Preface ix
Overview ix
Who Should Use This Guide ix
Objectives x
Document Organization x
Document Conventions x
Related Documentation xi
Obtaining Documentation xi
Cisco.com xii
Documentation CD-ROM xii
Ordering Documentation xii
Documentation Feedback xii
Obtaining Technical Assistance xiii
Cisco.com xiii
Technical Assistance Center xiii
Cisco TAC Website xiv
Cisco TAC Escalation Center xiv
Obtaining Additional Publications and Information xiv

CHAPTER 1

Product Overview 1-1
What’s New in This Release? 1-1
Components of SIP 1-2
SIP Clients 1-3
SIP Servers 1-3
What Is the Cisco SIP IP Phone? 1-4
BTXML Support 1-5
Cisco CallManager XML Support 1-5
Supported Features 1-6
Physical Features 1-6
Network Features 1-7
Configuration Features 1-7
Codec and Protocol Support 1-7
Dialing and Messaging Features 1-8
Getting Started with Your Cisco SIP IP Phone

Overview of the Initialization Process
Installing the Cisco SIP IP Phone
Installation Task Summary
Downloading Files to Your TFTP Server
Configuring SIP Parameters
  Configuring SIP Parameters Using a TFTP Server
  Configuring the SIP Parameters Manually
Configuring Network Parameters
  Configuring Network Parameters Using a DHCP Server
  Configuring the Network Parameters Manually
Connecting the Phone
  Adjusting the Placement of the Cisco SIP Phone
Verifying Startup
Using the Cisco SIP IP Phone Menu Interface
Reading the Cisco SIP IP Phone Icons
Customizing the Cisco SIP IP Phone Ring Types
Creating Dial Plans
  Updates to the Dial-Plan Template in Release 4.4 and Later
    Specifying the # in the Dial-Plan Template Example
    Specifying the * in the Dial-Plan Template Example
    Specifying a Secondary Dial Tone in the Dial-Plan Template Example

Managing Cisco SIP IP Phones
Changing Your Configuration
Contents

Chapter 3
Modifying the Network Settings 3-2
   Entering Configuration Mode 3-2
Unlocking Configuration Mode
   In Release 4.2 or Later 3-2
   In Release 4.1 or Earlier 3-2
Locking Configuration Mode
   In Release 4.2 or Later 3-3
   In Release 4.1 or Earlier 3-3
Changing the Network Settings 3-3

Modifying the SIP Settings 3-6
   Modifying SIP Parameters via a TFTP Server 3-9
   Modifying the Default SIP Configuration File 3-9
      Modifying the Phone-Specific SIP Configuration File 3-24
   Modifying the SIP Parameters Directly on Your Phone 3-26

Modifying Call Preferences 3-29
Setting the Date, Time, and Daylight Saving Time 3-30

Erasing the Locally Defined Settings 3-35
   Erasing the Locally Defined Network Settings 3-35
   Erasing the Locally Defined SIP Settings 3-35
   Viewing the Firmware Version 3-36

Upgrading the Cisco SIP IP Phone Firmware 3-37
   Upgrading to Release 5.0 and Release 5.1 3-37
   Upgrading from Release 2.2 or Later to Current Release 3-38
   Upgrading from Release 2.1 or Earlier to Current Release 3-39
   Dual Booting from SCCP or MGCP to a SIP Release 3-39

Performing an Image Upgrade and Remote Reboot 3-40

Chapter 4
Monitoring and Maintaining 4-1
   Using the Command-Line Interface (CLI) 4-1
      Accessing Status Information 4-7
         Viewing Status Messages 4-8
         Viewing Network Statistics 4-8
      Accessing Status Information 4-9
         Viewing Status Messages 4-9
         Viewing Network Statistics 4-10

