementary Services**, choose **Yes** in the **Conference Serv** drop-down list box.

Step 3 Click **Submit All Changes**.

Configure Missed Call Indication with the Configuration Utility

If a user is not on an active or held call and misses a call, the user needs to know about the missed call. To alert the user, configure the **Handset LED Alert** field on the Configuration Utility page. If you set this field to **Voicemail, Missed Call**, the LED on the Handset will turn on when the user has recently missed a call.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **Advanced** > **Voice** > **User**.

Step 2 In the **Supplementary Services** section, choose **Voicemail, Missed Call** in the **Handset LED Alert** drop-down list box.
The user can select **User Login** > **Voice** > **User**.

Step 3 Click **Submit All Changes.**

Enable Do Not Disturb

You can allow users to turn the do not disturb feature on or off. The caller receives a message that the user is unavailable. Users can press the **Ignore** softkey on their phones to divert a ringing call to another destination.

If the feature is enabled for the phone, users turn the feature on or off with the DND softkey.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **advanced** > **Voice** > **User**.

Step 2 In the **Supplementary Services** section, choose **Yes** in the **DND Setting** drop-down list box.

Step 3 Click **Submit All Changes**.

Configure Synchronization of DND and Call Forward

Enable synchronization of Do Not Disturb (DND) and Call Forward to allow changes to these features that are made on the phone to be made on the server. Changes made on the server are also made on the phone.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **advanced** > **Voice** > **Ext [n]** (where [n] is the extension number).

Step 2 In the **Call Feature Settings** section, set the **Feature Key Sync** field to **Yes**.

Step 3 Click **Submit All Changes**.

Configure Star Codes for DND

You can configure star codes that a user dials to turn on or off the do not disturb (DND) feature on a phone.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **advanced** > **Voice** > **Regional**.

Step 2 In the **Vertical Service Activation Codes** area, enter *78 in the **DND Act Code** field.

Step 3 In the **Vertical Service Activation Codes** area, enter *79 in the **DND Deact Code** field.

Step 4 Click **Submit All Changes**.

Shared Lines

A shared line is a directory number that appears on more than one phone. You can create a shared line by assigning the same directory number to different phones.

Incoming calls display on all phones that share a line, and anyone can answer the call. Only one call remains active at a time on a phone.

Call information displays on all phones that are sharing a line. If somebody turns on the privacy feature, you do not see the outbound calls made from the phone. However, you see inbound calls to the shared line.

All phones with a shared line ring when a call is made to the line. If you place the shared call on hold, anyone can resume the call by pressing the corresponding line key from a phone that shares the line. You can also press the Select button if the Resume icon is displayed.

The following shared line features are supported:

- Line Seizure
- Public Hold
- Private Hold

- Silent Barge (only through enabled programmable softkey)

The following features are supported as for a private line

- Transfer
- Conference
- Call Park / Call Retrieve
- Call Pickup
- Do Not Disturb
- Call Forward

You can configure each phone independently. Account information is usually the same for all IP phones, but settings such as the dial plan or preferred codec information can vary.

Configure a Shared Line

You can create a shared line by assigning the same directory number to different phones on the phone web page.

Procedure

Step 1 On the Configuration Utility page, click **Admin Login** > **advanced** > **Voice**.

Step 2 Click the **Ext_n tab** of the extension that is shared.

Step 3 Under **General** in the Line Enable list, choose **Yes**.

Step 4 Under **Share Line Appearance** in the Share Ext list, select **Shared**.
If you set this extension to **Private**, the extension does not share calls, regardless of the Share Call Appearance setting on the Phone tab. If you set this extension to **Shared**, calls follow the Share Call Appearance setting on the Phone tab.

Step 5 In the **Shared User ID field**, enter the user ID of the phone with the extension that is being shared.

Step 6 In the **Subscription Expires** field, enter the number of seconds before the SIP subscription expires. The default is 60 seconds.
Until the subscription expires, the phone gets NOTIFY messages from the SIP server on the status of the shared phone extension.

Step 7 In the **Restrict MWI** field, set the message waiting indicator:

- **Yes—**Lights only for messages on private lines (SIP).
- **No—**Lights for all messages.

Step 8 Under **Proxy and Registration**, enter the IP address of the proxy server in the Proxy field.

Step 9 Under **Subscriber Information,** enter a Display Name and User ID (extension number) for the shared extension.

Step 10 In the Phone tab, under **Miscellaneous Line Key Settings**, configure SCA Barge-In Enable:

- **Yes—**Allows users to take over the call on a shared line.

- **No—**Prevents users from taking over the call on a shared line.

Step 11 Click **Submit All Changes.**

Configure Voice Mail

You can configure the internal or external phone number or URL for the voice mail system. If you are using an external voice mail service, the number must include any digits required to dial out and any required area code

Procedure

Step 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**.

Step 2 Under **General**, enter the **Voice Mail Number**.

Step 3 Click **Submit All Changes**. The phone reboots.

Configure Voice Mail for each Extension

Procedure

Step 1 Click **Admin Login** > **advanced** > **Voice** > **Extn**.

Step 2 Under **Call Feature Settings**, enter the **Voice Mail Server**.

Step 3 (Optional) Enter the **Voice Mail Subscribe Interval**; the expiration time in seconds, of a subscription to a voice mail server.

Step 4 Click **Submit All Changes**.
The phone reboots.

Configure the Message Waiting Indicator

You can configure the Message Waiting Indicator for separate extensions on the phone. The Message Waiting Indicator lights based on the presence of new voicemail messages in the mailbox.

You can enable the indicator at the top of your IP phone to light when voice mail is left, or display a seeing message waiting notification.

Procedure

Step 1 Click **Admin Login** > **advanced** > **Voice** > **Extn**.

Step 2 Under **Call Feature Settings** in the **Message Waiting** , choose **Yes** to enable.

Assign a Ring Tone to an Extension

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **advanced** > **Voice** > **Ext(n)**, where **(n)** is the number of an extension.

Step 2 Under **Call Feature Settings**, use the **Default Ring (n)** drop-down list box to specify one of the following:

- No Ring
- Choose one of the available 12 ring tones.

Step 3 Click **Submit All Changes**.

Configure the Audio Settings

The user can modify volume settings by pressing the volume control button on the phone, then pressing the **Save** softkey.

Procedure

Step 1 Click **Admin Login** > **advanced** > **Voice** > **User**.

Step 2 In the **Audio Volume** section, configure a volume level between 1 and 10, with 1 being the lowest level:

- **Ringer Volume—**Sets the ringer volume.
- **Speaker Volume—**Sets the volume for the full-duplex speakerphone.
- **Headset Volume—**Sets the headset volume.
- **Handset Volume—**Sets the handset volume.
- **Electronic HookSwitch Control—**Enables or disables the EHS feature.

Step 3 Click **Submit All Changes.**

User Access Control

The Cisco IP Phone respects only the "ua" user access attribute. For a specific parameter, the "ua" attribute defines access by the user account to the administration web server. If the "ua" attribute is not specified, the phone applies the factory default user access for the corresponding parameter. This attribute does not affect access by the admin account.

Note The value of the element attribute encloses within double quotes.

The "ua" attribute must have one of the following values:

- na – no access
- ro – read-only
- rw – read/write

Phone Web Server

The web server allows administrators and users to log in to the phone by using a phone web user interface. Administrators and users have different privileges and see different options for the phone based on their role.

Configure the Web Server from the Phone Screen Interface

Use this procedure to enable the phone web user interface from the phone screen.

Procedure

Step 1 Press **Settings**.

Step 2 Select **Network configuration** > **Web Server**.

Step 3 Select **On** to enable or **Off** to disable.

Step 4 Press **Set**.

Direct action URL

If the Enable Direct Action URL setting is set to "Yes ", these Direct action URLs are accessible only for the admin. If Admin user is password protected, the client provides a login prompt before these are accessed. The Direct Action URLs are accessible via the phone web page via the path `/admin/<direct_action>`. The syntax is:

http[s]://<ip_or_hostname>/admin/<direct_action>[?<url>]

For example, http://10.1.1.1/admin/resync?http://server_path/config.xml

The following table provides a list of the different direct avtion URLs that are supported.

direct_action	Description	Example
resync	Initiates a one-time resync of the config file specified by URL. The URL to resync is provided by appending ? followed by the URL. The URL specified here will not be saved anywhere in the phone settings.	http://10.1.1.1/admin/resync?http://my_provision_server.com/cfg/device.cfg
upgrade	Initiates an upgrade of a phone to the specified load. The load is specified via the upgrade rule. the rule is specified by appending ? followed by URL path to the load. The upgrade rule specified is one time only and will not be saved in any property setting.	http://10.1.1.1/admin/upgrade?http://my_upgrade_server.com/loads/sip88xx.11.0.0MPP2123.loads
updateca	Initiates a one-time install of the Custom Certificate Authority (Custom CA) specified by the URL. The URL to download is provided by appending ? followed by the URL. The URL specified here will not be saved anywhere in the phone settings.	http://10.1.1.1/admin/updateca?http://my_cert_server.com/certs/myCompanyCA.pem
reboot	Initiates a reboot of the phone. Does not take any parameter with ?	http://10.1.1.1/admin/reboot
cfg.xml	Downloads a snapshot of the phone configuration in XML format. The passwords are hidden for security. Most of the information here corresponds to the properties on the phone web page under **Voice** tab.	http://10.1.1.1/admin/cfg.xml
status.xml	Downloads a snapshot of the phone status in XML format. Most of the information here corresponds to the **Status** tab in the phone web page.	http://10.1.1.1/admin/status.xml
screendump.bmp	Downloads a screenshot of the phone LCD UI at the time when this action is initiated.	http://10.1.1.1/admin/screendump.bmp
log.tar	Downloads a set of archived logs stored on the phone.	http://10.1.1.1/admin/log.tar

Enable Access to Phone Web Interface

Procedure

Step 1 Click **Admin Login** > **advanced** > **Voice** > **System**.

Step 2 Under the **System Configuration** section, choose **Yes** from the **Enable Web Server** drop-down list box.

Step 3 In the **Enable Protocol** drop-down list box, choose Http or Https.

Step 4 In the **Web Server Port** field, enter the port to access the web server. The default is port 80 for HTTP or port 443 for HTTPS.

Step 5 In the **Enable Web Admin Access** drop-down list box, you can enable or disable local access to the **Admin Login** of the phone web user interface. Defaults to **Yes** (enabled).

Step 6 In the **Admin Password** field, enter a password if you want the system administrator to log in to the phone web user interface with a password. The password prompt appears when an administrator clicks **Admin Login**. The minimum password length can be 4 characters or the maximum password length is 127 characters.

Note Password can contain any character except the Space key.

Step 7 In the **User Password** field, enter a password if you want users to log in to the phone web user interface with a password. The password prompt appears when users click **User Login**. The minimum password length can be 4 characters or the maximum password length is 127 characters.

Note Password can contain any character except the Space key.

Step 8 Click **Submit All Changes**.

XML Services

The phones provide support for XML services, such as an XML Directory Service or other XML applications. For XML services, only HTTP and HTTPS support are available.

The following Cisco XML objects are supported:

- CiscoIPPhoneMenu
- CiscoIPPhoneText
- CiscoIPPhoneInput
- CiscoIPPhoneDirectory
- CiscoIPPhoneIconMenu
- CiscoIPPhoneStatus
- CiscoIPPhoneExecute
- CiscoIPPhoneImage
- CiscoIPPhoneImageFile
- CiscoIPPhoneGraphicMenu
- CiscoIPPhoneFileMenu

- CiscoIPPhoneStatusFile
- CiscoIPPhoneResponse
- CiscoIPPhoneError
- CiscoIPPhoneGraphicFileMenu
- Init:CallHistory
- Key:Headset
- EditDial:n

There are more URIs supported which are available in the *Cisco Unified IP Phone Services Application Development Notes*.

For more information, see the *Cisco Unified IP Phone Services Application Development Notes* located here: http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/all_models/xsi/9-1-1/CUIP_BK_P82B3B16_00_phones-services-application-development-notes.html.

XML Directory Service

When an XML URL requires authentication, use the parameters XML UserName and XML Password.

The parameter XML UserName in XML URL is replaced by $XML UserName.

For example:

The parameter XML UserName is cisco. The XML Directory Service URL is http://www.sipurash.compath?username=$XML_User_Name.

This results in the request URL: `http://www.sipurash.com/path?username=cisco`.

XML Applications

When authentication is required for CGI/Execute URL via Post from an external application (for example, a web application) to the phones, the parameter `CISCO XML EXE Auth Mode` is used in 3 different scenarios:

- Trusted—No authentication is performed (local user password is set or not). This is the default.
- Local Credential—Authentication is based on digest authentication using the local user password, if the local user password is set. If not set, then no authentication is performed.
- Remote Credential—Authentication is based on digest authentication using the remote username/password as set in the XML application on the web page (to access an XML application server).

Macro Variables

You can use macro variables in XML URLs. The following macro variables are supported:

- User ID—UID1, UID2 to UIDn
- Display name—DISPLAYNAME1, DISPLAYNAME2 to DISPLAYNAMEn
- Auth ID—AUTHID1, AUTHID2 to AUTHIDn
- Proxy—PROXY1, PROXY2 to PROXYn

- MAC Address using lower case hex digits—MA
- Product Name—PN
- Product Series Numbe—PSN
- Serial Number—SERIAL_NUMBER

The following table shows the list of macros supported on the phones:

Macro Name	Macro Expansion
$	The form $$ expands to a single $ character.
A through P	Replaced by general purpose parameters GPP_A through GPP_P.
SA through SD	Replaced by special purpose parameters GPP_SA through GPP_SD. These parameters hold keys or passwords used in provisioning. **Note** $SA through $SD are recognized as arguments to the optional resync URL qualifier, --key.
MA	MAC address using lower case hex digits (000e08aabbcc).
MAU	MAC address using upper case hex digits (000E08AABBCC).
MAC	MAC address using lower case hex digits with colon to separate hex digit pairs (00:0e:08:aa:bb:cc).
PN	Product Name; for example IP Phone 8861.
PSN	Product Series Number; for example 8861.
SN	Serial Number string; for example 88012BA01234.
CCERT	SSL Client Certificate status, installed or not installed.
IP	IP address of the phone within its local subnet; for example 192.168.1.100.
EXTIP	External IP of the phone, as seen on the internet; for example 66.43.16.52.
SWVER	Software version string; for example 2.0.6(b).
HWVER	Hardware version string; for example 1.88.1.
PRVST	Provisioning State (a numeric string): • -1 = explicit resync request • 0 = power-up resync • 1 = periodic resync • 2 = resync failed, retry attempt

Macro Name	Macro Expansion
UPGST	Upgrade State (a numeric string): • 1 = first upgrade attempt • 2 = upgrade failed, retry attempt
UPGERR	Result message (ERR) of previous upgrade attempt; for example http_get failed.
PRVTMR	Seconds since last resync attempt.
UPGTMR	Seconds since last upgrade attempt.
REGTMR1	Seconds since Line 1 lost registration with SIP server.
REGTMR2	Seconds since Line 2 lost registration with SIP server.
UPGCOND	Legacy macro name.
SCHEME	File access scheme (TFTP, HTTP, or HTTPS, obtained after parsing resync or upgrade URL).
METH	Deprecated alias for SCHEME, do not use.
SERV	Request target server host name.
SERVIP	Request target server IP address (following DNS lookup).
PORT	Request target UDP/TCP port.
PATH	Request target file path.
ERR	Result message of resync or upgrade attempt.
UIDn	The contents of the Line n UserID configuration parameter
ISCUST	If unit is customized, value=1, otherwise 0. **Note** Customization status viewable on Web UI Info page.
INCOMINGNAME	Name associated with first connected, ringing, or inbound call.
REMOTENUMBER	Phone number of first connected, ringing, or inbound call. If there are multiple calls, the data associated with the first call found will be provided.
DISPLAYNAMEn	The contents of the Line N Display Name configuration parameter.
AUTHIDn	The contents of the Line N auth ID configuration parameter.

Configure a Phone to Connect to an XML Application

Procedure

Step 1 In the Configuration Utility, select **Admin Login** > **advanced** > **Voice** > **Phone**.

Step 2 Enter this information:

- XML Application Service Name—Name of the XML application. Displays on the user's phone as a menu item.
- XML Application Service URL—URL where the XML application is located.

If you configure an unused line button to connect to an XML application, the button connects to the URL configured above. If this is not what you want, you need to enter a different URL when you configure the line button.

Step 3 Click **Submit All Changes**.

Configure a Phone to Connect to an XML Directory Service

Procedure

Step 1 In the Configuration Utility, select **Admin Login** > **advanced** > **Voice** > **Phone**.

Step 2 Enter this information:

- XML Directory Service Name—Name of the XML Directory. Displays on the user's phone as a directory choice.
- XML Directory Service URL—URL where the XML Directory is located.

Step 3 Click **Submit All Changes**.

CHAPTER 7

Cisco IP Conference Phone Features and Setup

Phone Features and Setup Overview

After you install Cisco IP Phones in your network, configure their network settings, and add them to Third-Party Call Control System, you must use the Third-Party Call Control System to configure telephony features, optionally modify phone templates, set up services, and assign users.

You can modify additional settings for the Cisco IP Phone from Third-Party Call Control Configuration Utility. Use this web-based application to set up phone registration criteria and calling search spaces, to configure corporate directories and services, and to modify phone button templates, among other tasks.

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
- List of features supported
- User guide or quick reference for your voicemail system

Telephony Features for Cisco IP Phone

After you add Cisco IP Phones to Third-Party Call Control system, you can add functionality to the phones. The following table includes a list of supported telephony features, many of which you can configure by using Third-Party Call Control system.

Note The Third-Party Call Control system also provides several service parameters that you can use to configure various telephony functions.

Feature	Description and More Information
AES 256 Encryption Support for Phones	Enhances security by supporting TLS 1.2 and new ciphers.
Alphanumeric Dialing	Allows users to place a call with alphanumeric characters. You can use these characters for alphanumeric dialing: a-z, A-Z, 0-9, -, _, ., and +.
Any Call Pickup	Allows users to pick up a call on any line in their call pickup group, regardless of how the call was routed to the phone.

Feature	Description and More Information
Auto Answer	Connects incoming calls automatically after a ring or two. Auto Answer works with either the speakerphone or the headset.
Blind Transfer	Blind Transfer: This transfer joins two established calls (call is in hold or in connected state) into one call and drops the feature initiator from the call. Blind Transfer does not initiate a consultation call and does not put the active call on hold. Some JTAPI/TAPI applications are not compatible with the Join and Blind Transfer feature implementation on the Cisco IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines.
Call Back	Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available.
Call Display Restrictions	Determines the information that will display for calling or connected lines, depending on the parties who are involved in the call. RPID and PAID caller id handling are supported.
Call Forward	Allows users to redirect incoming calls to another number. Call Forward options include Call Forward All, Call Forward Busy, Call Forward No Answer.
Call Forward Notification	Allows you to configure the information that the user sees when receiving a forwarded call.
Call History for Shared Line	Allows you to view shared line activity in the phone Call History. This feature will: • Log missed calls for a shared line • Log all answered and placed calls for a shared line
Call Park	Allows users to park (temporarily store) a call and then retrieve the call by using another phone.
Call Pickup	Allows users to redirect a call that is ringing on another phone within their pickup group to their phone. You can configure an audio and visual alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group.
Call Waiting	Indicates (and allows users to answer) an incoming call that rings while on another call. Incoming call information appears on the phone display.
Caller ID	Caller identification such as a phone number, name, or other descriptive text appear on the phone display.
Caller ID Blocking	Allows a user to block their phone number or name from phones that have caller identification enabled.