Appendix A
Information About SIP Compliance with RFC 3261 A-1
      SIP Functions  A-1
SIP Methods A-2
SIP Responses A-2
  1xx Response—Information Responses A-2
  2xx Response—Successful Responses A-3
  3xx Response—Redirection Responses A-3
  4xx Response—Request Failure Responses A-4
  5xx Response—Server Failure Responses A-6
  6xx Response—Global Responses A-7
SIP Header Fields A-7
SIP Session Description Protocol Usage A-8
Transport Layer Protocols A-9
SIP Security Authentication A-9
SIP DNS Records Usage A-9
SIP DTMF Digit Transport A-9

APPENDIX B

SIP Call Flows B-1
  Call Flow Scenarios for Successful Calls B-1
    Gateway to Cisco SIP IP Phone B-2
      Call Setup and Disconnect B-2
      Call Setup and Hold B-4
      Call to a Gateway Acting as an Emergency Proxy from a Cisco SIP IP Phone B-6
    Cisco SIP IP Phone to Cisco SIP IP Phone B-7
      Simple Call Hold B-8
      Call Hold with Consultation B-10
      Call Waiting B-14
      Call Transfer Without Consultation B-18
      Call Transfer Without Consultation Using Failover B-22
      Call Transfer with Consultation B-25
      Call Transfer with Consultation Using Failover B-30
      Network Call Forwarding (Unconditional) B-34
      Network Call Forwarding (Busy) B-36
      Network Call Forwarding (No Answer) B-38
      Three-Way Calling B-41
    Call from a Cisco SIP IP Phone to a Gateway Acting as a Backup Proxy B-46
    Call from a Cisco SIP IP Phone to a Cisco SIP IP Phone By Way of a Backup Proxy B-48
    Call from Cisco SIP IP Phone to Cisco SIP IP Phone Using an Emergency Proxy B-50
  Call Flow Scenarios for Failed Calls B-52
    Gateway to Cisco SIP IP Phone B-52
    Called User Is Busy B-52
Preface

This chapter describes the objectives and organization of the Cisco SIP IP Phone Administrator Guide, Release 5.0 and Release 5.1 and explains how to find additional information on related products and services. It contains the following sections:

- Overview, page ix
- Who Should Use This Guide, page ix
- Objectives, page x
- Document Organization, page x
- Document Conventions, page xi
- Related Documentation, page xi
- Obtaining Documentation, page xi
- Obtaining Technical Assistance, page xiii

Overview

The Cisco SIP IP Phone Administrator Guide provides information about how to set up, connect cables to, and configure a Cisco Session Initiation Protocol (SIP) IP Phone 7940 or 7960 (hereafter referred to as a Cisco SIP IP phone). It also provides information on how to configure the network and SIP settings and change the settings and options of the Cisco SIP IP phone. The administrator guide also includes reference information such as Cisco SIP IP phone call flows and compliance information.

Who Should Use This Guide

Network engineers, system administrators, or telecommunications engineers should use this guide to learn the tasks required to set up the Cisco SIP IP phone in the network. The described tasks are administration-level tasks and are not intended for the end users of the phones. Many of the tasks involve configuring network settings that could affect the ability of the phone to function in the network and require an understanding of IP networking and telephony concepts.
Objectives

The Cisco SIP IP Phone Administrator Guide, Release 5.0 and Release 5.1 provides necessary information to get the Cisco SIP IP phone operational in a Voice-over-IP (VoIP) network. It is not the intent of this administrator guide to provide information on how to implement a SIP VoIP network. For information on implementing a SIP VoIP network, refer to the documents listed in the “Related Documentation” section on page xi.

Document Organization

This document is organized into the following chapters:

- **Chapter 1, “Product Overview”**—Describes SIP and the Cisco SIP IP phone.
- **Chapter 2, “Getting Started with Your Cisco SIP IP Phone”**—Describes how to install, connect, and configure the Cisco SIP IP phone.
- **Chapter 3, “Managing Cisco SIP IP Phones”**—Describes how to modify the Cisco SIP IP phone network and settings, how to access network and call status information, and how to upgrade the firmware.
- **Chapter 4, “Monitoring and Maintaining”**—Lists and describes debugging commands and other commands that can be used to troubleshoot the phone and network.
- **Appendix A, “Information About SIP Compliance with RFC 3261”**—Provides reference information about the Cisco SIP IP phone compliance to RFC 3261.
- **Appendix B, “SIP Call Flows”**—Provides reference information about the Cisco SIP IP phone call flows.
- **Appendix C, “Technical Specifications”**—Lists the physical and operating environment specifications, cable specifications, and connection specifications.
- **Appendix D, “Translated Safety Warnings”**—Lists translated safety warnings that should be followed when installing an electrical device such as the Cisco SIP IP phone.

Document Conventions

This document uses the following conventions:

- Commands and keywords are in **boldface** font.
- Arguments for which you supply values are in *italic* font.
- Elements in square brackets ([ ]) are optional.
- Required alternative keywords are grouped in braces and separated by vertical bars (for example, `{x | y | z}`).
- Optional alternative keywords are grouped in brackets and separated by vertical bars (for example, `[x | y | z]`).
- Terminal sessions and information that the system displays are in `screen` font.
- Information that you must enter is in **boldface screen** font.
- The pound sign (#), backward slash (\) and asterisk (*) on a telephone keypad are referred to as #, \, and * in this document.
Related Documentation

The following is a list of related Cisco SIP VoIP publications. For more information about implementing a SIP VoIP network, refer to the following publications:

- Session Initiation Protocol Gateway Call Flows
- Cisco IP Phone 7960 and 7940 Series at a Glance
- Regulatory Compliance and Safety Information for the Cisco IP Phone 7960, 7940, and 7910 Series
- Installing the Wall Mount Kit for the Cisco IP Phone

The following is a list of Cisco VoIP publications that provide information about implementing a VoIP network:

- Cisco IOS Voice Library, Release 12.3
- Cisco IOS Voice Command Reference, Release 12.3
- Cisco IOS IP Configuration Guide, Release 12.3
- Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.3
- Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.3

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.
Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:
http://www.cisco.com/univercd/home/home.htm
You can access the Cisco website at this URL:
http://www.cisco.com
International Cisco websites can be accessed from this URL:

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:
All users can order monthly or quarterly subscriptions through the online Subscription Store:
http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:
You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click Feedback at the top of the page.
You can e-mail your comments to bug-doc@cisco.com.
You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL: http://tools.cisco.com/RPF/register/register.do

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
Preface

Obtaining Additional Publications and Information

- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:


If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:


Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

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

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:


http://www.ciscopress.com

*Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

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

*iQ* Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access *iQ* Magazine at this URL:

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

Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:


Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

Product Overview

This chapter contains the following information about the Cisco SIP IP phone:

- What’s New in This Release?, page 1-1
- What Is the Cisco SIP IP Phone?, page 1-4
- Prerequisites, page 1-12
- Cisco SIP IP Phone Connections, page 1-12
- The Cisco SIP IP Phone with a Catalyst Switch, page 1-14

What’s New in This Release?

Release 5.0
Cisco has added image authentication to IP phone protocols, which means that tampering of the binary image is not allowed before the image is downloaded to the phone. Any tampering with the image will cause the phone to fail the authentication process and reject the image. Once you download the Release 5.0 image, you cannot downgrade to any earlier releases. See “Upgrading to Release 5.0 and Release 5.1” section on page 3-37.

Release 5.1
Release 5.1 is the second release of the signed Cisco IP phone image. Release 5.1 is compatible with Release 5.0 and later releases. Release 5.1 addresses user interface responsiveness and voice clipping issues. See “Upgrading to Release 5.0 and Release 5.1” section on page 3-37.
What Is Session Initiation Protocol?

Session Initiation Protocol (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.