Feature	Description and More Information
Calling Party Normalization	Calling party normalization presents phone calls to the user with a dialable phone number. Any escape codes are added to the number so that the user can easily connect to the caller again. The dialable number is saved in the call history and can be saved in the Personal Address Book.
Conference	Allows a user to talk simultaneously with multiple parties by calling each participant individually. Allows a noninitiator in a standard (ad hoc) conference to add or remove participants; also allows any conference participant to join together two standard conferences on the same line. **Note** Be sure to inform your users whether these features are activated.
Configurable RTP/sRTP Port Range	Provides a configurable port range (2048 to 65535) for Real-Time Transport Protocol (RTP) and secure Real-Time Transport Protocol (sRTP). The default RTP and sRTP port range is 16384 to 16538. You configure the RTP and sRTP port range in the SIP Profile.
Directed Call Pickup	Allows a user to pick up a ringing call on a DN directly by pressing the GPickUp softkey and entering the directory number of the device that is ringing.
Divert	Allows a user to transfer a ringing, connected, or held call directly to a voice-messaging system. When a call is diverted, the line becomes available to make or receive new calls.
Do Not Disturb (DND)	When DND is turned on, either no audible rings occur during the ringing-in state of a call, or no audible or visual notifications of any type occur.
Headset Sidetone Control	Allows an administrator to set the sidetone level of a wired headset.
Group Call Pickup	Allows a user to answer a call that is ringing on a directory number in another group.
Hold Status	Enables phones with a shared line to distinguish between the local and remote lines that placed a call on hold.
Hold/Resume	Allows the user to move a connected call from an active state to a held state. • No configuration required unless you want to use Music On Hold. See “Music On Hold” in this table for information. • See “Hold Reversion” in this table.
HTTP Download	Enhances the file download process to the phone to use HTTP by default. If the HTTP download fails, the phone reverts to using the TFTP download.
HTTPS for Phone Services	Increases security by requiring communication using HTTPS. **Note** When the web is in HTTPS mode, the phone is a HTTPS servers.

Feature	Description and More Information
Improve Caller Name and Number Display	Improves the display of caller names and numbers. If the Caller Name is known then the Caller Number is displayed instead of unknown.
Jitter Buffer	The Jitter Buffer feature handles jitter from 10 milliseconds (ms) to 1000 ms for both audio and video streams.
Join Across Lines	Allows users to combine calls that are on multiple phone lines to create a conference call. Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines.
Join	Allows users to combine two calls that are on one line to create a conference call and remain on the call.
Message Waiting	Defines directory numbers for message waiting on and off indicators. A directly-connected voice-message system uses the specified directory number to set or to clear a message waiting indication for a particular Cisco IP Phone.
Message Waiting Indicator	A light on the handset that indicates that a user has one or more new voice messages.
Minimum Ring Volume	Sets a minimum ringer volume level for an IP phone.
Missed Call Logging	Allows a user to specify whether missed calls will be logged in the missed calls directory for a given line appearance.
Multicasting Paging	Enables users to page some or all phones. If the phone is on an active call while a group page starts, the incoming page is ignored.
Multiple Calls Per Line Appearance	Each line can support multiple calls. By default, the phone supports two active calls per line, and a maximum of ten active calls per line. Only one call can be connected at any time; other calls are automatically placed on hold. The system allows you to configure maximum calls/busy trigger not more than 10/6. Any configuration more than 10/6 is not officially supported.
Music On Hold	Plays music while callers are on hold.
Mute	Mutes the handset or headset microphone.
No Alert Name	Makes it easier for end users to identify transferred calls by displaying the original caller's phone number. The call appears as an Alert Call followed by the caller's telephone number.
Onhook Dialing	Allows a user to dial a number without going off hook. The user can then either pick up the handset or press Dial.

Feature	Description and More Information
Pause in Speed Dial	Users can set up the speed-dial feature to reach destinations that require Forced Authorization Code (FAC) or Client Matter Code (CMC), dialing pauses, and additional digits (such as a user extension, a meeting access code, or a voicemail password) without manual intervention. When the user presses the speed dial, the phone establishes the call to the specified DN and sends the specified FAC, CMC, and DTMF digits to the destination and inserts the necessary dialing pauses.
Plus Dialing	Allows the user to dial E.164 numbers prefixed with a plus (+) sign. To dial the + sign, the user needs to press and hold the star (*) key for at least 1 second. This applies to dialing the first digit for an on-hook (including edit mode) or off-hook call.
Power Negotiation over LLDP	Allows the phone to negotiate power using Link Level Endpoint Discovery Protocol (LLDP) and Cisco Discovery Protocol (CDP).
Problem Reporting Tool	Submits phone logs or reports problems to an administrator.
Programmable Feature Buttons	You can assign features, such as New Call, Call Back, and Forward All to line buttons.
Redial	Allows users to call the most recently dialed phone number by pressing a button or the Redial softkey.
Remote Customization (RC)	Allows a service provider to customize the phone remotely. There is no need for either the service provider to physically touch the phone or a user to configure the phone. The service provider can work with a sales engineer at the time of ordering to set this up.
Ringtone Setting	Identifies ring type used for a line when a phone has another active call.
RTCP Hold For SIP	Ensures that held calls are not dropped by the gateway. The gateway checks the status of the RTCP port to determine if a call is active or not. By keeping the phone port open, the gateway will not end held calls.
Serviceability for SIP Endpoints	Enables administrators to quickly and easily gather debug information from phones. This feature uses SSH to remotely access each IP phone. SSH must be enabled on each phone for this feature to function.
Shared Line	Allows a user with multiple phones to share the same phone number or allows a user to share a phone number with a coworker.
Show Calling ID and Calling Number	The phones can display both the calling ID and calling number for incoming calls. The IP phone LCD display size limits the length of the calling ID and the calling number that display. The Show Calling ID and Calling Number feature applies to the incoming call alert only and does not change the function of the Call Forward and Hunt Group features. See "Caller ID" in this table.

Feature	Description and More Information
Show Duration for Call History	Displays the time duration of placed and received calls in the Call History details. If the duration is greater than or equal to one hour, the time is displayed in the Hour, Minute, Second (HH:MM:SS) format. If the duration is less than one hour, the time is displayed in the Minute, Second (MM:SS) format. If the duration is less than one minute, the time is displayed in the Second (SS) format.
Speed Dial	Dials a specified number that has been previously stored.
Time Zone Update	Updates the Cisco IP Phone with time zone changes.
Transfer	Allows users to redirect connected calls from their phones to another number. Some JTAPI/TAPI applications are not compatible with the Join and Direct Transfer feature implementation on the Cisco IP Phone and you may need to configure the Join and Direct Transfer Policy to disable join and direct transfer on the same line or possibly across lines.
Voice Message System	Enables callers to leave messages if calls are unanswered.
Web Access Enable by Default	Web services are enabled by default.

Feature Buttons and Softkeys

The following table provides information about features that are available on softkeys, features that are available on dedicated feature buttons, and features that you need to configure as programmable feature buttons. An “X” in the table indicates that the feature is supported for the corresponding button type or softkey. Of the two button types and softkeys, only programmable feature buttons require configuration in Cisco IP Phone administration.

Table 7: Features with Corresponding Buttons and Softkeys

Feature Name	Dedicated Feature Button	Programmable Feature Button	Softkey
Answer		X	X
Call Forward All		X	X
Call Park		X	X
Call Park Line Status		X	
Call Pickup (Pick Up)		X	X
Call Pickup Line Status		X	

Feature Name	Dedicated Feature Button	Programmable Feature Button	Softkey
Conference	X		X (only displayed during connected call conference scenario)
Divert			X
Do Not Disturb		X	X
Hold	X		X
Mute	X		
PLK Support for Queue Status		X	X
Redial		X	X
Speed Dial		X	X
Speed Dial Line Status		X	
Transfer	X		X (only displayed during connected call transfer scenario)

Configure a Speed Dial with the Configuration Utility Page

You can configure speed dials on the phone with the web interface.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **Voice** > **User**.

Step 2 In the **Speed Dial** section, enter a name and number that corresponds to the speed dial entry.

Step 3 Click **Submit All Changes**.

Speed Dial

Parameter	Description
Speed Dial Name	Indicates the name given to the speed dial.

Parameter	Description
Speed Dial Number	Indicates the number allocated to the speed dial.

Enable Conference Button with a Star Code

You can add a star code to the Conference button so that your user can press the button only once to add many active calls to a conference. You can enable this feature from the phone web page.

Before You Begin

The phone server must suppport this feature.

Procedure

Step 1 On the phone web page, select **Admin Login** > **Advanced** > **Voice** > **Ext(n)**, where n is an extension number.

Step 2 In the **Call Features Settings** section, select **Yes** for the **Conference Single Hardkey** field, enter a star code in the **Conference Bridge URL**, and press **Submit All Changes**. For example, you can enter *55 to represent the conference bridge URL of a telecom service provider.
You can also enable conference button with a xml file. Enter a string in this format:

```
<Conference_Bridge_URL_1_ ua="na">*55</Conference_Bridge_URL_1_>
```

```
<Conference_Single_Hardkey_1_ ua="na">Yes</Conference_Single_Hardkey_1_>
```

Configure Alphanumeric Dialing

You can configure a phone so that the user of the phone can make a call by dialing alphanumeric characters instead of dialing only digits. In the configuration utility page, you can configure alphanumeric dialing with speed-dial, blf, and call pickup.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **Advanced** > **Voice** > **Ext**.

Step 2 In the **Enable URI Dialing 1**, select **Yes** to enable alphanumeric dialing.
In the phone page, you can add a string on a line key in this format to enable speed dial with alphanumeric dialing capability:

fnc=sd;ext=xxxx.yyyy@$PROXY;nme=yyyy,xxxx

For example:

fnc=sd;ext=first.last@$PROXY;nme=Last,First
The above example will enable the user to dial "first.dial" to make a call.

Note The supported characters that you can use for alphanumeric dialing are a-z, A-Z, 0-9, -, _, ., and +.

.

Step 3 Click **Submit All Changes**.

Configure a Paging Group (Multicast Paging)

You can configure multicast paging so that users can page all the phones at once or page a group of phones without involving a server. On the Configuration Utility page, you configure a phone as a part of a paging group and can subscribe them to the same multicast address. This enables users to direct pages to specific groups of phones. When you assign each paging group with a unique number, the user dials the paging group number to start paging. All phones that are subscribed to the same multicast address (also configured on the Configuration Utility page) receive the page. The user hears a paging tone of three short beeps when there is an incoming paging call.

Keep these things in mind:

- Your network must support multicasting so that all devices in the same paging group are able to join the corresponding multicast group.
- If the phone is on an active call when a group page starts, the incoming page is ignored.
- Group paging is one way and uses the G711 codec. The paged phone can only listen to the call from the originator.
- Incoming pages are ignored when DND is enabled.
- When paging occurs, the speaker on the paged phones automatically powers on unless the handset or the headset is in use.
- If the phone is on an active call when a group page starts, the incoming page is ignored. When the call ends, the page is answered, if the page is active.
- When multiple pages occur, the pages are answered in chronological order. Until the active page ends, the next page is not answered.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **Advanced** > **Voice** > **Phone**.

Step 2 In the **Multiple Paging Group Parameters** section, enter a string in the **Group Paging Script** field in this format:
pggrp=multicast-address:port;[name=xxxx;]num=yyy;[listen={yes|no}]];

where:

- multicast-address = Multicast IP address of the phone that listens for and receives pages.
- port = Port on which to page; you must use different ports for each paging group.
- name (optional) = xxxx is the name of the paging group. Replace xxxx with a name. The name can consist maximum of 64 characters.
- num= yyy is a unique number that the user dials to access the paging group. Replace yyy with a number. The number can consist maximum of 64 characters and the allowed range is 1024 to 32767.

- listen = Indicates whether the phone listens on the page group. Only the first two groups with listen set to yes listen to group pages. If the field is not defined, the default value is no, so you must set this field to listen to the group pages.

You can add more paging groups by appending to the configuration string. Here is an example.

```
pggrp=224.168.168.168:34560;name=All;num=500;listen=yes;
pggrp=224.168.168.168:34562;name=GroupA;num=501;listen=yes;
pggrp=224.168.168.168:34564;name=GroupB;num=502;
pggrp=224.168.168.168:34566;name=GroupC;num=503;
```

This example creates four paging groups: All, GroupA, GroupB, and GroupC. Users dial 500 to send pages to all phones, 501 to send pages to phones configured as part of the GroupA group, 502 to send pages to phones configured as part of the GroupB group, and 503 to send pages to phones configured as part of the GroupC group. The configured phone receives pages directed to the groups All and GroupA.

Step 3 Click **Submit All Changes**.

Configuring Programmable Softkeys

You can customize the softkeys displayed on the phone. The default softkeys (when the phone is in an idle state) are Redial, Directory, Call Forward, and Do Not Disturb. Other softkeys are available during specific call states (for example, if a call is on hold, the Resume softkey displays).

Procedure

Step 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**

Step 2 Under **Programmable Softkeys**, edit the softkeys depending on the call state that you want the softkey to display. For more information, see Programmable Softkeys, on page 156.

In the Programmable Softkeys section, each phone state is displayed and the softkeys that are available to display during that state are listed. Each softkey is separated by a semicolon. Softkeys are shown in the format:

```
softkeyname  |[  position  ]
```

where softkeyname is the name of the key and position is where the key is displayed on the IP phone screen. Positions are numbered, with position one displayed on the lower left of the IP phone screen, followed by positions two through four. Additional positions (over four) are accessed by pressing the right arrow key on the phone. If no position is given for a softkey, the key will float and appears in the first available empty position on the IP phone screen.

Step 3 Click **Submit All Changes**.

Customize a Programmable Softkey

The phone provides sixteen programmable softkeys (fields PSK1 through PSK16). You can define the fields by a speed-dial script.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **advanced** > **Voice** > **Phone**.

Step 2 In the **Programmable Softkeys** section, set the **Programmable Softkey Enable** to **Yes**.

Step 3 Select a programmable softkey number field on which to configure a phone feature.

Step 4 Enter the string for the programmable soft key. See the different types of programmable softkeys described in Configure Speed Dial on a Programmable Softkey, on page 88.

Step 5 Click **Submit All Changes**.

Configure Speed Dial on a Programmable Softkey

You can configure programmable softkeys as speed dials. The speed dials can be extensions or phone numbers. You can also configure programmable softkeys with speed dials that perform an action that a vertical service activation code (or a star [*] code) defines. For example, if you configure a programmable softkey with a speed dial for *67, the call is placed on hold.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **advanced** > **Voice** > **Phone**.

Step 2 In the **Programmable Softkeys** section, set the **Programmable Softkey Enable** to **Yes**.

Step 3 To configure a speed dial PSK, enter the following in the PSK **number** field:

```
fnc=sd;ext=extensionname/starcode@$PROXY;vid=n;nme=name
```

Where:

- fnc= function of the key (speed dial)
- extensionname=extension being dialed or the star code action to perform
- vid= n is the extension that the speed dial will dial out
- name is the name of the speed dial being configured

Note The **name** field displays on the softkey on the IP phone screen. We recommend a maximum of 10 characters for a phone. If more characters are used, the label might be truncated on the phone screen.

Step 4 Edit the following:

- **Idle Key List:** Edit the field as described in the following example:

  ```
  redial|1;newcall|2;dnd;psk1
  ```

  If the user incorrectly configures the programmable softkey list features on the phone, the key list on the phone LCD does not update. For example:

  - If a user enters rdeial;newcall;cfwd (redial has been misspelt), the key list is not updated and the user does not see any change on the LCD.

- If a user enters redial;newcall;cfwd;delchar, the user will not see a change on the LCD, as the delchar softkey is not allowed in the **Idle Key List**. Hence, this is an incorrect configuration of the programmable softkey list.

- **PSK1:**

```
fnc=sd;ext=5014@$PROXY;nme=sktest1
```

Note In this example, we are configuring a softkey on a phone as a speed dial number for extension 5014 (sktest1).

You can also configure an XML service on the programmable soft key. Enter the string in this format:

```
fnc=xml;url=http://xml.service.url;nme=name
```

Step 5 Click **Submit All Changes**.

Programmable Softkeys for Braavos

The following softkey lists have been updated for Braavos.