SIP provides the capabilities to do the following:

- Determine the location of the target endpoint—SIP supports address resolution, name mapping, and call redirection.
- Determine the media capabilities of the target endpoint—Via Session Description Protocol (SDP), SIP determines the “lowest level” of common services between the endpoints. Conferences are established using only the media capabilities that can be supported by all endpoints.
- Determine the availability of the target endpoint—If a call cannot be completed because the target endpoint is unavailable, SIP determines whether the called party is already on the phone or did not answer in the allotted number of rings. It then returns a message that indicates why the target endpoint was unavailable.
- Establish a session between the originating and target endpoint—If the call can be completed, SIP establishes a session between the endpoints. SIP also supports midcall changes, such as the addition of another endpoint to the conference or the changing of a media characteristic or codec.
- Handle the transfer and termination of calls—SIP supports the transfer of calls from one endpoint to another. During a call transfer, SIP simply establishes a session between the transferee and a new endpoint (specified by the transferring party) and terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates the sessions between all parties.

Conferences can consist of two or more users and can be established using multicast or multiple unicast sessions.

---

Note

The term *conference* means an established session (or call) between two or more endpoints. In this document, the terms conference and call are used interchangeably.

Components of SIP

SIP is a peer-to-peer protocol. The peers in a session are called user agents (UAs). A user agent can function in one of the following roles:

- User agent client (UAC)—A client application that initiates the SIP request.
- User agent server (UAS)—A server application that contacts the user when a SIP request is received and that returns a response on behalf of the user.

Typically, a SIP endpoint is capable of functioning as both a UAC and a UAS, but functions only as one or the other per transaction. Whether the endpoint functions as a UAC or a UAS depends on the UA that initiated the request.

From an architecture standpoint, the physical components of a SIP network can also be grouped into two categories: clients and servers. Figure 1-1 illustrates the architecture of a SIP network.
In addition, the SIP servers can interact with other application services, such as Lightweight Directory Access Protocol (LDAP) servers, a database application, or an eXtensible Markup Language (XML) application. These application services provide back-end services such as directory, authentication, and billing services.

**Figure 1-1 SIP Architecture**

SIP clients include the following:
- Phones—Acts as either a UAS or UAC. Softphones (PCs that have phone capabilities installed) and Cisco SIP IP phones can initiate SIP requests and respond to requests.
- Gateways—Provides call control. Gateways provide many services, the most common being a translation function between SIP conferencing endpoints and other terminal types. This function includes translation between transmission formats and between communications procedures. In addition, the gateway also translates between audio and video codecs and performs call setup and clearing on both the LAN side and the switched-circuit network side.

SIP servers include the following:
- Proxy server—Receives SIP requests from a client and then forwards the requests because it is an intermediate device. Basically, proxy servers receive SIP messages and forward them to the next SIP server in the network. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.
What Is the Cisco SIP IP Phone?

Cisco SIP IP phones are full-featured telephones that can be plugged directly into an IP network and can be used very much like a standard PBX telephone. The Cisco SIP IP phone is an IP telephony instrument that can be used in VoIP networks.

The Cisco SIP IP phone terminals can attach to the existing data network infrastructure, via 10BASE-T/100BASE-T interfaces on an Ethernet switch. When used with a voice-capable Ethernet switch (one that understands type of service [ToS] bits and can prioritize VoIP traffic), the phones eliminate the need for a traditional proprietary telephone set and key system and PBX.

The Cisco SIP IP phone complies with RFC 3261, as described in Appendix A, “Information About SIP Compliance with RFC 3261.”

Figure 1-2 illustrates the physical features of the Cisco SIP IP phone.

- LCD screen—Desktop, which displays information about your Cisco SIP IP phone, such as the time, date, your phone number, caller ID, line and call status, and the soft key tabs.
- Line or speed-dial buttons—Opens a new line or speed dials the number on the LCD screen.
- Footstand adjustment—Adjusts the angle of the phone base.
What Is the Cisco SIP IP Phone?

- **Soft keys**—Activates the feature described by the text message directly above on the LCD screen.
- **Information (i) button**—Provides online help for selected keys or features and network statistics about the active call. Pressing the i button and then the up or down scroll key displays a descriptor of the key. For example, pressing the i button, then the up or down scroll key, displays a screen instructing you how to scroll up and down on the LCD.
- **On-screen mode buttons**—Retrieves information about current settings, recent calls, available services, and voice-mail messages.
- **Volume buttons**—Adjusts the volume of the handset, headset, speaker, and ringer and adjust the brightness contrast settings on the LCD screen.
- **Function toggles**—Includes the following options:
  - Headset and speaker—Toggles these functions enabling you to answer the phone using a headset or speakerphone.
  - Mute—Stops or resumes voice transmission.
- **Scroll key**—Enables you to move among different soft key options displayed on the LCD screen.
- **Dialing pad**—Press the dial-pad buttons to dial a phone number. Dial-pad buttons work exactly like those on your existing telephone.
- **Handset**—Lift the handset and press the dial-pad numbers to place a call, review voice-mail messages, or answer a call.

**BTXML Support**

Basic Telephony eXtensible Markup Language (BTXML) is supported on the Cisco SIP IP phone. BTXML defines XML elements for controlling the user interface of an IP telephone. BTXML describes what information is displayed on the screen and how the user provides input using soft keys and hard keys. User interface control is internal to the phone; there is no external BTXML user interface control.

**Cisco CallManager XML Support**

The Cisco SIP IP phone supports customer-written Cisco CallManager XML cards that can be accessed using buttons or soft keys on the phone. These cards can provide data such as stock quotes, calendars, and directory lookups. The XML cards can be accessed by the following methods:

- From the Services soft key, configured using the services_url parameter.
- By pressing the directory button and selecting External Directory, configured using the directory_url parameter.
- By downloading a bit-map to be used as the phone logo (branding), configured using the logo_url parameter.

See Chapter 3, “Managing Cisco SIP IP Phones,” for information about configuring these parameters. The Cisco SIP IP phone supports Cisco CallManager XML up to version 3.0 but does not support the XML objects added in Cisco CallManager XML version 3.1, which are:

- CiscoIPPhoneIconMenu
- CiscoIPPhoneExecute
- CiscoIPPhoneError
- CiscoIPPhoneResponse
The following exceptions apply to the Cisco SIP IP phone:

- External directories cannot be appended to the main list of directories under the directory button. If external directories are provisioned for the Cisco SIP IP phone, they can be accessed by pressing the directory button and selecting the External Directory option.
- The Cisco SIP IP phone removes white space when the Cisco CallManager XML cards are displayed. Multiple spaces are consolidated into a single space.
- Setting \( x \) and \( y \) coordinates for the CiscoIPPhoneImage object is not supported. The image always appears at location 0,0. Centering of the image is not supported if \( x \) and \( y \) are set to –1.
- The Cisco SIP IP phone displays any valid title it receives. This differs from the Cisco CallManager phones in that the CiscoIPPhoneGraphicMenu object does not display a title even if it receives one and the CiscoIPPhoneImage object displays the previous menu item or “Services” rather than received titles.
- Cisco CallManager phones allow embedded carriage returns and line feeds in menu items. In the Cisco SIP IP phone, carriage returns and line feeds are discarded.
- The Cisco SIP IP phone always displays the full set of directory soft keys. For Cisco CallManager phones, the soft keys can change depending on what type of object it receives.
- A parameter is sent along with the initial request for a Services or Directory URL, which differentiates the Cisco SIP IP phone from other types of phones.