Keyword	Key Label	Definition	Available Phone States
acd_login	Agt signin	Logs user in to Automatic Call Distribution (ACD).	Idle
acd_logout	AgtSignOut	Logs user out of ACD.	Idle
answer	Answer	Answers an incoming call.	Ringing
astate	Agt Status	Checks the ACD status.	Idle
avail	Avail	Denotes that a user who is logged in to an ACD server has set his status as available.	Idle
barge	Barge	Allows another user to interrupt a shared call.	Shared-Active, Shared-Held
bargesilent	BargeSilent	Allows another user to interrupt a shared call with the mic disabled.	Shared-Active

Keyword	Key Label	Definition	Available Phone States
bxfer	BlindXfer	Performs a blind call transfer (transfers a call without speaking to the party to whom the call is transferred). Requires that Blind Xfer Serv is enabled.	Connected
call (or dial)	Call	Calls the selected item in a list.	Dialing Input
cancel	Cancel	Cancels a call (for example, when conferencing a call and the second party is not answering.	Off-Hook
cfwd	Forward / Clr fwd	Forwards all calls to a specified number.	Idle, Off-Hook, Shared-Active, Hold, Shared-Held
conf	Conference	Initiates a conference call. Requires that Conf Server is enabled and there are two or more calls that are active or on hold.	Connected
confLx	Conf line	Conferences active lines on the phone. Requires that Conf Serv is enabled and there are two or more calls that are active or on hold.	Connected
delchar	delChar - backspace Icon	Deletes a character when entering text.	Dialing Input
dir	Contacts	Provides access to phone directories.	Idle, Miss, Off-Hook (no input), Connected, Start-Xfer, Start-Conf, Conferencing, Hold, Ringing, Shared-Active, Shared-Held
dnd	DND / Clr Dnd	Sets Do Not Disturb to prevent calls from ringing the phone.	Idle, Off-Hook, Hold, Shared-Active, Shared-Held, Conferencing, Start-Conf, Start-Xfer

Keyword	Key Label	Definition	Available Phone States
em_login (or signin)	Sign in	Logs user in to Extension Mobility.	Idle
em_logout (or signout)	Sign out	Logs user out of Extension Mobility.	Idle
endcall	End call	Ends a call.	Connected, Start-Xfer, Start-Conf, Conferencing, Hold
favorites	Favorites	Provides access to "Speed Dials".	Idle, Miss, Off-Hook (no input), Connected, Start-Xfer, Start-Conf, Conferencing, Hold, Ringing, Shared-Active, Shared-Held
gpickup	GrPickup	Allows user to answer a call ringing on an extension by discovering the number of the ringing extension.	Idle, Off-Hook
hold	Hold	Put a call on Hold.	Connected, Start-Xfer, Start-Conf, Conferencing
ignore	Decline	Ignores an incoming call.	Ringing
join	Join	Connects a conference call. If the conference host is user A and users B & C are participants, when A presses "Join", A will drop off and users B & C will be connected.	Conferencing
lcr	Call Rtn/lcr	Returns the last missed call.	Idle, Missed-Call,Off-Hook (no input)
left	Left arrow icon	Moves the cursor to the left.	Dialing Input
messages	Messages	Provides access to voicemail.	Idle, Miss, Off-Hook (no input), Connected, Start-Xfer, Start-Conf, Conferencing, Hold, Ringing, Shared-Active, Shared-Held

Keyword	Key Label	Definition	Available Phone States
miss	Miss	Displays the list of missed calls.	Missed-Call
newcall	New Call	Begins a new call.	Idle, Hold, Shared-Active, Shared-Held
option	Option	Opens a menu of input options.	Off-Hook
park	Park	Puts a call on hold at a designated "park" number.	Connected
phold	PrivHold	Puts a call on hold on an active shared line.	Connected
pickup	PickUp	Allows a user to answer a call ringing on another extension by entering the extension number.	Idle, Off-Hook
recents	Recents	Displays the All calls list from call history.	Idle, Off-Hook, Hold, Shared-Active, Shared-Held
redial	Redial	Displays the redial list.	Idle, Connected, Start-Conf, Start-Xfer, Off-Hook (no input), Hold
resume	Resume	Resumes a call that is on hold.	Hold, Shared-Held
right	Right arrow icon	Moves the cursor to the right.	Dialing (input)
settings	Settings	Provides access to "Information and Settings".	All
starcode	Input Star Code/*code	Displays a list of star codes that can be selected.	Off-Hook, Dialing (input)
unavail	Unavail	Denotes that a user who is logged in to an ACD server has set his status as unavailable.	Idle

Keyword	Key Label	Definition	Available Phone States
unpark	Unpark	Resumes a parked call.	Idle, Off-Hook, Connected, Shared-Active
xfer	Transfer	Performs a call transfer. Requires that Attn Xfer Serv is enabled and there is at least one connected call and one idle call.	Connected, Start-Xfer, Start-Conf
xferlx	Xfer line	Transfers an active line on the phone to a called number. Requires that Attn Xfer Serv is enabled and there are two or more calls that are active or on hold.	Connected

Configure Provisioning Authority

You can set up provisioning authority so that users can access their personalized phone settings from other phones. For example, people who work different shifts or who work at different desks during the week can share an extension, yet have their own personalized settings.

The **Sign in** softkey appears on the phone when you enable provisioning authority on the phone. Users enter their usernames and passwords to access their personal phone settings. Users can also ignore the sign-in and use the phone as a guest. After signing on, users have access to their personal directory numbers on the phone. When the user signs out, the phone reverts to a basic profile with limited features.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **advanced** > **Voice** > **Provisioning**.

Step 2 In the **Configuration Profile** section, set the **Profile Rule** field to the phone configuration file's URL.

Example:
http://192.0.2.1:80/dms/CP-8851-3PCC/8851System.xml
The **EM Enable** and **EM User Domain** fields are filled in, based on the information provided in the phone configuration file.

Step 3 In the **Extension Mobility** section, set the amount of time (in minutes) that the phone can be inactive before it automatically signs out from the provisioning authority in **Inactivity timer(m)**.
To access **Extension Mobility** section, select **Admin Login** > **advanced** > **Voice** > **Phone**.

Step 4 Set the amount of time (in seconds) that the user has to cancel the sign-out in **Countdown Timer(s)**.

Step 5 (Optional) If the **Programmable Softkey Enable** field in the **Programmable Softkeys** section is set to **Yes**, add signin to **Idle Key List**.

Example:

newcall|1;signin|2

Step 6 Click **Submit All Changes**.

Configure Provisioning Authority in the Phone Configuration File

You can enable provisioning authority in the default configuration file for your phones, so that you don't need to set up the feature manually for each phone.

Procedure

Step 1 In the phone configuration file, set the following parameters:

a) Set the Provisioning Authority profile rules in the **Profile_Rule** parameters.

Example:

```
<Profile_Rule ua="na">("$EMS" eq "mobile" and "$MUID" ne "" and "$MPWD" ne "")?[--uid
$MUID$PDOM --pwd $MPWD]
http://10.74.121.51:80/dms/CP-8851-3PCC/8851System.xml|http://10.74.121.51:80/dms/CP-8851-3PCC/8851System.xml</Profile_Rule>
```

b) Set the **EM_Enable** parameter to Yes.

Example:

```
<EM_Enable ua="na">Yes</EM_Enable>
```

c) Enter the enter the domain for the phone, or the authentication server in the **EM_User_Domain** parameter.

Example:

```
<EM_User_Domain ua="na">@10.74.121.51</EM_User_Domain>
```

Step 2 Save the configuration file and upload it to your provisioning server.

Step 3 On the Configuration Utility page, select **Admin Login** > **advanced** > **Voice** > **Provisioning**.

Step 4 Enter the filepath to the configuration file in one of the **Profile Rule** fields.

Example:

http://<SERVER IP ADDRESS>:80/dms/td_8861/8861System.xml

Step 5 Click **Submit All Changes**.

Enable Hoteling on a Phone

You can allow users to sign into phones as guests. This is called hoteling.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **advanced** > **Voice** > **Ext [n]** (where [n] is the extension number).

Step 2 In the **Call Feature Settings** section, set **Enable Broadsoft Hoteling** to **Yes**.

Step 3 Set the amount of time (in seconds) that the user can be signed in as a guest on the phone in **Hoteling Subscription Expires**.

Step 4 Click **Submit All Changes**.

Set User Password

Users can set their own password on their phones, or you can set a password for them.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **advanced** > **Voice** > **System**.

Step 2 Set a password in the **User Password** field.

Step 3 Click **Submit All Changes**.

Download Problem Reporting Tool Logs

Users submit problem reports to you with the Problem Reporting Tool.

If you are working with Cisco TAC to troubleshoot a problem, they typically require the logs from the Problem Reporting Tool to help resolve the issue.

To issue a problem report, users access the Problem Reporting Tool and provide the date and time that the problem occurred, and a description of the problem. You need to download the problem report from the Configuration Utility page.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **Info** > **Debug Info** > **Device Logs**.

Step 2 In the **Problem Reports** area, click the problem report file to download.

Step 3 Save the file to your local system and open the file to access the problem reporting logs.

Configure PRT Upload

You must use a server with an upload script to receive the problem reports that the user sends from the phone.

- If the URL specified in the **PRT Upload Rule** field is valid, users get a notification alert on the phone UI saying that they have successfully submitted the problem report.
- If the **PRT Upload Rule** field is empty or has an invalid URL, users get a notification alert on the phone UI saying that the data upload failed.

The phone uses an HTTP/HTTPS POST mechanism, with parameters similar to an HTTP form-based upload. The following parameters are included in the upload (utilizing multipart MIME encoding):

- devicename (example: "SEP001122334455")
- serialno (example: "FCH12345ABC")
- username (The user name is either the **Station Display Name** or the **User ID** of the extension. The **Station Display Name** is first considered. If this field is empty, then the **User ID** is chosen.)
- prt_file (example: "probrep-20141021-162840.tar.gz")

A sample script is shown below. This script is provided for reference only. Cisco does not provide support for the upload script installed on a customer's server.

```
<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used:  upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, "'\"");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "'\"");

$username = $_POST['username'];
$username = trim($username, "'\"");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
        header("HTTP/1.0 500 Internal Server Error");
        die("Error: You must select a file to upload.");
}

?>
```

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **advanced** > **Voice** > **Provisioning**.

Step 2 In the **Problem Report Tool** section, enter the path to the PRT upload script in the **PRT Upload Rule** field.

Example:
https://proxy.example.com/prt_upload.php

or

http://proxy.example.com/prt_upload.php

Step 3 Use the **PRT Upload Method** drop-down list box to choose the upload method:

- POST
- PUT

Step 4 Click **Submit All Changes**.

Configure a Phone to Accept Pages Automatically

The Single Paging or Intercom feature enables a user to directly contact another user by phone. If the phone of the person being paged has been configured to accept pages automatically, the phone does not ring. Instead, a direct connection between the two phones is automatically established when paging is initiated.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **advanced** > **Voice** > **User**.
Step 2 In the **Supplementary Services** section, choose **Yes** for the **Auto Answer Page** field.
Step 3 Click **Submit All Changes**.

Server-Configured Paging

You can configure a paging group on a server so that users can page a group of phones. For more details, refer to your server documentation.

Manage Phones with TR-069

You can use the protocols and standards defined in Technical Report 069 (TR-069) to manage phones. TR-069 explains the common platform for management of all phones and other customer-premises equipment (CPE) in large-scale deployments. The platform is independent of phone types and manufacturers.

As a bidirectional SOAP/HTTP-based protocol, TR-069 provides the communication between CPEs and Auto Configuration Servers (ACS).

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **advanced** > **Voice** > **TR-069**.

Step 2 Set up the fields as described in theTR-069, on page 171 table.

Step 3 Click **Submit All Changes**.

View TR-069 Status

When you enable TR-069 on a user phone, you can view status of TR-069 parameters on the Configuration page.

Procedure

On the Configuration Utility page, select **Admin Login** > **advanced** > **Info** > **Status** > **TR-069 Status**.
You can view status of TR-069 parameters in the TR-069 Status, on page 116 table.

Report All Phone Issues with the Configuration Utlility

If you are working with Cisco TAC to troubleshoot a problem, they typically require the logs from the Problem Reporting Tool to help resolve the issue. You can generate PRT logs using the Configuration Utlility and upload them to a remote log server.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **advanced** > **Info** > **Debug Info**.

Step 2 In the **Problem Reports** section, click **Generate PRT**.
The **Report Problem** dialog appears.

Step 3 Enter the following information in the **Report Problem** dialog:

a) Enter the date that you experienced the problem in the **Date** field. The current date appears in this field by default.
b) Enter the time that you experienced the problem in the **Time** field. The current time appears in this field by default.
c) In the **Select Problem** drop-down list box, choose the description of the problem from the available options.

Step 4 Click **Submit** in the **Report Problem** dialog.
The Submit button is enabled only if you select a value in the **Select Problem** drop-down list box.

You get a notification alert on the Configuration Utility page that indicates if the PRT upload was successful or not.

Identify Phone Issues with a URL in the Phone Web Page

When the phone is not working or doesn't register, a network error or any misconfiguration might be the cause. To identify the cause, add a specific IP address or a domain name to the phone admin page. Then, try to access so that the phone can ping the destination and display the cause.

Procedure

In a supported web browser, enter a URL that consist of your phone IP address and the destination IP that you want to ping.
Enter a URL in the format:

```
http:/<Phone IP>/admin/ping?<ping destination>
```

where:

Phone IP = actual IP address of your phone.

/admin = path to access admin page of your phone.

ping destination = any IP address or domain name that you want to ping. Only alphanumeric characters, '-', and "_" are allowed as the ping destination. Otherwise the phone shows an error on the web page. If the <ping destination> includes spaces, only the first part of the address is used as the pinging destination. For example, "http://<Phone IP>/admin/ping?192.168.1.1 cisco.com" will actually ping 192.168.1.1.

Factory Reset the Phone from Phone Web Page

You can restore your phone to its original manufacturer settings so that the phone can be reconfigured, do it from the phone web page.

Procedure

Enter the URL in a supported web browser and click **Confirm Factory Reset**.
You can enter URL in the format:

```
http://<Phone IP>/admin/factory-reset
```

where:

Phone IP = actual IP address of your phone.

/admin = path to access admin page of your phone.

factory-reset = command that you need to enter in the phone web page to factory-reset your phone.

CHAPTER 8

Corporate and Personal Directory Setup

Personal Directory Setup

The Personal Directory allows a user to store a set of personal numbers.

Personal Directory consists of the following feature:

- Personal Address Book (PAB)

Users can use these methods to access Personal Directory features:

- From a web browser: Users can access the PAB and Speed Dials features from the Configuration Utility web page.
- From the Cisco IP Phone: Choose Contacts to search the corporate directory or the user personal directory.

To configure Personal Directory from a web browser, users must access their Configuration Utility. You must provide users with a URL and sign-in information.

LDAP Configuration

The Cisco IP Phone supports Lightweight Directory Access Protocol (LDAP) v3. LDAP Corporate Directory Search allows a user to search a specified LDAP directory for a name, phone number, or both. LDAP-based directories, such as Microsoft Active Directory 2003 and OpenLDAP-based databases, are supported.

Users access LDAP from the **Directory** menu on their IP phone. An LDAP search returns up to 20 records.

The instructions in this section assume that you have the following equipment and services:

- An LDAP server, such as OpenLDAP or Microsoft Active Directory Server 2003.

Prepare the LDAP Corporate Directory Search

Procedure

Step 1 Click **Admin Login** > **advanced** > **Voice** > **System**.

Step 2 In the **IPv4 Settings** section, in the **Primary DNS** field, enter the IP address of the DNS server.
This step is required only if you are using Active Directory with authentication set to MD5.

Step 3 In the **Optional Network Configuration** section, in the **Domain** field, enter the LDAP domain.
This step is required only if you are using Active Directory with authentication set to MD5.

Some sites might not deploy DNS internally and instead use Active Directory 2003. In this case, it is not necessary to enter a Primary DNS address and an LDAP Domain. However, with Active Directory 2003, the authentication method is restricted to Simple.

Step 4 Click the **Phone** tab.

Step 5 In the **LDAP** section, use the **LDAP Dir Enable** drop-down list box to choose **Yes**.
This action enables LDAP and causes the name that is defined in the **Corp Dir Name** field to appear in the phone directory.

Step 6 Configure the LDAP fields. See the LDAP, on page 153

Step 7 Click **Submit All Changes**.

Configure the BroadSoft Settings

The BroadSoft directory service enables users to search and view their personal, group, or enterprise contacts. This application feature uses BroadSoft's Extended Services Interface (XSI).

To improve security, the phone firmware places access restrictions on the host server and directory name entry fields.

The following table describes the access restrictions that apply to the BroadSoft settings:

Field	Access Restriction
Directory Name	Admin password is required (if set)
XSI Host Server	Admin password is required (if set)
Directory Type	Enterprise/Group/Personal
Directory User ID	None
Directory Password	None

Procedure

Step 1 Click **Admin Login** > **advanced** > **Voice** > **Phone**.

Step 2 In the **Broadsoft Settings** section, choose **Yes** from the **Directory Enable** drop down list box.

Step 3 In the **XSI Host Server** field, enter the name of server.

Step 4 In the **Directory Name** field, enter the name of directory.

Step 5 In the **Directory Type** field, choose the type of BroadSoft directory from the drop down list.

Step 6 In the **Directory User ID** field, enter the BroadSoft user id of the phone user.

Step 7 In the **Directory Password** field, enter the password.

Step 8 Click **Submit All Changes**.

Configure the XML Directory Service

Procedure

Step 1 In the Configuration Utility page, click **Admin Login** > **advanced** > **Voice** > **Phone**.

Step 2 In the **XML Directory Service Name** field, enter the name of XML directory.

Step 3 In the **XML Directory Service URL** field, enter the url where XML directory is located.

Step 4 In the **XML User Name** field, enter the username of XML service.

Step 5 In the **XML Password** field, enter the password of XML service.

Step 6 Click **Submit All Changes**.

PART IV

Cisco IP Phone Troubleshooting

CHAPTER 9

Monitoring Phone Systems

Monitoring Phone Systems Overview

You can view a variety of information about the phone using the phone status menu on the phone and the phone web pages. This information includes:

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

This chapter 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.

Related Topics

Troubleshooting , on page 175

Cisco IP Phone Status

The following sections describes how to view model information, status messages, and network statistics on the Cisco IP Phone.

- Model Information: 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 that displays 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.

Display the Phone Information Window

Procedure

Step 1 Press **Settings** softkey.

Step 2 Select **Status** > **Product Information**.
When a user password is set, a corresponding icon (lock or certificate) displays at the top-right corner of the phone screen.

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

View the Phone Status

Procedure

Step 1 Press **Settings** softkey.

Step 2 Select **Status** > **Phone Status**.
You can view the following information:

- **Elapsed time—**Total time elapsed since the last reboot of the system
- **Tx (Packets)—**Transmitted packets from the phone.
- **Rx (Packets)—**Received packets from the phone.

View the Status Messages on the Phone

Procedure

Step 1 Press **Settings** softkey.

Step 2 Select **Information and settings** > **Status** > **Status messages**.
You can view a log of the various phone statuses since provisioning was last done.

Note Status messages reflect UTC time and are not affected by the timezone settings on the phone.

Step 3 Press **Back**.

View the Network Status

Procedure

Step 1 Press **Settings** softkey.

Step 2 Select **Status** > **Network Status**.
You can view the following information:

- **Network type—**Indicates the type of Local Area Netwrok (LAN) connection that the phone uses.
- **Network status—**Indicates if the phone is connected to a network.
- **IP address—**IP address of the phone.
- **VLAN ID—**VLAN ID of the phone.
- **Addressing type—**Indicates if the phone has DHCP or Static IP enabled.
- **IP status—**Status of IP that the phone uses.
- **Subnet mask—**Subnet mask used by the phone.
- **Default router—**Default router used by the phone.
- **DNS 1—**Primary Domain Name System (DNS) server that the phone uses.
- **DNS 2—**Optional Backup DNS server that the phone uses.
- **MAC address—**Unique Media Access Control (MAC) address of the phone.
- **Host name—**Displays the current host name assigned to the phone.
- **Domain—**Displays the network domain name of the phone. Default: cisco.com
- **Switch port link—**Status of the switch port.
- **Switch port config—**Indicates speed and duplex of the network port.

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 that are not available on the phone.

A single call can use 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, follow these steps:

Procedure

Step 1 Press **Settings** softkey.

Step 2 Select **Status** > **Phone Status** > **Call Statistics**.

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

Call Statistics Fields

The following table describes the items on the Call Statistics screen.

Table 8: Call Statistics Items for the Cisco IP Phone

Item	Description
Receiver Codec	Type of received voice stream (RTP streaming audio from codec): G.729, G.722, G.711 mu-law, G.711 A-law, OPUS, and iLBC.
Sender Codec	Type of transmitted voice stream (RTP streaming audio from codec): G.729, G.722, G.711 mu-law, G.711 A-law, OPUS, and iLBC.
Receiver Size	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).
Sender Size	Size of voice packets, in milliseconds, in the transmitting voice stream.
Rcvr Packets	Number of RTP voice packets that were received since voice stream opened. **Note** This number is not necessarily identical to the number of RTP voice packets that were received since the call began because the call might have been placed on hold.
Sender Packets	Number of RTP voice packets that were transmitted since voice stream opened. **Note** This number is not necessarily identical to the number of RTP voice packets that were transmitted since the call began because the call might have been placed on hold.
Avg Jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network), in milliseconds, that was observed since the receiving voice stream opened.