For more information about using XML on your Cisco SIP IP phone, refer to the following links or documents:

- IP Telephony at the following URL: http://www.hotdispatch.com/cisco-ip-telephony
- Cisco CallManager Services Developer Kit at the following URL: http://www.cisco.com/warp/public/570/avvid/voice_ip/cm_xml/cm_xmldown.shtml
- Developing Cisco IP Phone Services by Darrick Deel, Mark Nelson, and Anne Smith, ISBN 1-58705-060-9.

### Supported Features

In addition to the features illustrated in Figure 1-2 on page 1-4, the Cisco SIP IP phone also provides the following features.

### Physical Features

- Adjustable ring tone.
- Hearing-aid compatible handset.
- Headset compatibility.
- Integrated two-port Ethernet switch that allows the telephone and a computer to share a single Ethernet jack.
- Direct connection to a 10BASE-T or 100BASE-T Ethernet (RJ-45) network (half- or full-duplex connections are supported).
- Large (4.25 x 3 in or 10.79 x 7.62 cm) display with adjustable contrast.
Chapter 1  Product Overview

What Is the Cisco SIP IP Phone?

Network Features

- IP address assignment—Using Dynamic Host Configuration Protocol (DHCP) client or manually configuring using a local setup menu.
- Network startup using DHCP and TFTP.
- Telnet support—Allows the user to use Telnet to connect directly to the Cisco SIP IP phone to debug and troubleshoot the phone. See the “Managing Cisco SIP IP Phones” section on page 3-1 for more information on configuration parameters.
- Ping support—Allows the user to use ping to see if a Cisco SIP IP phone is operational and how long the response time is from the phone.
- Traceroute support—Allows the user to use traceroute to see the path that a Cisco SIP IP phone traverses in the route to its desired destination.

Configuration Features

The Cisco SIP IP phone provides the ability to do the following:
- Configure Ethernet port mode and speed
- Register with or unregister from a proxy server
- Register with or unregister from a backup proxy server
- Specify a TFTP boot directory
- Configure a label for phone identification display purposes
- Configure a name for caller identification purposes for each active line on a phone
- Configure a 12- or 24-hour user interface time display
- Lock and unlock the phone from the Settings menu

Codec and Protocol Support

- G.711 (u-law and a-law) and G.729a audio compression.
- In-band dual tone multifrequency (DTMF) support for touch-tone dialing.
- Out-of-band DTMF signaling for codecs that do not transport the DTMF signaling correctly (for example, G.729 or G.729a).
- Local (180 Ringing) or remote (183 Session Progress) call progress tone.
- Audio/Video Transport (AVT) payload type negotiation.
- Current date and time support via Simple Network Time Protocol (SNTP) and time zone and daylight saving time support.
- Call redirection information support via the Diversion header.
- Third-party call control via delayed media negotiation. A delayed media negotiation is one where the Session Description Protocol (SDP) information is not completely advertised in the initial call setup.
- Support for endpoints specified as fully qualified domain names (FQDNs) in the SDP.
- Remote reset and dial-plan update support (via the Event header in NOTIFY messages).

Refer to the “Supported Protocols” section on page 1-11 for additional supported protocols.
Dialing and Messaging Features