Item	Description
Max Jitter	Maximum jitter, in milliseconds, that was observed since the receiving voice stream opened.
Receiver Discarded	Number of RTP packets in the receiving voice stream that were discarded (bad packets, too late, and so on). **Note** The phone discards payload type 19 comfort noise packets that Cisco Gateways generate, because they increment this counter.
Rcvr Lost Packets	Missing RTP packets (lost in transit).
Voice-Quality Metrics	
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames that were received from start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
Conceal Seconds	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Seconds	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.

Cisco IP Phone Web Page

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.

Related Topics

Access the Web-Based Configuration Utility, on page 52
Determine the IP Address of the Phone, on page 52
Allow Web Access to the Cisco IP Phone, on page 53

Info

The fields on this tab are read-only and cannot be edited.

Status

System Information

Parameter	Description
Host Name	Displays the current host name assigned to the phone.
Domain	Displays the network domain name of the phone. Default: cisco.com
Primary NTP Server	Displays the primary NTP server assigned to the phone.
Secondary NTP Serve	Displays the secondary NTP server assigned to the phone.

IPv4 Information

Parameter	Description
IP Status	Indicates that the connection is established.
Connection Type	Indicates the type of internet connection for the phone: • DHCP • Static IP
Current IP	Displays the current IP address assigned to the IP phone.
Current Netmask	Displays the network mask assigned to the phone.
Current Gateway	Displays the default router assigned to the phone.
Primary DNS	Displays the primary DNS server assigned to the phone.
Secondary DNS	Displays the secondary DNS server assigned to the phone.

Reboot History

For information about Reboot History, see the Reboot Reasons, on page 190.

Product Information

Parameter	Description
Product Name	Model number of the Cisco IP Phone.
Software Version	Version number of the Cisco IP Phone firmware.
MAC Address	Hardware address of the Cisco IP Phone.

Parameter	Description
Customization	For an RC unit, this field indicates whether the unit has been customized or not. Pending indicates a new RC unit that is ready for provisioning. If the unit has already retrieved its customized profile, this field displays the name of the company that provisioned the unit.
Serial Number	Serial number of the Cisco IP Phone.
Hardware Version	Version number of the Cisco IP Phone hardware.
Client Certificate	Status of the client certificate, which authenticates the Cisco IP Phone for use in the ITSP network. This field indicates if the client certificate is properly installed in the phone.

Downloaded Locale Package

Parameter	Description
Download Status	Displays the downloaded locale package status.
Download URL	Displays the location from where the local package is downloaded.

Phone Status

Parameter	Description
Current Time	Current date and time of the system; for example, 08/06/14 1:42:56 a.m.
Elapsed Time	Total time elapsed since the last reboot of the system; for example, 7 days, 02:13:02.
SIP Messages Sent	Total number of SIP messages sent (including retransmissions).
SIP Bytes Sent	Total number of SIP messages received (including retransmissions).
SIP Messages Recv	Total number of bytes of SIP messages sent which includes retransmissions.
SIP Bytes Recv	Total number of bytes of SIP messages received (including retransmissions).
Network Packets Sent	Total number of network packets sent.
Network Packets Recv	Total number of network packets received.
External IP	External IP of the phone.
Operational VLAN ID	ID of the VLAN currently in use if applicable.

Parameter	Description
SW Port	Displays the type of Ethernet connection from the IP phone to the switch.
Upgrade Status	Displays status of the last phone upgrade.
SW Port Config	Displays the type of SW port configuration.
Last Successful Login	Displays the time when the phone has last successful log in.
Last Failed Login	Displays the time when the phone has last failed log in.

Dot1x Authentication

Parameter	Description
Transaction status	Indicates if the phone is authenticated.
Protocol	Displays the protocol of the registered phone.

Ext Status

Parameter	Description
Registration State	Shows "Registered" if the phone is registered, or "Not Registered" if the phone is not registered to the ITSP.
Last Registration At	Last date and time the line was registered.
Next Registration In Seconds	Number of seconds before the next registration renewal.
Message Waiting	Indicates whether message waiting is enabled or disabled.
Mapped SIP Port	Port number of the SIP port mapped by NAT.
Hoteling State	Indicates whether Hoteling is enabled or disabled.
Extended Function Status	Indicates whether extended function is enabled.

Line Call Status

Parameter	Description
Call State	Status of the call.
Tone	Type of tone that the call uses.
Encoder	Codec used for encoding.

Parameter	Description
Decoder	Codec used for decoding.
Type	Direction of the call.
Remote Hold	Indicates whether the far end placed the call on hold.
Callback	Indicates whether the call was triggered by a call back request.
Mapped RTP Port	The port mapped for Real Time Protocol traffic for the call.
Peer Name	Name of the internal phone.
Peer Phone	Phone number of the internal phone.
Duration	Duration of the call.
Packets Sent	Number of packets sent.
Packets Recv	Number of packets received.
Bytes Sent	Number of bytes sent.
Bytes Recv	Number of bytes received.
Decode Latency	Number of milliseconds for decoder latency.
Jitter	Number of milliseconds for receiver jitter.
Round Trip Delay	Number of milliseconds for delay in the RTP-to-RTP interface round trip.
Packets Lost	Number of packets lost.
Loss Rate	The fraction of RTP data packets from the source lost since the beginning of reception. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
Packet Discarded	The fraction of RTP data packets from the source lost since the beginning of reception. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
Discard Rate	The fraction of RTP data packets from the source that have been discarded since the beginning of reception, due to late or early arrival, under-run or overflow at the receiving jitter buffer. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
Burst Duration	The mean duration, expressed in milliseconds, of the burst periods that have occurred since the beginning of reception. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).

Parameter	Description
Gap Duration	The mean duration, expressed in milliseconds, of the gap periods that have occurred since the beginning of reception. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
R-Factor	Voice quality metric that describes the segment of the call that is carried over this RTP session. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
MOS-LQ	The estimated mean opinion score for listening quality (MOS-LQ) is a voice quality metric on a scale from 1 to 5, in which 5 represents excellent and 1 represents unacceptable. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).
MOS-CQ	The estimated mean opinion score for conversational quality (MOS-CQ) is defined as including the effects of delay and other effects that affect conversational quality. Defined in RFC-3611—RTP Control Protocol Extended Reports (RTCP XR).

TR-069 Status

Parameter	Description
TR-069 Feature	Indicates if TR-069 function is enabled or disabled.
Periodic Inform Time	Displays the inform time interval from CPE to ACS.
Last Inform Time	Indicates the last inform time.
Last Transaction Status	Displays the success or the failure status.
Last Session	Indicates the start and end time of the session.
ParameterKey	Displays the key for reference checkpoint for parameter set configured.

Custom CA Status

These fields display the status of provisioning using a custom Certificate Authority (CA).

Parameter	Description
Custom CA Provisioning Status	Indicates whether provisioning using a custom CA succeeded or failed: • Last provisioning succeeded on mm/dd/yyyy HH:MM:SS; or • Last provisioning failed on mm/dd/yyyy HH:MM:SS

Parameter	Description
Custom CA Info	Displays information about the custom CA: • Installed—Displays the "CN Value," where "CN Value" is the value of the CN parameter for the Subject field in the first certificate. • Not Installed—Displays if no custom CA certificate is installed.

Custom CA certificates are configured in the Provisioning tab. For more information about custom CA certificates, see the *Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series Multiplatform Phones Provisioning Guide*.

Provisioning Status

Parameter	Description
Provisioning Profile	Displays the profile file name of the phone.
Provisioning Status 1	Displays the provisioning status (resync) of the phone.
Provisioning Status 2	
Provisioning Status 3	
Provisioning Failure Reason	Displays the reason for the failure of provisioning of the phone.

Note The Upgrade and Provisioning Status are displayed in reverse chronological order (like reboot history) displaying status with time and reason.

Debug Info

Console Logs

Displays the syslog output of the phone in the reverse order, where messages is the latest one. The display includes hyperlinks to individual log files. The console log files include debug and error messages received on the phone and the time stamp reflects UTC time, regardless of time zone settings.

Parameter	Description
Debug Message 1	messages
Debug Message 2	messages.1
Debug Message 3	messages.2

Parameter	Description
Debug Message 4	messages.3
Debug Message 5	messages.4
Debug Message 6	messages.5
Debug Message 7	messages.6
Debug Message 8	messages.7

Problem Reports

Parameter	Description
Report Problem	Displays the tab Generate PRT.
Prt file	Displays the file name of the PRT logs.

Attendant Console Status

Attendant Console Status

Parameter	Description
Console Subscribe Expires	Displays the time when subscription of the key expansion module that is added to the phone will expire.
Subscribe Retry Interval	Displays the time when subscription of the key expansion module that is added to the phone will try to subscribe again.

Unit

Enter the programming information for each line key for the Attendant Console unit.

Parameter	Description
Unit Enable	Indicates whether the key expansion module that is added to the phone is enabled.
Unit Online	Indicates whether the key expansion module that is added to the phone is active.
HW Version	Displays the hardware version of the key expansion module that is added to the phone..
SW Version	Displays the software version of the key expansion module that is added to the phone.

Network Statistics

Ethernet Information

Parameter	Description
TxFrames	Total number of packets that the phone transmitted.
TxBroadcasts	Total number of broadcast packets that the phone transmitted.
TxMulticasts	Total number of multicast packets that the phone transmitted.
TxUnicasts	Total number of unicast packets that the phone transmitted.
RxFrames	Total number of packets received by the phone.
RxBroadcasts	Total number of broadcast packets that the phone received.
RxMulticasts	Total number of multicast packets that the phone received.
RxUnicasts	Total number of unicast packets that the phone received.

Network Port Information

Parameter	Description
RxtotalPkt	Total number of packets that the phone received.
Rxunicast	Total number of unicast packets that the phone received.
Rxbroadcast	Total number of broadcast packets that the phone received.
Rxmulticast	Total number of multicast packets that the phone received.
RxDropPkts	Total number of packets dropped.
RxUndersizePkts	The total number of packets received that are less than 64 octets long, which excludes framing bits, but includes FCS octets, and are otherwise well formed.
RxOversizePkts	The total number of packets received that are longer than 1518 octets, which excludes framing bits, but includes FCS octets, and are otherwise well formed.
RxJabbers	The total number of packets received that are longer than 1518 octets, which excludes framing bits, but incudes FCS octets, and do not end with an even number of octets (alignment error), or had an FCS error.

Parameter	Description
RxAlignErr	Total number of packets between 64 and 1522 bytes in length that were received and that had a bad Frame Check Sequence (FCS).
Rxsize64	Total number of received packets, including bad packets, that were between 0 and 64 bytes in size.
Rxsize65to127	Total number of received packets, including bad packets, that were between 65 and 127 bytes in size.
Rxsize128to255	Total number of received packets, including bad packets, that were between 128 and 255 bytes in size.
Rxsize256to511	Total number of received packets, including bad packets, that were between 256 and 511 bytes in size.
Rxsize512to1023	Total number of received packets, including bad packets, that were between 512 and 1023 bytes in size.
Rxsize1024to1518	Total number of received packets, including bad packets, that were between 1024 and 1518 bytes in size.
TxtotalGoodPkt	Total number of good packets (multicast, broadcast, and unicast) that the phone received.
lldpFramesOutTotal	Total number of LLDP frames that the phone sent out.
lldpAgeoutsTotal	Total number of LLDP frames that timed out in the cache.
lldpFramesDiscardedTotal	Total number of LLDP frames that were discarded when any of the mandatory TLVs is missing, out of order, or contains out of range string length.
lldpFramesInErrorsTotal	Total number of LLDP frames that were received with one or more detectable errors.
lldpFramesInTotal	Total number of LLDP frames that the phone received.
lldpTLVDiscardedTotal	Total number of LLDP TLVs that were discarded.
lldpTLVUnrecognizedTotal	Total number of LLDP TLVs that were not recognized on the phone.
CDPNeighborDeviceId	Identifier of a device connected to this port that CDP discovered.
CDPNeighborIP	IP address of the neighbor device discovered that CDP discovered.
CDPNeighborPort	Neighbor device port to which the phone is connected discovered by CDP.

Parameter	Description
LLDPNeighborDeviceId	Identifier of a device connected to this port discovered by LLDP discovered.
LLDPNeighborIP	IP address of the neighbor device that LLDP discovered.
LLDPNeighborPort	Neighbor device port to which the phone connects that LLDP discovered.
PortSpeed	Speed and duplex information.

Access Port Information

Parameter	Description
RxtotalPkt	Total number of packets that the phone received.
Rxunicast	Total number of unicast packets that the phone received.
Rxbroadcast	Total number of broadcast packets that the phone received.
Rxmulticast	Total number of multicast packets that the phone received.
RxDropPkts	Total number of packets dropped.
RxUndersizePkts	The total number of packets received that are less than 64 octets long, which excludes framing bits, but includes FCS octets, and are otherwise well formed.
RxOversizePkts	The total number of packets received that are longer than 1518 octets, which excludes framing bits, but includes FCS octets, and are otherwise well formed.
RxJabbers	The total number of packets received that are longer than 1518 octets, which excludes framing bits, but incudes FCS octets, and do not end with an even number of octets (alignment error), or had an FCS error.
RxAlignErr	Total number of packets between 64 and 1522 bytes in length that were received and that had a bad Frame Check Sequence (FCS).
Rxsize64	Total number of received packets, including bad packets, that were between 0 and 64 bytes in size.
Rxsize65to127	Total number of received packets, including bad packets, that were between 65 and 127 bytes in size.
Rxsize128to255	Total number of received packets, including bad packets, that were between 128 and 255 bytes in size.

Parameter	Description
Rxsize256to511	Total number of received packets, including bad packets, that were between 256 and 511 bytes in size.
Rxsize512to1023	Total number of received packets, including bad packets, that were between 512 and 1023 bytes in size.
Rxsize1024to1518	Total number of received packets, including bad packets, that were between 1024 and 1518 bytes in size.
TxtotalGoodPkt	Total number of good packets (multicast, broadcast, and unicast) that the phone received.
lldpFramesOutTotal	Total number of LLDP frames that the phone sent out.
lldpAgeoutsTotal	Total number of LLDP frames that timed out in the cache.
lldpFramesDiscardedTotal	Total number of LLDP frames that were discarded when any of the mandatory TLVs is missing, out of order, or contains out of range string length.
lldpFramesInErrorsTotal	Total number of LLDP frames that were received with one or more detectable errors.
lldpFramesInTotal	Total number of LLDP frames that the phone received.
lldpTLVDiscardedTotal	Total number of LLDP TLVs that were discarded.
lldpTLVUnrecognizedTotal	Total number of LLDP TLVs that were not recognized on the phone.
CDPNeighborDeviceId	Identifier of a device connected to this port that CDP discovered.
CDPNeighborIP	IP address of the neighbor device discovered that CDP discovered.
CDPNeighborPort	Neighbor device port to which the phone is connected discovered by CDP.
LLDPNeighborDeviceId	Identifier of a device connected to this port discovered by LLDP discovered.
LLDPNeighborIP	IP address of the neighbor device that LLDP discovered.
LLDPNeighborPort	Neighbor device port to which the phone connects that LLDP discovered.
PortSpeed	Speed and duplex information.

Voice

System

System Configuration

Parameter	Description
Restricted Access Domains	This feature is used when implementing software customization.
Enable Web Server	Enable/disable web server of the IP phone. Default: Yes
Enable Protocol	Choose the type of protocol: • Http • Https If you specify the HTTPS protocol, you must include https: in the URL.
Enable Direct Action Url	Enables the direct action of the URL. Default: Yes
Session Max Timeout	Allows you to enter maximum timeout of the session. Default: 3600
Session Idle Timeout	Allows you to enter idle timeout of the session. Default: 3600
Web Server Port	Allows you to enter port number of the phone web user interface. Default: • 80 for protocol HTTP. • 443 for protocol HTTPS. If you specify a port number other than the default value for that protocol, you must include the nondefault port number in the server URL. Example: https://192.0.2.1:999/admin/advanced
Enable Web Admin Access	Allows you to enable or disable local access to the phone web user interface. Select Yes or No from the drop-down menu. Default: Yes
Admin Password	Allows you to enter password for the administrator. Default: No password

Parameter	Description
User Password	Allows you to enter password for the user. Default: Blank
Phone-UI-readonly	Allows you to make the phone menus and options that the phone users see as read-only fields.
Phone-UI-User-Mode	Allows you to restrict the menus and options that phone users see when they use the phone interface. Choose yes to enable this parameter and restrict access. Default: No Specific parameters are then designated as “na” or “ro” using provisioning files. Parameters designated as “na” will not appear on the phone interface. Parameters designated as “ro” will not be editable by the user.

IPv4 Settings

Parameter	Description
Connection Type	Internet connection type that is configured for the phone. Options are DHCP and Static IP. Default: DHCP
NetMask	Subnet mask of the phone.
Static IP	IP address of the phone.
Gateway	IP address of the gateway.
Primary DNS	Primary Domain Name Server (DNS) assigned to the phone.
Secondary DNS	Secondary Domain Name Server (DNS) if assigned to the phone.

802.1X Authentication

Parameter	Description
Enable 802.1X Authentication	Enables/disables 802.1X Default: No

Optional Network Configuration

Parameter	Description
Host Name	The hostname of the Cisco IP Phone.

Parameter	Description
Domain	The network domain of the Cisco IP Phone. If you are using LDAP, see the LDAP Configuration, on page 101.
DNS Query Mode	Specified mode of DNS query. • Paraller • Sequential
DNS Caching Enable	When set to Yes, the DNS query results are not cached. Default: Yes
Switch Port Config	Allows you to select speed and duplex of the network port. Values are: • Auto 10MB half 10MB full 100 MB half 100MB full 100 half 1000 full
Syslog Server	Specify the syslog server name and port. This feature specifies the server for logging IP phone system information and critical events. If both Debug Server and Syslog Server are specified, Syslog messages are also logged to the Debug Server.
Debug Level	The debug level from 0 to 2. The higher the level, the more debug information is generated. Zero (0) means that no debug information is generated. To log SIP messages, you must set the Debug Level to at least 2. Default: 0
Primary NTP Server	IP address or name of the primary NTP server used to synchronize its time. Default: Blank
Secondary NTP Server	IP address or name of the secondary NTP server used to synchronize its time. Default: Blank

Parameter	Description
DNS Server Order	Specifies the method for selecting the DNS server: • Manual-Dhcp • Manual • Dhcp-Manual
Enable SSLv3	Choose Yes to enable SSLv3. Choose No to disable. Default: No

VLAN Settings

Parameter	Description
Enable VLAN	Choose Yes to enable VLAN. Choose No to disable.
Enable CDP	Enable CDP only if you are using a switch that has Cisco Discovery Protocol. CDP is negotiation based and determines which VLAN the IP phone resides in.
Enable LLDP-MED	Choose Yes to enable LLDP-MED for the phone to advertise itself to devices that use that discovery protocol. When the LLDP-MED feature is enabled, after the phone has initialized and Layer 2 connectivity is established, the phone sends out LLDP-MED PDU frames. If the phone receives no acknowledgment, the manually configured VLAN or default VLAN will be used if applicable. If the CDP is used concurrently, the waiting period of 6 seconds is used. The waiting period will increase the overall startup time for the phone.
Network Startup Delay	Setting this value causes a delay for the switch to get to the forwarding state before the phone will send out the first LLDP-MED packet. The default delay is 3 seconds. For configuration of some switches, you might need to increase this value to a higher value for LLDP-MED to work. Configuring a delay can be important for networks that use Spanning Tree Protocol.
VLAN ID	If you use a VLAN without CDP (VLAN enabled and CDP disabled), enter a VLAN ID for the IP phone. Note that only voice packets are tagged with the VLAN ID. Do not use 1 for the VLAN ID.

Inventory Settings

Parameter	Description
Asset ID	Provides the ability to enter an asset ID for inventory management when using LLDP-MED. The default value for Asset ID is empty. Enter a string of less than 32 characters if you are using this field. The Asset ID can be provisioned only by using the web management interface or remote provisioning. The Asset ID is not displayed on the phone screen. Changing the Asset ID field causes the phone to reboot.

SIP

SIP Parameters

Parameter	Description
Max Forward	SIP Max Forward value, which can range from 1 to 255. Default: 70
Max Redirection	Number of times an invite can be redirected to avoid an infinite loop. Default: 5
Max Auth	Maximum number of times (from 0 to 255) a request can be challenged. Default: 2
SIP User Agent Name	Used in outbound REGISTER requests. Default: $VERSION If empty, the header is not included. Macro expansion of $A to $D corresponding to GPP_A to GPP_D allowed
SIP Server Name	Server header used in responses to inbound responses. Default: $VERSION
SIP Reg User Agent Name	User-Agent name to be used in a REGISTER request. If this is not specified, the <SIP User Agent Name> is also used for the REGISTER request. Default: Blank
SIP Accept Language	Accept-Language header used. To access, click the SIP tab, and fill in the SIP Accept Language field. There is no default. If empty, the header is not included.

Parameter	Description
DTMF Relay MIME Type	MIME Type used in a SIP INFO message to signal a DTMF event. This field must match that of the Service Provider. Default: application/dtmf-relay
Hook Flash MIME Type	MIME Type used in a SIPINFO message to signal a hook flash event.
Remove Last Reg	Enables you to remove the last registration before registering a new one if the value is different. Select yes or no from the drop-down menu.
Use Compact Header	If set to yes, the phone uses compact SIP headers in outbound SIP messages. If inbound SIP requests contain normal headers, the phone substitutes incoming headers with compact headers. If set to no, the phones use normal SIP headers. If inbound SIP requests contain compact headers, the phones reuse the same compact headers when generating the response, regardless of this setting. Default: No
Escape Display Name	Enables you to keep the Display Name private. Select Yes if you want the IP phone to enclose the string (configured in the Display Name) in a pair of double quotes for outbound SIP messages. Default: Yes.
Talk Package	Enables support for the BroadSoft Talk Package that lets users answer or resume a call by clicking a button in an external application. Default: No
Hold Package	Enables support for the BroadSoft Hold Package, which lets users place a call on hold by clicking a button in an external application. Default: No
Conference Package	Enables support for the BroadSoft Conference Package that enables users to start a conference call by clicking a button in an external application. Default: No
RFC 2543 Call Hold	If set to yes, unit includes c=0.0.0.0 syntax in SDP when sending a SIP re-INVITE to the peer to hold the call. If set to no, unit will not include the c=0.0.0.0 syntax in the SDP. The unit will always include a=sendonly syntax in the SDP in either case. Default: Yes

Parameter	Description
Random REG CID on Reboot	If set to yes, the phone uses a different random call-ID for registration after the next software reboot. If set to no, the Cisco IP phone tries to use the same call-ID for registration after the next software reboot. The Cisco IP phone always uses a new random Call-ID for registration after a power-cycle, regardless of this setting. Default: No.
SIP TCP Port Min	Specifies the lowest TCP port number that can be used for SIP sessions. Default: 5060
SIP TCP Port Max	Specifies the highest TCP port number that can be used for SIP sessions. Default: 5080
Caller ID Header	Provides the option to take the caller ID from PAID-RPID-FROM, PAID-FROM, RPID-PAID-FROM, RPID-FROM, or FROM header. Default: PAID-RPID-FROM
Hold Target Before Refer	Controls whether to hold call leg with transfer target before sending REFER to the transferee when initiating a fully-attended call transfer (where the transfer target has answered). Default: No
Dialog SDP Enable	When enabled and the Notify message body is too big causing fragmentation, the Notify message xml dialog is simplified; Session Description Protocol (SDP) is not included in the dialog xml content.
Keep Referee When Refer Failed	If set to yes, it configures the phone to immediately handle NOTIFY sipfrag messages.
Display Diversion Info	Display the Diversion info included in SIP message on LCD or not.
Display Anonymous From Header	Show the caller ID from the SIP INVITE message “From” header when set to Yes, even if the call is an anonymous call. When the parameter is set to no, the phone displays "Anonymous Caller" as the caller ID.
Sip Accept Encoding	Supports the content-encoding gzip feature. The options are none and gzip. If gzip is selected, the SIP message header contains the string “Accept-Encoding: gzip”, and the phone is able to process the SIP message body, which is encoded with the gzip format.
Disable Local Name To Header	The options are No and Yes. If No is selected, no changes are made. The default value is No. If Yes is selected, it disables the display name in “Directory”, “Call History”, and in the “To” header during an outgoing call.

SIP Timer Values

Parameter	Description
SIP T1	RFC 3261 T1 value (RTT estimate) that can range from 0 to 64 seconds. Default: 0.5 seconds
SIP T2	RFC 3261 T2 value (maximum retransmit interval for non-INVITE requests and INVITE responses) that can range from 0 to 64 seconds. Default: 4 seconds
SIP T4	RFC 3261 T4 value (maximum duration a message remains in the network), which can range from 0 to 64 seconds. Default: 5 seconds.
SIP Timer B	INVITE time-out value, which can range from 0 to 64 seconds. Default: 16 seconds.
SIP Timer F	Non-INVITE time-out value, which can range from 0 to 64 seconds. Default: 16 seconds.
SIP Timer H	INVITE final response, time-out value, which can from 0 to 64 seconds. Default: 16 seconds.
SIP Timer D	ACK hang-around time, which can range from 0 to 64 seconds. Default: 16 seconds.
SIP Timer J	Non-INVITE response hang-around time, which can range from 0 to 64 seconds. Default: 16 seconds.
INVITE Expires	INVITE request Expires header value. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 2000000. Default: 240 seconds
ReINVITE Expires	ReINVITE request Expires header value. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 2000000. Default: 30
Reg Min Expires	Minimum registration expiration time allowed from the proxy in the Expires header or as a Contact header parameter. If the proxy returns a value less than this setting, the minimum value is used.
Reg Max Expires	Maximum registration expiration time allowed from the proxy in the Min-Expires header. If the value is larger than this setting, the maximum value is used.

Parameter	Description
Reg Retry Intv	Interval to wait before the Cisco IP Phone retries registration after failing during the last registration.The range is from 1 to 2147483647 Default: 30 See the note below for additional details.
Reg Retry Long Intvl	When registration fails with a SIP response code that does not match<Retry Reg RSC>, the Cisco IP Phone waits for the specified length of time before retrying. If this interval is 0, the phone stops trying. This value should be much larger than the Reg Retry Intvl value, which should not be 0. Default: 1200 See the note below for additional details.
Reg Retry Random Delay	Random delay range (in seconds) to add to <Register Retry Intvl> when retrying REGISTER after a failure. Minimum and maximum random delay to be added to the short timer. The range is from 0 to 2147483647. Default: 0
Reg Retry Long Random Delay	Random delay range (in seconds) to add to <Register Retry Long Intvl> when retrying REGISTER after a failure. Default: 0
Reg Retry Intvl Cap	Maximum value of the exponential delay. The maximum value to cap the exponential backoff retry delay (which starts at the Register Retry Intvl and doubles every retry). Defaults to 0, which disables the exponential backoff (that is, the error retry interval is always at the Register Retry Intvl). When this feature is enabled, the Reg Retry Random Delay is added to the exponential backoff delay value. The range is from 0 to 2147483647. Default: 0
Sub Min Expires	Sets the lower limit of the REGISTER expires value returned from the Proxy server.
Sub Max Expires	Sets the upper limit of the REGISTER minexpires value returned from the Proxy server in the Min-Expires header. Default: 7200.
Sub Retry Intvl	This value (in seconds) determines the retry interval when the last Subscribe request fails. Default: 10.

Note The phone can use a RETRY-AFTER value when it is received from a SIP proxy server that is too busy to process a request (503 Service Unavailable message). If the response message includes a RETRY-AFTER header, the phone waits for the specified length of time before to REGISTER again. If a RETRY-AFTER header is not present, the phone waits for the value specified in the Reg Retry Interval or the Reg Retry Long Interval.

Response Status Code Handling

Parameter	Description
Try Backup RSC	This parameter may be set to invoke failover upon receiving specified response codes. Default: Blank For example, you can enter numeric values 500 or a combination of numeric values plus wild cards if multiple values are possible. For the later, you can use 5?? to represent all SIP Response messages within the 500 range. If you want to use multiple ranges, you can add a comma "," to delimit values of 5?? and 6??
Retry Reg RSC	Interval to wait before the phone retries registration after failing during the last registration. Default: Blank For example, you can enter numeric values 500 or a combination of numeric values plus wild cards if multiple values are possible. For the later, you can use 5?? to represent all SIP Response messages within the 500 range. If you want to use multiple ranges, you can add a comma "," to delimit values of 5?? and 6??

RTP Parameters

Parameter	Description
RTP Port Min	Minimum port number for RTP transmission and reception. Minimum port number for RTP transmission and reception. Should define a range that contains at least 10 even number ports (twice the number of lines); for example, configure RTP port min to 16384 and RTP port max to 16538. Default: 16384
RTP Port Max	Maximum port number for RTP transmission and reception. Should define a range that contains at least 10 even number ports (twice the number of lines); for example, configure RTP port min to 16384 and RTP port max to 16538. Default: 16538

Parameter	Description
RTP Packet Size	Packet size in seconds, which can range from 0.01 to 0.13. Valid values must be a multiple of 0.01 seconds. Default: 0.02
Max RTP ICMP Err	Number of successive ICMP errors allowed when transmitting RTP packets to the peer before the phone terminates the call. If value is set to 0, the phone ignores the limit on ICMP errors.
RTCP Tx Interval	Interval for sending out RTCP sender reports on an active connection. It can range from 0 to 255 seconds. Default: 0

SDP Payload Types

Parameter	Description
G722.2 Dynamic Payload	G722 Dynamic Payload type. Default: 96
iLBC Dynamic Payload	iLBC Dynamic Payload type. Default: 97
iSAC Dynamic Payload	iSAC Dynamic Payload type. Default: 98
OPUS Dynamic Payload	OPUS Dynamic Payload type. Default: 99
AVT Dynamic Payload	AVT dynamic payload type. Ranges from 96-127. Default: 101
INFOREQ Dynamic Payload	INFOREQ Dynamic Payload type.
G711u Codec Name	G711u codec name used in SDP. Default: PCMU
G711a Codec Name	G711a codec name used in SDP. Default: PCMA
G729a Codec Name	G729a codec name used in SDP. Default: G729a
G729b Codec Name	G729b codec name used in SDP. Default: G729b

Parameter	Description
G722 Codec Name	G722 codec name used in SDP. Default: G722
G722.2 Codec Name	G722.2 codec name used in SDP. Default: G722.2
iLBC Codec Name	iLBC codec name used in SDP. Default: iLBC
iSAC Codec Name	iSAC codec name used in SDP. Default: iSAC
OPUS Codec Name	OPUS codec name used in SDP. Default: OPUS
AVT Codec Name	AVT codec name used in SDP. Default: telephone-event

NAT Support Parameters

Parameter	Description
Handle VIA received	Enables the phone to process the received parameter in the VIA header. Default: No
Handle VIA rport	Enables the phone to process the rport parameter in the VIA header. Default: No
Insert VIA received	Enables to insert the received parameter into the VIA header of SIP responses if the received-from IP and VIA sent-by IP values differ. Default: No
Insert VIA rport	Enables to insert the rport parameter into the VIA header of SIP responses if the received-from IP and VIA sent-by IP values differ. Default: No
Substitute VIA Addr	Enables the user to use NAT-mapped IP:port values in the VIA header. Default: No
Send Resp To Src Port	Enables to send responses to the request source port instead of the VIA sent-by port. Default: No

Parameter	Description
STUN Enable	Enables the use of STUN to discover NAT mapping. Default: No
STUN Test Enable	If the STUN Enable feature is enabled and a valid STUN server is available, the phone can perform a NAT-type discovery operation when it powers on. It contacts the configured STUN server, and the result of the discovery is reported in a Warning header in all subsequent REGISTER requests. If the phone detects symmetric NAT or a symmetric firewall, NAT mapping is disabled. Default: No
STUN Server	IP address or fully-qualified domain name of the STUN server to contact for NAT mapping discovery. You can use a public STUN server or set up your own STUN server. Default: Blank
EXT IP	External IP address to substitute for the actual IP address of phone in all outgoing SIP messages. If 0.0.0.0 is specified, no IP address substitution is performed. If this parameter is specified, phone assumes this IP address when generating SIP messages and SDP (if NAT Mapping is enabled for that line). Default: Blank
EXT RTP Port Min	External port mapping number of the RTP Port Minimum number. If this value is not zero, the RTP port number in all outgoing SIP messages is substituted for the corresponding port value in the external RTP port range. Default: 0
NAT Keep Alive Intvl	Interval between NAT-mapping keep alive messages. Default: 15
Redirect Keep Alive	If enabled, the IP phone redirects the keepalive message when SIP_301_MOVED_PERMANENTLY is received as the registration response.

Provisioning

Configuration Profile

Parameter	Description
Provision Enable	Allows or denies resync actions. Default: 160,159,66,150

Parameter	Description
Resync On Reset	The device performs a resync operation after power-up and after each upgrade attempt when set to **Yes**. Default: Yes
Resync Random Delay	A random delay following the boot-up sequence before performing the reset, specified in seconds. In a pool of IP Telephony devices that are scheduled to simultaneously powered up, this introduces a spread in the times at which each unit sends a resync request to the provisioning server. This feature can be useful in a large residential deployment, in the case of a regional power failures. Default: 2
Resync At (HHmm)	Time in 24-hour format (hhmm) to resync the device. When this parameter is provisioned, the Resync Periodic parameter is ignored. Default: Blank
Resync At Random Delay	To avoid flooding the server with simultaneously resync requests from multiple phones set to resync at the same time, the phone triggers the resync up to ten minutes after the specified time. The input value (in seconds) is converted to minutes. The default value is 600 seconds (10 minutes). If the parameter value is set to less than 600, the default value is used. Default: 600
Resync Periodic	Time in seconds between periodic resyncs. If this value is empty or zero, the device does not resync periodically. Default: 3600
Resync Error Retry Delay	If a resync operation fails because the IP Telephony device was unable to retrieve a profile from the server, if the downloaded file is corrupt, or an internal error occurs, the device tries to resync again after a time specified in seconds. If the delay is set to 0, the device does not try to resync again following a failed resync attempt. Default: 3600
Forced Resync Delay	Forced resync delay typically takes place when it is time to a resync and you are in an active call. For example, if you set 5 minute for Periodic Resync and you place a call right after the resync, the resync happens while you are 6 minutes into the call (normal time of Resync + Forced Resync Delay). Default: 14400

Parameter	Description
Resync From SIP	Controls requests for resync operations via a SIP NOTIFY event sent from the service provider proxy server to the IP Telephony device. If enabled, the proxy can request a resync by sending a SIP NOTIFY message containing the Event: resync header to the device. Default: Yes
Resync After Upgrade Attempt	Enables or disables the resync operation after any upgrade occurs. If Yes is selected, sync is triggered. Default: Yes
Resync Trigger 1 Resync Trigger 2	If the logical equation in these parameters evaluates to FALSE, Resync is not triggered even when Resync On Reset is set to TRUE. Only Resync via direct action URL and SIP notify ignores these Resync Trigger. Default: Blank
Resync Fails On FNF	A resync is considered unsuccessful if a requested profile is not received from the server. This can be overridden by this parameter. When it is set to **No**, the device accepts a `file-not-found` response from the server as a successful resync. Default: Yes
Profile Rule Profile Rule B Profile Rule C Profile Rule D	Remote configuration profile rules evaluated in sequence. Each resync operation can retrieve multiple files, potentially managed by different servers. Default: /$PSN.xml
DHCP Option To Use	DHCP options, delimited by commas, used to retrieve firmware and profiles. Default: 66,160,159,150,60,43,125
Log Request Msg	The message sent to the syslog server at the start of a resync attempt. Default: `$PN $MAC –Requesting % $SCHEME://$SERVIP:$PORT$PATH`
Log Success Msg	The syslog message issued upon successful completion of a resync attempt. Default: `$PN $MAC -Successful Resync  % $SCHEME://$SERVIP:$PORT$PATH`
Log Failure Msg	The syslog message that is issued after a failed download attempt. Default: `$PN $MAC -- Resync failed: $ERR`

Parameter	Description
HTTP Report Method	Allows to select HTTP options. Options are POST and PUT.
User Configurable Resync	Allows a user to resync the phone from the phone screen. Default: Yes

Firmware Upgrade

Parameter	Description
Upgrade Enable	Allows firmware update operations independent of resync actions. Default: Yes
Upgrade Error Retry Delay	The interval applied in the event of an upgrade failure. The firmware upgrade error timer activates after a failed firmware upgrade attempt and is initialized with this value. The next firmware upgrade attempt occurs when this timer counts down to zero. Default: 3600 seconds

Upgrade Rule	A firmware upgrade script that defines upgrade conditions and associated firmware URLs. It uses the same syntax as Profile Rule.
	Use the following format to enter the upgrade rule:
	`protocol://server[:port]/profile_pathname`
	For example:
	`tftp://192.168.1.5/image/sip88xx.10-3-1-9-3PCC.loads`
	If no protocol is specified, TFTP is assumed. If no server-name is specified, the host that requests the URL is used as the server name. If no port is specified, the default port is used (69 for TFTP, 80 for HTTP, or 443 for HTTPS).
	Default: Blank

Log Upgrade Request Msg	Syslog message issued at the start of a firmware upgrade attempt. Default: $PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH
Log Upgrade Success Msg	Syslog message issued after a firmware upgrade attempt completes successfully. Default: $PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR
Log Upgrade Failure Msg	Syslog message issued after a failed firmware upgrade attempt. Default: $PN $MAC -- Upgrade failed: $ERR

For information about the Provisioning page, see the *Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series Multiplatform Phones Provisioning Guide*.