- Dial-plan support that enables automatic dialing and automatic generation of a secondary dial tone.
- Local directory configuration (save and recall) and automatic dial completion—Each time a call is successfully made or received, the number is stored in a local directory that is maintained on the phone. The maximum number of entries is 32. Entries are aged-out according to usage and age. The oldest entry that has been called the least number of times is overwritten first. This feature cannot be programmed by the user; however, up to 20 entries can be “locked” (via the Locked soft key) so that they will never be deleted.
- Message waiting indication (via unsolicited NOTIFY)—Lights to indicate that a new voice message is in a subscriber’s mailbox. If the subscriber listens to the message but does not save or delete the message, the light remains on. If a subscriber listens to the new message or messages, and saves or deletes them, the light goes off. The message waiting indicator is controlled by the voice-mail server. The indication will be saved over a phone upgrade or reboot.
- Speed dial to voice mail using the messages button.
- Do not disturb—Allows the user to instruct the system to intercept incoming calls during specified periods of time when the user does not want to be disturbed.
- Multiple directory numbers—Allows the Cisco SIP IP phone to have up to six directory numbers or lines.
- Call waiting (enabled)—Plays an audible tone to indicate that an incoming call is waiting. The user can then put the existing call on hold and accept the other call. The user can alternate between the two calls.
- Call waiting (disabled)—Allows the user to instruct the system to block call waiting calls during a specified period of time.
- Direct number dialing—Allows users to initiate or receive a call using a standard E.164 number format in a local, national, or international format.
- Direct URL dialing—Provides the ability to place a call using an e-mail address instead of a phone number.
- Caller ID blocking—Allows the user to instruct the system to block a phone number or e-mail address from phones that have caller identification capabilities.
- Anonymous call blocking—Allows the user to instruct the system to block any calls for which the identification is blocked.
- Three-way conferencing—Supports one phone conferencing with two other phones by providing mixing on the initiating phone. To set up a three-way conference call, see the “Making Conference Calls” section in Chapter 3 of the Cisco IP Phone Models 7960 and 7940 User Guide.

Call Options

- Call forward (network)—Allows the Cisco SIP IP phone user to request forwarding service from the network (via a third-party tool that enables this feature to be configured). When a call is placed to the user’s phone, it is redirected to the appropriate forward destination by the SIP proxy server.
- Call hold—Allows the Cisco SIP IP phone user (user A) to place a call (from user B) on hold. When user A places user B on hold, the two-way RTP voice path between user A and user B is temporarily disconnected, but the call session is still connected. When user A takes user B off hold, the two-way RTP voice path is reestablished.
• Call transfer—Allows the Cisco SIP IP phone user (user A) to transfer a call from one user (user B) to another user (user C). User A places user B on hold and calls user C. If user C accepts the transfer, a session is established between user B and user C and the session between user A and user B is terminated.

• Three-way calling—Allows a “bridged” three-way call. When a three-way call is established, the Cisco SIP IP phone through which the call is established acts as a bridge, mixing the audio media for the other parties.

Routing and Proxy Features

• User-defined proxy routing
  The Route attribute of the template tag in the dial-plan template file can be used to indicate to which proxy (default, emergency, FQDN) the call should be initially routed. For example, to configure an emergency proxy, specify the value of the Route attribute as “emergency.”

• Backup SIP proxy
  When the primary proxy does not respond to the INVITE message sent by the Cisco SIP IP Phone after the configured number of retries, the Cisco SIP IP Phone sends the INVITE to the backup proxy. This is independent from the proxy defined in the Route attribute in the dial-plan template used.
  The Cisco SIP IP phone attempts to register with the backup proxy. All interactions with the backup proxy, such as authentication challenges, are treated the same as the interactions with the primary proxy.
  The backup proxy is used only with new INVITE messages that fail to communicate with the primary proxy. Once the backup proxy is used, it is active for the duration of the call.
  The location of the backup SIP proxy can be defined as an IP address in the default configuration file. Refer to the proxy_backup and proxy_backup_port parameters in the “Modifying the SIP Settings” section on page 3-6.

• Emergency SIP proxy
  An optional emergency SIP proxy can be configured with the Route attribute of the template tag in the dial-plan template file.
  When an emergency SIP proxy is configured and a call is initiated, the phone generates an INVITE message to the address specified in the proxy_emergency parameter. The emergency proxy is used for the call duration.
  The location of the emergency proxy can be defined as an IP address in the default configuration file. Refer to the proxy_emergency and proxy_emergency_port parameters in the “Modifying the SIP Settings” section on page 3-6.