CA Settings

Parameter	Description
Custom CA Rule	The URL to download Custom CA. Default: Blank

HTTP Settings

Parameter	Description
HTTP User Agent Name	Allows you to enter a name for HTTP user. Default: Blank

Problem Report Tool

Parameter	Description
PRT Upload Rule	Path to the PRT upload script.
PRT Upload Method	Method used to upload PRT logs to the remote server. Can be either HTTP POST or PUT. Default: POST

General Purpose Parameters

Parameter	Description
GPP A - GPP P	The general purpose parameters GPP_* are used as free string, registers when configuring the Cisco IP phones to interact with a particular provisioning server solution. They can be configured to contain diverse values, including the following: • Encryption keys. • URLs. • Multistage provisioning status information. • Post request templates. • Parameter name alias maps. • Partial string values, eventually combined into complete parameter values. Default: Blank

Regional

Call Progress Tones

Parameter	Description
Dial Tone	Prompts the user to enter a phone number.
Outside Dial Tone	Alternative to the Dial Tone. It prompts the user to enter an external phone number, as opposed to an internal extension. It is triggered by a, (comma) character encountered in the dial plan.
Prompt Tone	Prompts the user to enter a call forwarding phone number.
Busy Tone	Played when a 486 RSC is received for an outbound call.
Reorder Tone	Played when an outbound call has failed or after the far end hangs up during an established call. Reorder Tone is played automatically when <Dial Tone> or any of its alternatives times out.
Ring Back Tone	Played during an outbound call when the far end is ringing.
Call Waiting Tone	Played when a call is waiting.
Confirm Tone	Brief tone to notify the user that the last input value has been accepted.
MWI Dial Tone	Played instead of the Dial Tone when there are unheard messages in the caller's mailbox.
Cfwd Dial Tone	Played when all calls are forwarded.
Holding Tone	Informs the local caller that the far end has placed the call on hold.
Conference Tone	Played to all parties when a three-way conference call is in progress.
Secure Call Indication Tone	Played when a call has been successfully switched tosecure mode. It should be played only for a short while (less than 30 seconds) and at a reduced level (less than -19 dBm) so it does not interfere with the conversation.
Page Tone	Specifies the tone transmitted when the paging feature is enabled.
Alert Tone	Played when an alert occurs.
System Beep	Audible notification tone played when a system error occurs.
Call Pickup Tone	Provides the ability to configure an audio indication for call pickup.

Distinctive Ring Patterns

Parameter	Description
Cadence 1	Cadence script for distinctive ring 1. Defaults to 60(2/4).
Cadence 2	Cadence script for distinctive ring 2. Defaults to 60(.3/.2, 1/.2,.3/4).
Cadence 3	Cadence script for distinctive ring 3. Defaults to 60(.8/.4,.8/4).
Cadence 4	Cadence script for distinctive ring 4. Defaults to 60(.4/.2,.3/.2,.8/4).
Cadence 5	Cadence script for distinctive ring 5. Defaults to 60(.2/.2,.2/.2,.2/.2,1/4).
Cadence 6	Cadence script for distinctive ring 6. Defaults to 60(.2/.4,.2/.4,.2/4).
Cadence 7	Cadence script for distinctive ring 7. Defaults to 60(4.5/4).
Cadence 8	Cadence script for distinctive ring 8. Defaults to 60(0.25/9.75)
Cadence 9	Cadence script for distinctive ring 9. Defaults to 60(.4/.2,.4/2).

Control Timer Values (sec)

Parameter	Description
Reorder Delay	Delay after far end hangs up before reorder (busy) tone is played. 0 = plays immediately, inf = never plays. Range: 0–255 seconds. Set to 255 to return the phone immediately to on-hook status and to not play the tone.
Interdigit Long Timer	Long timeout between entering digits when dialing. The interdigit timer values are used as defaults when dialing. The Interdigit_Long_Timer is used after any one digit, if all valid matching sequences in the dial plan are incomplete as dialed. Range: 0–64 seconds. Default: 10

Parameter	Description
Interdigit Short Timer	Short timeout between entering digits when dialing. The Interdigit_Short_Timer is used after any one digit, if at least one matching sequence is complete as dialed, but more dialed digits would match other as yet incomplete sequences. Range: 0–64 seconds. Default: 3

Vertical Service Activation Codes

Parameter	Description
Call Return Code	This code calls the last caller. Defaults to *69.
Blind Transfer Code	Begins a blind transfer of the current call to the extension specified after the activation code. Defaults to *88.
Cfwd All Act Code	Forwards all calls to the extension specified after the activation code. Defaults to *72.
Cfwd All Deact Code	Cancels call forwarding of all calls. Defaults to *73.
Cfwd Busy Act Code	Forwards busy calls to the extension specified after the activation code. Defaults to *90.
Cfwd Busy Deact Code	Cancels call forwarding of busy calls. Defaults to *91.
Cfwd No Ans Act Code	Forwards no-answer calls to the extension specified after the activation code. Defaults to *92.
Cfwd No Ans Deact Code	Cancels call forwarding of no-answer calls. Defaults to *93.
CW Act Code	Enables call waiting on all calls. Defaults to *56.
CW Deact Code	Disables call waiting on all calls. Defaults to *57.
CW Per Call Act Code	Enables call waiting for the next call. Defaults to *71.

Parameter	Description
CW Per Call Deact Code	Disables call waiting for the next call. Defaults to *70.
Block CID Act Code	Blocks caller ID on all outbound calls. Defaults to *67.
Block CID Deact Code	Removes caller ID blocking on all outbound calls. Defaults to *68.
Block CID Per Call Act Code	Removes caller ID blocking on the next inbound call. Defaults to *81.
Block CID Per Call Deact Code	Removes caller ID blocking on the next inbound call. Defaults to *82.
Block ANC Act Code	Blocks all anonymous calls. Defaults to *77.
Block ANC Deact Code	Removes blocking of all anonymous calls. Defaults to *87.
DND Act Code	Enables the do not disturb feature. Defaults to *78.
DND Deact Code	Disables the do not disturb feature. Defaults to *79.
Secure All Call Act Code	Makes all outbound calls secure. Defaults to *16.
Secure No Call Act Code	Makes all outbound calls not secure. Defaults to *17.
Paging Code	The star code used for paging the other clients in the group. Defaults to *96.
Call Park Code	The star code used for parking the current call. Defaults to *38.
Call Pickup Code	The star code used for picking up a ringing call. Defaults to *36.

Parameter	Description
Call Unpark Code	The star code used for picking up a call from the call park. Defaults to *39.
Group Call Pickup Code	The star code used for picking up a group call. Defaults to *37.
Referral Services Codes	These codes tell the IP phone what to do when the user places the current call on hold and is listening to the second dial tone. One or more *code can be configured into this parameter, such as *98, or *97|*98|*123, and so on. Max total length is 79 chars. This parameter applies when the user places the current call on hold (by Hook Flash) and is listening to second dial tone. Each *code (and the following valid target number according to current dial plan) entered on the second dial-tone triggers the phone to perform a blind transfer to a target number that is prepended by the service *code. For example, after the user dials *98, the IP phone plays a special dial tone called the Prompt Tone while waiting for the user the enter a target number (which is checked according to dial plan as in normal dialing). When a complete number is entered, the phone sends a blind REFER to the holding party with the Refer-To target equals to *98<target_number>. This feature allows the phone to hand off a call to an application server to perform further processing, such as call park. The *codes should not conflict with any of the other vertical service codes internally processed by the IP phone. You can empty the corresponding *code that you do not want to the phone to process.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Feature Dial Services Codes</td><td>These codes tell the phone what to do when the user is listening to the first or second dial tone.

One or more *code can be configured into this parameter, such as *72, or *72|*74|*67|*82, and so forth. The maximum total length is 79 characters. This parameter applies when the user has a dial tone (first or second dial tone). Enter *code (and the following target number according to current dial plan) entered at the dial tone triggers the phone to call the target number prepended by the *code. For example, after user dials *72, the phone plays a prompt tone awaiting the user to enter a valid target number. When a complete number is entered, the phone sends a INVITE to *72<target_number> as in a normal call. This feature allows the proxy to process features like call forward (*72) or BLock Caller ID (*67).

The *codes should not conflict with any of the other vertical service codes internally processed by the phone. You can empty the corresponding *code that you do not want to the phone to process.

You can add a parameter to each *code in Features Dial Services Codes to indicate what tone to play after the *code is entered, such as *72‘c‘|*67‘p‘. Below are a list of allowed tone parameters (note the use of back quotes surrounding the parameter without spaces)

• c = Cfwd Dial Tone
• d = Dial Tone
• m = MWI Dial Tone
• o = Outside Dial Tone
• p = Prompt Dial Tone
• s = Second Dial Tone
• x = No tones are place, x is any digit not used above

If no tone parameter is specified, the phone plays Prompt tone by default.

If the *code is not to be followed by a phone number, such as *73 to cancel call forwarding, do not include it in this parameter. In that case, simple add that *code in the dial plan and the phone sends INVITE *73@..... as usual when user dials *73.</td></tr>
</table>

Vertical Service Announcement Codes

Parameter	Description
Service Annc Base Number	Defaults to blank.
Service Annc Extension Codes	Defaults to blank.

Outbound Call Codec Selection Codes

Parameter	Description
Prefer G711u Code	Makes this codec the preferred codec for the associated call. Defaults to *017110.
Force G711u Code	Makes this codec the only codec that can be used for the associated call. Defaults to *027110.
Prefer G711a Code	Makes this codec the preferred codec for the associated call. Defaults to *017111
Force G711a Code	Makes this codec the only codec that can be used for the associated call. Defaults to *027111.
Prefer G722 Code	Makes this codec the preferred codec for the associated call. Defaults to *01722. Only one G.722 call at a time is allowed. If a conference call is placed, a SIP re-invite message is sent to switch the calls to narrowband audio.
Force G722 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *02722. Only one G.722 call at a time is allowed. If a conference call is placed, a SIP re-invite message is sent to switch the calls to narrowband audio.
Prefer G722.2 Code	Makes this codec the preferred codec for the associated call.
Force G722.2 Code	Makes this codec the only codec that can be used for the associated call.
Prefer G729a Code	Makes this codec the preferred codec for the associated call. Defaults to *01729.
Force G729a Code	Makes this codec the only codec that can be used for the associated call. Defaults to *02729.
Prefer iLBC Code	Makes this codec the preferred codec for the associated call.
Force iLBC Code	Makes this codec the only codec that can be used for the associated call.

Parameter	Description
Prefer ISAC Code	Makes this codec the preferred codec for the associated call.
Force ISAC Code	Makes this codec the only codec that can be used for the associated call.
Prefer OPUS Code	Makes this codec the preferred codec for the associated call.
Force OPUS Code	Makes this codec the only codec that can be used for the associated call.

Time

Parameter	Description
Set Local Date (mm/dd/yyyy)	Sets the local date (mm represents the month and dd represents the day). The year is optional and uses two or four digits. Default: Blank
Set Local Time (HH/mm)	Sets the local time (hh represents hours and mm represents minutes). Seconds are optional. Default: Blank
Time Zone	Selects the number of hours to add to GMT to generate the local time for caller ID generation. Choices are GMT-12:00, GMT-11:00,…, GMT, GMT+01:00, GMT+02:00, …, GMT+13:00. Default: GMT-08:00
Time Offset (HH/mm)	This specifies the offset from GMT to use for the local system time. Default: 00/00
Ignore DHCP Time Offset	When used with some routers that have DHCP with time offset values configured, the IP phone uses the router settings and ignores the IP phone time zone and offset settings. To ignore the router DHCP time offset value, and use the local time zone and offset settings, choose yes for this option. Choosing no causes the IP phone to use the router's DHCP time offset value. Default: Yes.

Parameter	Description
Daylight Saving Time Rule	Enter the rule for calculating daylight saving time; it should include the start, end, and save values. This rule is comprised of three fields. Each field is separated by ; (a semicolon) as shown below. Optional values inside [ ] (the brackets) are assumed to be 0 if they are not specified. Midnight is represented by 0:0:0 of the given date. This is the format of the rule: Start = <start-time>; end=<end-time>; save = <save-time>. The <start-time> and <end-time> values specify the start and end dates and times of daylight saving time. Each value is in this format: <month> /<day> / <weekday>[/HH:[mm[:ss]]] The <save-time> value is the number of hours, minutes, and/or seconds to add to the current time during daylight saving time. The <save-time> value can be preceded by a negative (-) sign if subtraction is desired instead of addition. The <save-time> value is in this format: [/[+|-]HH:[mm[:ss]]] The <month> value equals any value in the range 1-12 (January-December). The <day> value equals [+|-] any value in the range 1-31. If <day> is 1, it means the <weekday> on or before the end of the month (in other words the last occurrence of < weekday> in that month).
Daylight Saving Time Rule (continued)	The <weekday> value equals any value in the range 1-7 (Monday-Sunday). It can also equal 0. If the <weekday> value is 0, this means that the date to start or end daylight saving is exactly the date given. In that case, the <day> value must not be negative. If the <weekday> value is not 0 and the <day> value is positive, then daylight saving starts or ends on the <weekday> value on or after the date given. If the <weekday> value is not 0 and the <day> value is negative, then daylight saving starts or ends on the <weekday> value on or before the date given. Where: • HH stands for hours (0-23). • mm stands for minutes (0-59). • ss stands for seconds (0-59). Default: 3/-1/7/2;end=10/-1/7/2;save=1.
Daylight Saving Time Enable	Enables Daylight Saving Time. Default: Yes

Language

Parameter	Description
Dictionary Server Script	Defines the location of the dictionary server, the languages available, and the associated dictionary. See the Dictionary Server Script, on page 49. Default: Blank

Language Selection	Specifies the default language. The value must match one of the languages supported by the dictionary server. The script (dx value) is:
	`<Language_Selection ua="na"> </Language_Selection>`
	Default: Blank
	The maximum number of characters is 512. For example:
	`<Language_Selection ua="na"> Spanish </Language_Selection>`

Locale	Choose the locale that should be set in the HTTP Accept-Language header Default: en-US

Phone

General

Parameter	Description
Station Name	Name of the phone.
Station Display Name	Name to identify the phone; appears on the phone screen. You can use spaces in this field and the name does not have to be unique.
Voice Mail Number	A phone number or URL to check voice mail. Default: None
Select Logo	Select from None, PNG Picture, or Text Logo. Default: None

Handsfree

Parameter	Description
Bluetooth Mode	Shows the method of Bluetooth connection. • Phone—Pairs with a Bluetooth headset only. • Handsfree—Operates as a handsfree device with a Bluetooth-enabled mobile phone. • Both—Uses a Bluetooth headset, or operates with a Bluetooth-enabled mobile phone.
Line	Specifies the line number for which the Bluetooth is enabled.

Line Key

Parameter	Description
Extension	Specifies the n extensions to be assigned to Line Key n. Default: Line Key n
Short Name	Specifies the user name for Line Key. Default: $USER
Share Call Appearance	Specifies whether the incoming call appearance is shared with other phones or it is private.
Extended Function	Use to assign Busy Lamp Field, Call Pickup, and Speed Dial Functions to Idle Lines on the IP phone.

Miscellaneous Line Key Settings

Parameter	Description
Line ID Mapping	Specifies the shared call appearance line ID mapping. If Vertical First is set, the first call makes the LED flash. If Horizontal first is set, the second call makes the same LED flash. **Note** 7811 Cisco IP Phone does not support Line ID Mapping. Default: Vertical First
SCA Barge-In-Enable	Enables the SCA Barge-In. Default: No
SCA Sticky Auto Line Seize	If enabled, restricts to automatically pick up an incoming call on a shared line when you take the phone off-hook.

Parameter	Description
Call Appearances Per Line	This parameter allows you to choose the number of calls per line button. You can choose a value from 2 to 10. Default: 2

Supplementary Services

Parameter	Description
Conference Serv	Enable/disable three-way conference service. Default: Yes
Attn Transfer Serv	Enable/disable attended-call-transfer service. Default: Yes
Blind Transfer Serv	Enable/disable blind-call-transfer service. Default: Yes
DND Serv	Enable/disable do not disturb service. Default: Yes
Block ANC Serv	Enable/disable block-anonymous-call service. Default: Yes
Block CID Serv	Enable/disable blocking outbound Caller-ID service. Default: Yes
Cfwd All Serv	Enable/disable call-forward-all service. Default: Yes
Cfwd Busy Serv	Enable/disable call-forward-on-busy service. Default: Yes
Cfwd No Ans Serv	Enable/disable call-forward-no-answer service. Default: Yes

Ringtone

Parameter	Description
Ring	Ring tone scripts for different rings.

Parameter	Description
Silent Ring Duration	Controls the duration of the silent ring. For example, if the parameter is set to 20 seconds, the phone plays the silent ring for 20 seconds then sends 480 response to INVITE message.

Extension Mobility

Parameter	Description
EM Enable	Options to enable or to disable the extension mobility support for the phone. Default: No
EM User Domain	Name of the domain for the phone or the authentication server. Default: Blank
Inactivity Timer(m)	Specifies the duration for which the extension mobility remains inactive.
Countdown Timer(s)	Specifies the duration for which it waits before it logs out". Default is 10

BroadSoft Settings

Parameter	Description
Directory Enable	Set to Yes to enable BroadSoft directory for the phone user. Default: No
XSI Host Server	Enter the name of the server; for example, xsi.iop1.broadworks.net. Default: Blank
Directory Name	Name of the directory. Displays on the phone as a directory choice. Default: Blank
Directory Type	Select the type of BroadSoft directory: Enterprise: Allows users to search on last name, first name, user or group ID, phone number, extension, department, or email address. Group: Allows users to search on last name, first name, user ID, phone number, extension, department, or email address. Personal: Allows users to search on last name, first name, or telephone number. Default: Enterprise

Parameter	Description
Directory User ID	BroadSoft User ID of the phone user; for example, johndoe@xdp.broadsoft.com. Default: Blank
Directory Password	Alphanumeric password associated with the User ID. Default: Blank

XML Service

Parameter	Description
XML Directory Service Name:	Name of the XML Directory. Displays on the user's phone as a directory choice Default: Blank
XML Directory Service URL	URL where the XML Directory is located. Default: Blank
XML User Name	XML service username for authentication purposes Default: Blank
XML Password	XML service password for authentication purposes Default: Blank

LDAP

Parameter	Description
LDAP Dir Enable	Choose Yes to enable LDAP. Default: No
Corp Dir Name	Enter a free-form text name, such as "Corporate Directory." Default: Blank
Server	Enter a fully qualified domain name or IP address of an LDAP server in the following format: nnn.nnn.nnn.nnn Enter the host name of the LDAP server if the MD5 authentication method is used. Default: Blank

Parameter	Description
Search Base	Specify a starting point in the directory tree from which to search. Separate domain components [dc] with a comma. For example: dc=cv2bu,dc=com Default: Blank
Client DN	Enter the distinguished name domain components [dc]; for example: dc=cv2bu,dc=com If you are using the default Active Directory schema (Name(cn)->Users->Domain), an example of the client DN follows: cn="David Lee",dc=users,dc=cv2bu,dc=com Default: Blank
User Name	Enter the username for a credentialed user on the LDAP server. Default: Blank
Password	Enter the password for the LDAP username. Default: Blank
Auth Method	Select the authentication method that the LDAP server requires. Choices are: None—No authentication is used between the client and the server. Simple—The client sends its fully-qualified domain name and password to the LDAP server. Might present security issues. Digest-MD5—The LDAP server sends authentication options and a token to the client. The client returns an encrypted response that is decrypted and verified by the server. Default: None
Last Name Filter	This defines the search for surnames [sn], known as last name in some locations. For example, sn:(sn=*$VALUE*). This search allows the provided text to appear anywhere in a name: beginning, middle, or end. Default: Blank
First Name Filter	This defines the search for the common name [cn]. For example, cn:(cn=*$VALUE*). This search allows the provided text to appear anywhere in a name: beginning, middle, or end. Default: Blank
Search Item 3	Additional customized search item. Can be blank if not needed. Default: Blank

Parameter	Description
Search Item 3 Filter	Customized filter for the searched item. Can be blank if not needed. Default: Blank
Search Item 4	Additional customized search item. Can be blank if not needed. Default: Blank
Search Item 4 Filter	Customized filter for the searched item. Can be blank if not needed. Default: Blank
Display Attrs	Format of LDAP results displayed on phone, where: • a—Attribute name • cn—Common name • sn—Surname (last name) • telephoneNumber—Phone number • n—Display name For example, n=Phone causes “Phone:” to be displayed in front of the phone number of an LDAP query result when the detail soft button is pressed. • t—type When t=p, that is, t is of type phone number, the retrieved number can be dialed. Only one number can be made dialable. If two numbers are defined as dialable, only the first number is used. For example, a=ipPhone, t=p; a=mobile, t=p; This example results in only the IP Phone number being dialable and the mobile number is ignored. • p—phone number When p is assigned to a type attribute, example t=p, the retrieved number is dialable by the phone. For example, a=givenName,n=firstname;a=sn,n=lastname;a=cn,n=cn;a=telephoneNumber,n=tele,t=p Default: Blank

Parameter	Description
Number Mapping	Can be blank if not needed. **Note** With the LDAP number mapping, you can manipulate the number that was retrieved from the LDAP server. For example, you can append 9 to the number if your dial plan requires a user to enter 9 before dialing. Add the 9 prefix by adding (<:9xx.>) to the LDAP Number Mapping field. For example, 555 1212 would become 9555 1212. If you do not manipulate the number in this fashion, a user can use the Edit Dial feature to edit the number before dialing out. Default: Blank

Programmable Softkeys

Parameter	Description
Programmable Softkey Enable	Enables programmable softkeys.
Idle Key List	Softkeys that display when the phone is idle.
Off Hook Key List	Softkeys that display when the phone is off-hook.
Dialing Input Key List	Softkeys that display when the user must enter dialing data.
Progressing Key List	Softkeys that display when a call is attempting to connect.
Connected Key List	Softkeys that display when a call is connected.
Start-Xfer Key List	Softkeys that display when a call transfer has been initiated.
Start-Conf Key List	Softkeys that display when a conference call has been initiated.
Conferencing Key List	Softkeys that display when a conference call is in progress.
Releasing Key List	Softkeys that display when a call is released.
Hold Key List	Softkeys that display when one or more calls are on hold.
Ringing Key List	Softkeys that display when a call is incoming.
Shared Active Key List	Softkeys that display when a call is active on a shared line.
Shared Held Key List	Softkeys that display when a call is on hold on a shared line.
PSK 1 through PSK 16	Programmable softkey fields. Enter a string in these fields to configure softkeys that display on the phone screen. You can create softkeys for speed dials to numbers or extensions, vertical service activation codes (* codes), or XML scripts.

User

Hold Reminder

Parameter	Description
Hold Reminder Timer	Specifies the time delay (in seconds), that a ring splash is heard on an active call when another call was placed on hold. Default: 0
Hold Reminder Ringtone	Specifies the volume of the timer ringtone.

Call Forward

Parameter	Description
Cfwd Setting	Select **Yes** to enable call forwarding.
Cfwd All Dest	Enter the extensions to which the call is forwarded.
Cfwd Busy Dest	Enter the extensions to forward calls to when the line is busy. Default: voicemail
Cfwd No Ans Dest	Enter the extension to forward calls to when the call is not answered. Default: voicemail
Cfwd No Ans Delay	Enter the delay in time (in seconds) to wait before forwarding a call that is unanswered. Default: 20 seconds

Speed Dial

You can configure speed dials on the Cisco IP Phone from the LCD GUI or the web GUI.

Speed Dial 2 to 9: Target phone number (or URL) assigned to speed dial 2, 3, 4, 5, 6, 7, 8, or 9. Press the digit key (2-9) to dial out the assigned number.

Default: Blank

Supplementary Services

Parameter	Description
CW Setting	Enables or disables the Call Waiting service. Default: Yes
Block CID Setting	Enables or disables the Block CID service. Default: No

Parameter	Description
Block ANC Setting	Enables or disables the Block ANC service. Default: No
DND Setting	Enables or disables the DND settings options for a user.
Handset LED Alert	Enables or disables LED alert on the handset. Options are: Voicemail and Voicemail, Missed Call. Default: Voicemail
Secure Call Setting	Enables or disables Secure Call. Default: No
Auto Answer Page	Enables or disables automatic answering of paged calls. Default: Yes
Preferred Audio Device	Choose the type of audio that the phone will use. Options are: Speaker and Headset. Default: None
Time Format	Choose the time format for the phone (12 or 24 hour). Default: 12hr
Date Format	Choose the date format for the phone (month/day or day/month). Default: month/day
Miss Call Shortcut	Enables or disables the option for creating a missed call shortcut.
Alert Tone Off	Enables or disables the alert tone.
Log Missed Calls for EXT (n)	Enables or disables the missed calls logs for a specific extension.
Shared Line DND Cfwd Enable	Enable/disable the Shared Line DND Call Forward.

Audio

Parameter	Description
Ringer Volume	Sets the default volume for the ringer. Default: 9
Speaker Volume	Sets the default volume for the speakerphone. Default: 8

Parameter	Description
Handset Volume	Sets the default volume for the handset. Default: 10
Headset Volume	Sets the default volume for the headset. Default: 10

LCD

Parameter	Description
Back Light Timer (minutes)	Select the number of minutes before the back light should turn off (1m, 5m, or 30m) or Always On. Default: 5m
Brightness	Enter a number value from 1 to 15. The higher the number, the greater the brightness on the IP phone screen. Default: 10

Extension

Extension

In a configuration profile, the Line parameters must be appended with the appropriate numeral to indicate the line to which the setting applies. For example:

```
[1] to specify line one
[2] to specify line two
```

General

Parameter	Description
Line Enable	To enable this line for service, select yes. Otherwise, select No. Default: Yes

Share Line Appearance

Parameter	Description
Share Ext	Indicates whether this extension is to be shared with other Cisco IP phones or private. Default: Yes
Shared User ID	The user identified assigned to the shared line appearance. Default: Blank

Parameter	Description
Subscription Expires	Number of seconds before the SIP subscription expires. Before the subscription expiration, the phone gets NOTIFY messages from the SIP server on the status of the shared phone extension. Default: 3600
Restrict MWI	When enabled, the message waiting indicator lights only for messages on private lines. Default: No

NAT Settings

Parameter	Description
NAT Mapping Enable	To use externally mapped IP addresses and SIP/ RTP ports in SIP messages, select yes. Otherwise, select no. Default: No
NAT Keep Alive Enable	To send the configured NAT keep alive message periodically, select yes. Otherwise, select no. Default: No
NAT Keep Alive Msg	Enter the keep alive message that should be sent periodically to maintain the current NAT mapping. If the value is $NOTIFY, a NOTIFY message is sent. If the value is $REGISTER, a REGISTER message without contact is sent. Default: $NOTIFY
NAT Keep Alive Dest	Destination that should receive NAT keep alive messages. If the value is $PROXY, the messages are sent to the current or outbound proxy.

Network Settings

Parameter	Description
SIP TOS/DiffServ Value	Time of service (ToS)/differentiated services (DiffServ) field value in UDP IP packets carrying a SIP message. Defaults to 0x68.
RTP ToS/DiffServ Value	ToS/DiffServ field value in UDP IP packets carrying RTP data. Defaults to 0xb8.

SIP Settings

Parameter	Description
SIP Transport	Select from **UDP**, **TCP**, or **TLS**. Default: UDP
SIP Port	Port number of the SIP message listening and transmission port. Default: 5060
SIP 100REL Enable	Support of 100REL SIP extension for reliable transmission of provisional responses (18x) and use of PRACK requests. Select **Yes** to enable. Default: No
EXT SIP Port	The external SIP port number.
Auth Resync-Reboot	The Cisco IP Phone authenticates the sender when it receives a NOTIFY message with the following requests: • resync • reboot • report • restart • XML-service Select **Yes** to enable. Default: Yes
SIP Proxy-Require	The SIP proxy can support a specific extension or behavior when it sees this header from the user agent. If this field is configured and the proxy does not support it, it responds with the message, unsupported. Enter the appropriate header in the field provided.
SIP Remote-Party-ID	The Remote-Party-ID header to use instead of the From header. Select **Yes** to enable. Default: Yes
Referor Bye Delay	Controls when the phone sends BYE to terminate stale call legs upon completion of call transfers. Multiple delay settings (Referor, Refer Target, Referee, and Refer-To Target) are configured on this screen. For the Referror Bye Delay, enter the appropriate period of time in seconds. Default: 4
Refer-To Target Contact	Indicates the refer-to target. Select **Yes** to send the **SIP Refer** to the contact. Default: No

Parameter	Description
Referee Bye Delay	For the Referee Bye Delay, enter the appropriate period of time in seconds. Default: 0
Refer Target Bye Delay	For the Refer Target Bye Delay, enter the appropriate period of time in seconds. Default: 0
Sticky 183	When enabled, the IP telephony ignores further 180 SIP responses after receiving the first 183 SIP response for an outbound INVITE. To enable this feature, select **Yes**. Otherwise, select **No**. Default: No
Auth INVITE	When enabled, authorization is required for initial incoming INVITE requests from the SIP proxy. To enable this feature, select **Yes**. Default: No
Ntfy Refer On 1xx-To-Inv	If set to **Yes**, as a transferee, the phone will send a NOTIFY with Event:Refer to the transferor for any 1xx response returned by the transfer target, on the transfer call leg. If set to **No**, the phone will only send a NOTIFY for final responses (200 and higher).
Set G729 annexb	Configure G.729 Annex B settings.
Set iLBC mode	Select iLBC 20ms or 30ms frame size mode. Default: 20
User Equal Phone	When a tel URL is converted to a SIP URL and the phone number is represented by the user portion of the URL, the SIP URL includes the optional : user=phone parameter (RFC3261). For example: To: sip:+12325551234@example.com; user=phone To enable this optional parameter, select **Yes**. Default: No

Call Feature Settings

Parameter	Description
Blind Attn-Xfer Enable	Enables the phone to perform an attended transfer operation by ending the current call leg and performing a blind transfer of the other call leg. If this feature is disabled, the phone performs an attended transfer operation by referring the other call leg to the current call leg while maintaining both call legs. To use this feature, select Yes. Otherwise, select No. Default: No
Message Waiting	Indicates whether the Message Waiting Indicator on the phone is lit. This parameter toggles a message from the SIP proxy to indicate if a message is waiting.
Auth Page	Specifies whether to authenticate the invite before auto answering a page. Default: No
Default Ring	Type of ring heard. Choose from No Ring or 1 through 10. Ring options are Sunlight, Chirp 1, Chirp 2, Delight, Evolve, Mellow, Mischief, Reflections, Ringer, Ascent, Are you there, and Chime.
Auth Page Realm	Identifies the Realm part of the Auth that is accepted when the Auth Page parameter is set to Yes. This parameter accepts alphanumeric characters.
Conference Bridge URL	URL used to join into a conference call, generally in the form of the word conference or user@IPaddress:port.
Auth Page Password	Identifies the password used when the Auth Page parameter is set to Yes. This parameter accepts alphanumeric characters.
Mailbox ID	Identifies the voice mailbox number/ID for the phone.
Voice Mail Server	Identifies the SpecVM server for the phone, generally the IP address, and port number of the VM server.
Voice Mail Subscribe Interval	The expiration time, in seconds, of a subscription to a voice mail server.
Broadsoft ACD	Enables support for basic BroadSoft Automatic CallDistribution (ACD). The supported values for this option are Yes and No. Default: No
Auto Ans Page On Active Call	Determines the behavior of the phone when a page call arrives.
Feature Key Sync	Enable/disable the Feature Key synchronization. Applies to DND and Call Forward All features.

Parameter	Description
Call Park Monitor Enable	BroadSoft server only specific feature. If call park is enabled on the server or on any of the programmable line key, you need to enable this field for call park notification to work. Default: No
Enable Broadsoft Hoteling	When this parameter is set to yes, the phone sends out subscription message (without body) to the server. Default: No
Hoteling Subscription Expires	An expiration value that is added in the subscription message. Default value is 3600.

Proxy and Registration

Parameter	Description
Proxy	SIP proxy server and port number set by the service provider for all outbound requests. For example: 192.168.2.100:6060. The port number is optional. Default: 5060
Outbound Proxy	All outbound requests are sent as the first hop. Enter an IP address or domain name.
Alternate Proxy Alternate Outbound Proxy	This feature provides fast fall back when there is network partition at the Internet or when the primary proxy (or primary outbound proxy) is not responsive or available. The feature works well in a Verizon deployment environment as the alternate proxy is the Integrated Service Router (ISR) with analog outbound phone connection. Enter the proxy server addresses and port numbers in these fields. After the phone is registered to the primary proxy and the alternate proxy (or primary outbound proxy and alternate outbound proxy), the phone always sends out INVITE and Non-INVITE SIP messages (except registration) via the primary proxy. The phone always registers to both the primary and alternate proxies. If there is no response from the primary proxy after timeout (per the SIP RFC spec) for a new INVITE, the phone attempts to connect with the alternate proxy. The phone always tries the primary proxy first, and immediately tries the alternate proxy if the primary is unreachable. Active transactions (calls) never fall back between the primary and alternate proxies. If there is fall back for a new INVITE, the subscribe/notify transaction will fall back accordingly so that the phone's state can be maintained properly. You must also set Dual Registration in the Proxy and Registration section to Yes.

Parameter	Description
Use OB Proxy In Dialog	Determines whether to force SIP requests to be sent to the outbound proxy within a dialog. Ignored if the **Use Outbound Proxy** field is set to **No** or if the **Outbound Proxy** field is empty. Default: Yes
Register	Enables periodic registration with the proxy. This parameter is ignored if a proxy is not specified. To enable this feature, select **Yes**. Default: Yes
Make Call Without Reg	Enables making outbound calls without successful (dynamic) registration by the phone. If set to No, the dial tone plays only when registration is successful. To enable this feature, select **Yes**. Default: No
Register Expires	Defines how often the phone renews registration with the proxy. If the proxy responds to a REGISTER with a lower expires value, the phone renews registration based on that lower value instead of the configured value. If registration fails with an "Expires too brief" error response, the phone retries with the value specified in the Min-Expires header of the error. The range is from 32 to 2000000. Default: 3600 seconds
Ans Call Without Reg	If enabled, the user does not have to be registered with the proxy to answer calls. Default: No
Use DNS SRV	Enables DNS SRV lookup for the proxy and outbound proxy. To enable this feature, select **Yes**. Otherwise, select **No**. Default: No
DNS SRV Auto Prefix	Enables the phone to automatically prepend the proxy or outbound proxy name with _sip._udp when performing a DNS SRV lookup on that name. Default: No
Proxy Fallback Intvl	Sets the delay after which the phone retries from the highest priority proxy (or outbound proxy) after it has failed over to a lower priority server. The phone should have the primary and backup proxy server list from a DNS SRV record lookup on the server name. It needs to know the proxy priority; otherwise, it does not retry. The range is from 0 to 65535. Default: 3600 seconds

Parameter	Description
Proxy Redundancy Method	Select **Normal** or **Based on SRV Port**. The phone creates an internal list of proxies returned in the DNS SRV records. If you select Normal, the list contains proxies ranked by weight and priority. If you select Based on SRV Port, the phone uses normal, then inspects the port number based on the first-listed proxy port. Default: Normal
Dual Registration	Set to **Yes** to enable the Dual registration/Fast Fall back feature. To enable the feature you must also configure the alternate proxy/alternate outbound proxy fields in the Proxy and Registration section.
Auto Register When Failover	If set to No, the fallback happens immediately and automatically. If the Proxy Fallback Intvl is exceeded, all the new SIP messages go to the primary proxy. If set to Yes, the fallback happens only when current registration expires, which means only a REGISTER message can trigger fallback. For example, when the value for Register Expires is 3600 seconds and Proxy Fallback Intvl is 600 seconds, the fallback is triggered 3600 seconds later and not 600 seconds later. When the value for Register Expires is 600 seconds and Proxy Fallback Intvl is 1000 seconds, the fallback is triggered at 1200 seconds. After successfully registering back to primary server, all the SIP messages go to primary server.

Subscriber Information

Parameter	Description
Display Name	Name displayed as the caller ID.
User ID	Extension number for this line.
Password	Password for this line. Default: Blank (no password required)
Auth ID	Authentication ID for SIP authentication. Default: Blank

Parameter	Description
SIP URI	The parameter by which the user agent will identify itself for this line. If this field is blank, the actual URI used in the SIP signaling should be automatically formed as: sip:UserName@Domain where UserName is the username given for this line in the User ID, and Domain is the domain given for this profile in the User Agent Domain. If the User Agent Domain is an empty string, then the IP address of the phone should be used for the domain. If the URI field is not empty, but if a SIP or SIPS URI contains no @ character, the actual URI used in the SIP signaling should be automatically formed by appending this parameter with an @ character followed by the IP address of the device.

Audio Configuration

Parameter	Description
Preferred Codec	Preferred codec for all calls. The actual codec used in a call still depends on the outcome of the codec negotiation protocol. Select one of the following: • G711u • G711a • G729a • G729ab • G722 • G722.2 • iLBC • OPUS • iSAC Default: G711u
Use Pref Codec Only	Select **No** to use any code. Select **Yes** to use only the preferred codes. When you select Yes, calls fail if the far end does not support the preferred codecs. Default: No
Second Preferred Codec	Codec to use if the first codec fails. Default: Unspecified

Parameter	Description
Third Preferred Codec	Codec to use if the second codec fails. Default: Unspecified
G711u Enable	Enables use of the G.711u codec. Default: Yes
G711a Enable	Enables use of the G.711a codec. Default: Yes
G729a Enable	To enable use of the G.729a codec at 8 kbps, select **Yes**. Otherwise, select **No**. Default: Yes
G722 Enable	Enables use of the G.722 codec. Default: Yes
G722.2 Enable	Enables use of the G.722.2 codec. Default: No
iLBC Enable	Enables use of the iLBC codec. Default: Yes
OPUS Enable	Enables the use of OPUS codec. Default: Yes
Silence Supp Enable	To enable silence suppression so that silent audio frames are not transmitted, select **Yes**. Otherwise, select **No**. Default: No
DTMF Tx Method	The method for transmitting DTMF signals to the far end. The options are: • AVT—Audio video transport. Sends DTMF as AVT events. • InBand—Sends DTMF by using the audio path. • Auto—Uses InBand or AVT based on the outcome of codec negotiation. • INFO—Uses the SIP INFO method.
Use Remote Pref Codec	Lists all codecs or it uses the default codecs supported. Default: Default.

Parameter	Description
Codec Negotiation	When set to Default, the Cisco IP phone responds to an Invite with a 200 OK response advertising the preferred codec only. When set to List All, the Cisco IP phone responds listing all the codecs that the phone supports. The default value is Default, or to respond with the preferred codec only.
Encryption Method	Encryption method to be used during secured call. Options are AES 128 and AES 256 GCM Default: 128.

Dial Plan

Parameter	Description
Dial Plan	Dial plan script for the selected extension. The dial plan syntax allows the designation of three parameters for use with a specific gateway: • uid – The authentication user-id • pwd – The authentication password • nat – If this parameter is present, use NAT mapping. Separate each parameter with a semi-colon (;).
Caller ID Map	Inbound caller ID numbers can be mapped to a different string. For example, a number that begins with +44xxxxxx can be mapped to 0xxxxxx. This feature has the same syntax as the Dial Plan parameter. With this parameter, you can specify how to map a caller ID number for display on screen and recorded into call logs.
Enable URI Dialing	Enables or disables URI dialing.
Emergency Number	Enter a comma-separated list of emergency numbers. When one of these numbers is dialed, the unit disables processing of CONF, HOLD, and other similar softkeys or buttons to avoid accidentally putting the current call on hold. The phone also disables hook flash event handling. Only the far end can terminate an emergency call. The phone is restored to normalcy after the call is terminated and the receiver is back on-hook. Maximum number length is 63 characters. Defaults to blank (no emergency number).

Att Console

General

> **Note** The attendant console tab, labeled **Att Console**, is only available in **Admin Login** > **advanced** mode.

Parameter	Description
Subscribe Expires	Specifies how long the subscription remains valid. After the specified period of time elapses, the Cisco Attendant Console initiates a new subscription. Default: 1800
Subscribe Retry Interval	Specifies the length of time to wait to try again if the subscription fails. Default: 30
Subscribe Delay	Length of delay before attempting to subscribe. Default: 1
BLF List URL	Domain name or user name that is defined in the Broadsoft server for the phone. Default: Blank
Use Line Keys For BLF List	Options to enable or disable the line keys for BLF. Default: No
Call Pickup Audio Notification	By default, this parameter is set to **No**. If you set it to **Yes**, the phone plays the Call Pickup tone when there are incoming calls to any of the lines that the user is monitoring with the Call Pickup function. Default: No
BXfer to Starcode Enable	When set to **Yes**, the phone performs a blind transfer when the *code is defined in a speed dial extended function,. If set to **No**, the current call is held and a new call is started to the speed dial destination. Default: No
BXfer On Speed Dial Enable	When set to **Yes**, the phone performs a blind transfer when the speed dial function key is selected. When set to no, the current connected call is held and a new call to the speed dial destination is started. For example, when a user parks a call using the speed dial function, if the parameter is enabled, a blind transfer is performed to the parking lot. If the parameter is not enabled, an attended transfer is performed to the parking lot. Default: No

Parameter	Description
BLF Label Display Mode	Options to select a mode which displays on the phone screen for BLF. Default: Blank

Unit

Enter the programming information for each line key for the Attendant Console unit.

Parameter	Description
Unit Enable	Indicates whether the key expansion module that is added to the phone is enabled.
Unit Online	Indicates whether the key expansion module that is added to the phone is active.
HW Version	Displays the hardware version of the key expansion module that is added to the phone..
SW Version	Displays the software version of the key expansion module that is added to the phone.

TR-069

TR-069

Parameter	Description
Enable TR-069	Settings that enables or disables the TR-069 function.
ACS URL	URL of the ACS that uses the CPE WAN Management Protocol. This parameter must be in the form of a valid HTTP or HTTPS URL. The host portion of this URL is used by the CPE to validate the ACS certificate when it uses SSL or TLS.
ACS Username	Username that authenticates the CPE to the ACS when ACS uses the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE. If the user name is not configured, admin is used as default.

Parameter	Description
ACS Password	Password to access to the ACS for a specific user. This password is used only for HTTP-based authentication of the CPE. If the password is not configured, admin is used as default.
ACS URL In Use	URL of the ACS that is currently in use. This is a read-only field.
Connection Request URL	URL of the ACS that makes the connection request to the CPE.
Connection Request Username	Username that authenticates the ACS that makes the connection request to the CPE.
Connection Request Password	Password used to authenticate the ACS that makes a connection request to the CPE.
Periodic Informal Interval	Duration in seconds of the interval between CPE attempts to connect to the ACS when Periodic Inform Enable is set to yes. Default value is 20 seconds.
Periodic Inform Enable	Settings that enables or disables the CPE connection requests. Default value is Yes.
TR-069 Traceability	Settings that enables or disables TR-069 transaction logs. The default value is No.
CWMP V1.2 Support	Settings that enables or disables CPE WAN Management Protocol (CWMP) support. If set to disable, the phone does not send any Inform messages to the ACS nor accept any connection requests from the ACS. Default value is Yes.
TR-069 VoiceObject Init	Settings to modify voice objects. Select Yes to initialize all voice objects to factory default values or select No to retain the current values.
TR-069 DHCPOption Init	Settings to modify DHCP settings. Select Yes to initialize the DHCP settings from the ACS or select No to retain the current DHCP settings.

Parameter	Description
TR-069 Fallback Support	Settings that enables or disables the TR-069 fallback support. If the phone attempts to discover the ACS with DHCP and is unsuccessful, the phone next uses DNS to resolve the ACS IP address.
BACKUP ACS URL	Backup URL of the ACS that uses the CPE WAN Management Protocol. This parameter must be in the form of a valid HTTP or HTTPS URL. The host portion of this URL is used by the CPE to validate the ACS certificate when it uses SSL or TLS.
BACKUP ACS User	Backup username that authenticates the CPE to the ACS when ACS uses the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
BACKUP ACS Password	Backup password to access to the ACS for a specific user. This password is used only for HTTP-based authentication of the CPE.

Note If you do not configure the above parameters, you can also fetch them through DHCP options 60,43, and 125.

Call History

Displays the call history for the phone. To change the information displayed, select the type of call history from the following tabs:

- All Calls
- Missed
- Received
- Placed

Select **Add to Directory** to add the call information to your Personal Directory.

Personal Directory

The Personal Directory allows a user to store a set of personal numbers. Directory entries can include the following contact information:

- No. (the directory number)
- Name

- Work
- Mobile
- Home
- Speed Dials

To edit contact information, click **Edit Contacts**.

CHAPTER 10

Troubleshooting

General Troubleshooting Information

The following table provides general troubleshooting information for the Cisco IP Phone.

Table 9: Cisco IP Phone Troubleshooting

Summary	Explanation
Connecting a Cisco IP Phone to another Cisco IP Phone	Cisco does not support connecting an IP phone to another IP Phone through the PC port. Each IP Phone should connect directly to a switch port. If phones are connected together in a line by using the PC port, the phones do not work. **Note** The Cisco 7832 conference phone does not have a PC port.
Prolonged broadcast storms cause IP phones to reset, or be unable to make or answer a call	A prolonged Layer 2 broadcast storm (lasting several minutes) on the voice VLAN may cause IP phones to reset, lose an active call, or be unable to initiate or answer a call. Phones may not come up until a broadcast storm ends.

Summary	Explanation
Moving a network connection from the phone to a workstation	If you power your phone through the network connection, you must be careful if you decide to unplug the network connection of the phone and plug the cable into a desktop computer. **Caution** The network card in the computer cannot receive power through the network connection; if power comes through the connection, the network card can be destroyed. To protect a network card, wait 10 seconds or longer after unplugging the cable from the phone before plugging it into a computer. This delay gives the switch enough time to recognize that there is no longer a phone on the line and to stop providing power to the cable.
Changing the telephone configuration	By default, the administrator password settings are locked to prevent users from making changes that could impact their network connectivity. You must unlock the administrator password settings before you can configure them. **Note** If the administrator password is not set in common phone profile, then user can modify the network settings.
Codec mismatch between the phone and another device	The RxType and the TxType statistics show the codec that is used for a conversation between this Cisco IP Phone and the other device. The values of these statistics should match. If they do not, verify that the other device can handle the codec conversation, or that a transcoder is in place to handle the service. See Display Call Statistics Window, on page 109 for details.
Sound sample mismatch between the phone and another device	The RxSize and the TxSize statistics show the size of the voice packets that are used in a conversation between this Cisco IP Phone and the other device. The values of these statistics should match. See Display Call Statistics Window, on page 109 for details.
Loopback condition	A loopback condition can occur when the following conditions are met: • The SW Port Configuration option on the phone is set to 10 Half (10-BaseT/half duplex). • The phone receives power from an external power supply. • The phone is powered down (the power supply is disconnected). In this case, the switch port on the phone can become disabled and the following message appears in the switch console log: HALF_DUX_COLLISION_EXCEED_THRESHOLD To resolve this problem, reenable the port from the switch.

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.

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 with the handset off-hook. When the phone is powered up in this way, it attempts to launch a 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.

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.

Phone Cannot Connect Using DNS

Problem

The DNS settings may be incorrect.

Solution

If you use DNS to access the TFTP server or Third-Party Call Control Manager, you must ensure that you specify a DNS server.

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

Get a new configuration file remotely from the provisioning server using `resync`.

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 on their desk, you should investigate the cause. If the network connection and Third Party Call Control connection are stable, a Cisco IP Phone should not reset.

Typically, a phone resets if it has problems in connecting to the Ethernet network or to Third Party Call Control.

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.

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 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.

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.

Audio Problems

The following sections describe how to resolve audio 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.

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. The phones display the message Configuring IP or Registering.

Solution

1. Verify the following:
    a. The Ethernet cable is attached.
    b. The Third-Party Call Control system is active.
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.

Report All Phone Issues with the Configuration Utlility

If you are working with Cisco TAC to troubleshoot a problem, they typically require the logs from the Problem Reporting Tool to help resolve the issue. You can generate PRT logs using the Configuration Utlility and upload them to a remote log server.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **advanced** > **Info** > **Debug Info**.

Step 2 In the **Problem Reports** section, click **Generate PRT**.
The **Report Problem** dialog appears.

Step 3 Enter the following information in the **Report Problem** dialog:

a) Enter the date that you experienced the problem in the **Date** field. The current date appears in this field by default.
b) Enter the time that you experienced the problem in the **Time** field. The current time appears in this field by default.
c) In the **Select Problem** drop-down list box, choose the description of the problem from the available options.

Step 4 Click **Submit** in the **Report Problem** dialog.
The Submit button is enabled only if you select a value in the **Select Problem** drop-down list box.

You get a notification alert on the Configuration Utility page that indicates if the PRT upload was successful or not.

Troubleshooting Procedures

These procedures can be used to identify and correct problems.

Check DHCP Settings

Procedure

Step 1 On the phone, press **Settings**.

Step 2 Check the DHCP server field.
Check the DHCP option for enabled or disabled.

Step 3 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 4 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

Verify DNS Settings

Procedure

Step 1 On the phone, press **Settings**.

Step 2 Check that the DNS Server 1 field is set correctly.

Step 3 You should also verify that a CNAME entry was made in the DNS server for the TFTP server and for the Third-Party Call Control.
You must also ensure that DNS is configured to do reverse lookups.

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/cisco/web/psa/troubleshoot.html

CHAPTER 11

Maintenance

Basic Reset

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

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

Table 10: Basic Reset Methods

Operation	Action	Explanation
Restart phone	Press **Settings** and choose **Admin Settings** > **Cold Reboot**.	Resets any user and network setup changes that you have made, but that the phone has not written to its Flash memory, to previously saved settings, then restarts the phone.
Reset settings	To reset settings, press **Setings** and choose **Admin Settings** > **Factory Reset**.	Restores phone configuration or settings to factory default.

Perform a Factory Reset with the Phone Keypad

Use these steps to reset the phone to factory default settings using the phone keypad.

Procedure

Step 1 Unplug the phone:

- If using PoE, unplug the LAN cable.
- If using the power cube, unplug the power cube.

Step 2 Wait 5 seconds.

Step 3 Press and hold # and plug the phone back in.

Step 4 When the phone boots up, the headset button, the speaker button, and the mute button light up. When the light on the Mute button turns off, press **123456789*0#** in sequence.
When you press **1**, the lights on the headset button turns off. The light on the Select button flashes when a button is pressed.

After you press these buttons, the phone goes through the factory reset process.

If you press the buttons out of sequence, the phone powers on normally.

Caution Do not power down the phone until it completes the factory reset process, and the main screen appears.

Perform Factory Reset from Phone Menu

Procedure

Step 1 Press **Settings**.

Step 2 Scroll to **Admin Settings** and select **Factory Reset**.

Step 3 To restore phone configuration or settings to factory default, press **Ok**.

Factory Reset the Phone from Phone Web Page

You can restore your phone to its original manufacturer settings so that the phone can be reconfigured, do it from the phone web page.

Procedure

Enter the URL in a supported web browser and click **Confirm Factory Reset**.
You can enter URL in the format:

```
http://<Phone IP>/admin/factory-reset
```

where:

Phone IP = actual IP address of your phone.

/admin = path to access admin page of your phone.

factory-reset = command that you need to enter in the phone web page to factory-reset your phone.

Identify Phone Issues with a URL in the Phone Web Page

When the phone is not working or doesn't register, a network error or any misconfiguration might be the cause. To identify the cause, add a specific IP address or a domain name to the phone admin page. Then, try to access so that the phone can ping the destination and display the cause.

Procedure

In a supported web browser, enter a URL that consist of your phone IP address and the destination IP that you want to ping.
Enter a URL in the format:

```
http:/<Phone IP>/admin/ping?<ping destination>
```

where:

Phone IP = actual IP address of your phone.

/admin = path to access admin page of your phone.

ping destination = any IP address or domain name that you want to ping. Only alphanumeric characters, '-', and "_" are allowed as the ping destination. Otherwise the phone shows an error on the web page. If the <ping destination> includes spaces, only the first part of the address is used as the pinging destination. For example, "http://<Phone IP>/admin/ping?192.168.1.1 cisco.com" will actually ping 192.168.1.1.

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 11: 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.

Voice Quality Reporting

You can capture voice quality metrics for Voice over Internet Protocol (VoIP) sessions with a Session Initiation Protocol (SIP) event package. Voice call quality information derived from RTP and call information from SIP is conveyed from a User Agent (UA) in a session (reporter) to a third party (collector).

The Cisco IP phone uses User Datagram Protocol (UDP) to send a SIP PUBLISH message to a collector server.

Supported Scenarios for Voice Quality Reporting

Currently, only the basic call scenario supports voice quality reporting. A basic call can be a peer to peer incoming or outgoing call. The phone sends the SIP Publish message when a call ends.

Mean Opinion Scores and Codecs

The voice quality metrics use Mean Opinion Score (MOS) to rate the quality. A MOS rating of 1 is the lowest quality; a MOS rating of 5 is the highest quality. The following table gives a description of the codecs and MOS scores. For other codecs, the phone does not send the SIP Publish message.

Codec	Complexity and Description	MOS	Minimum Call Duration for Valid MOS Value
G.711 (A-law and u-law)	Very low complexity. Supports uncompressed 64 kbps digitized voice transmission at one to ten 5 ms voice frames-per-packet. This codec provides the highest voice quality and uses the most bandwidth of any of the available codecs.	A minimum value of 4.1 indicates good voice quality.	10 seconds
G.729A	Low to medium complexity.	A minimum value of 3.5 indicates good voice quality.	30 seconds
G.729AB	Contains the same reduced complexity modifications present in the G.729A.	A minimum value of 3.5 indicates good voice quality.	30 seconds

Configure Voice Quality Reporting

You can enable voice quality reporting on the phone with the web interface. Each extension on a phone has a separate voice quality report. For each extension on the phone, use the corresponding **Voice Quality Report Address** field to configure the generation of voice quality report.

Procedure

Step 1 On the Configuration Utility page, select **Admin Login** > **advanced** > **Voice** > **Ext x**.
Where:

- Ext x = the extension number on the phone

Step 2 In **SIP Settings**, enter a value in the **Voice Quality Report Address x** field. You can enter either a domain name or an IP address in this field.
You can also add a port number along with the domain name or an IP address in this field. If you do not enter a port number, the value of the **SIP UDP Port** (5060) is used by default. If the collector server URL parameter is blank, a SIP PUBLISH message is not sent out.

Step 3 Click **Submit All Changes**.

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.

View Phone Information

Procedure

To check the current status of the Cisco IP Phone, click the **Info** tab.
The Info tab shows information about all phone extensions, including phone statistics and the registration status.

Reboot Reasons

The phone stores the most recent five reasons that the phone was refreshed or rebooted. When the phone is reset to factory defaults, this information is deleted.

The following table describes the reboot and refresh reasons for the Cisco IP Phone.

Reason	Description
Upgrade	The reboot was a result of an upgrade operation (regardless whether the upgrade completed or failed).

Reason	Description
Provisioning	The reboot was the result of changes made to parameter values by using the IP phone screen or phone web user interface, or as a result of synchronization.
SIP Triggered	The reboot was triggered by a SIP request.
RC	The reboot was triggered as a result of remote customization.
User Triggered	The user manually triggered a cold reboot.
IP Changed	The reboot was triggered after the phone IP address changed.

You can view the reboot history as follows:

- From the phone web user interface
- From the IP phone screen
- From the phone Status Dump file (http://*phoneIP*/status.xml or http://*phoneIP*/admin/status.xml)

Reboot History on the Phone Web User Interface

On the **Info** > **System Status** page, the **Reboot History** section displays the device reboot history, the five most recent reboot dates and times, and a reason for the reboot. Each field displays the reason for the reboot and a time stamp that indicates when the reboot took place.

For example:

```
Reboot Reason 1: [08/13/14 06:12:38] User Triggered
Reboot Reason 2: [08/10/14 10:30:10] Provisioning
Reboot Reason 3: [08/10/14 10:28:20] Upgrade
```

The reboot history displays in reverse chronological order; the reason for the most recent reboot displays in **Reboot Reason 1**.

Reboot History on the Cisco IP Phone Screen

Reboot History is located under **Apps** > **Admin Settings** > **Status** menu. In the Reboot History window, the reboot entries displays in reverse chronological order, similar to the sequence that displays on the phone web user interface.

Reboot History in the Status Dump File

The reboot history is stored in the Status Dump file (http://<*phone_IP_address*>/admin/status.xml).

In this file, tags **Reboot_Reason_1** to **Reboot_Reason_3** store the reboot history, as shown in this example:

```
<Reboot_History>
<Reboot_Reason_1>[08/10/14 14:03:43]Provisioning</Reboot_Reason_1>
<Reboot_Reason_2>[08/10/14 13:58:15]Provisioning</Reboot_Reason_2>
<Reboot_Reason_3>[08/10/14 12:08:58]Provisioning</Reboot_Reason_3>
<Reboot_Reason_4>
```

```
<Reboot_Reason_5>
<Reboot_History/>
```

Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect Cisco IP Phone voice and video quality, and in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

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

To reduce or eliminate any adverse effects to the phones, schedule administrative network tasks during a time when the phones are not being used or exclude the phones from testing.