• Support of DNS SRV
  The Domain Name Server (DNS SRV) is used to locate servers for a given service.
  SIP on Cisco SIP IP phones uses a DNS SRV query to determine the IP address of the SIP proxy or redirect server. The query string generated is in compliance with RFC 2782 and prepends the protocol label with an underscore (_), as in “_protocol._transport.” The addition of the underscore reduces the risk of the same name being used for unrelated purposes.
  In compliance with RFC 2782 and the draft-ietf-sip-srv-01 specification, the system can remember multiple IP addresses and use them properly. In the draft-ietf-sip-srv-01 specification, it is assumed that all proxies returned for the SRV record are equivalent such that the phone can register with any of the proxies and initiate a call using any other proxy.
What Is the Cisco SIP IP Phone?

- Configurable voice activity detection
  Voice activity detection (VAD) can be enabled or disabled with the enable_vad parameter. Use a value of 0 to disable and a value of 1 to enable. Refer to the enable_vad parameter in “Modifying the SIP Settings” section on page 3-6.

- Distinctive alerting
  If the INVITE message contains an Alert-Info header, distinctive ringing is invoked. The format of the header is “Alert-info: x”. The value of “x” can be any number. This header is received only by the phone and is not generated by the phone.

  Distinctive ringing is supported when the phone is idle or during a call. In the idle mode, the phone rings with a different cadence. The selected ringing type plays twice with a short pause in between. In call-waiting mode, two short beeps are generated instead of one long beep.

- Network Address Translation and outbound proxy
  Network Address Translation (NAT) can be enabled or disabled with the nat_enable parameter. You can configure the address of the NAT or firewall server using the nat_address parameter.

  You can configure the IP address and port number of the outbound proxy server. When outbound proxy is enabled, all SIP requests are sent to the outbound proxy server instead of to the proxyN_address. All responses continue to reconcile the normal Via processing rules. The media stream is not routed through the outbound proxy.

  NAT and outbound proxy modes can be independently enabled or disabled. The received= tag is added to the Via header of all responses if there is no received= tag in the uppermost Via header and the source IP address is different from the IP address in the uppermost Via header. Responses are sent back to the source under the following conditions:
  - If a received= tag is in the uppermost Via header, the response is sent back to the IP address contained in the received= tag.
  - If there is no received= tag and the IP address in the uppermost Via header is different from the source IP address, the response is sent back to the source IP address. Otherwise the response is sent back to the IP address in the uppermost Via header.

  For information on how to use the standard telephony features and URL dialing, refer to the documents listed in the “Related Documentation” section on page xi.

Character Support

The Cisco SIP IP phone supports the ISO 8859-1 Latin1 characters. The following languages are supported:

- French (fr), Spanish (es), Catalan (ca), Basque (eu), Portuguese (pt), Italian (it), Albanian (sq), Rhaeto-Romanic (rm), Dutch (nl), German (de), Danish (da), Swedish (sv), Norwegian (no), Finnish (fi), Faroese (fo), Icelandic (is), Irish (ga), Scottish (gd), English (en), Afrikaans (af), and Swahili (sw).

The following languages are not supported:

- Zulu (zu) and other Bantu languages using Latin Extended-B letters, Arabic in North Africa, and Guarani (gn) missing GEIUY with tilde (~).

Note

The XML cards, information text, and menus are all in English. These items are built into the phone image and cannot be changed.
ISO 8859-1 Latin1 characters can be used in the following areas:

- Caller ID information. When a SIP message is received with ISO 8859-1 Latin1 characters in the caller ID strings, those caller ID strings are displayed on the Cisco SIP IP phone LCD with the correct ISO 8859-1 Latin1 characters.

- Services menu applications written in CMXML. The customer can develop language-specific applications for a particular region. For example, an application that displayed the current weather in Sweden using Swedish language characters can be displayed on the Cisco SIP IP phone. If the customer develops the same application for a Spanish town, the application could be translated into Spanish.

- Line key labels. The line keys can be configured to support the Latin1 characters. The line key name can be specified in the configuration file, and it will be displayed correctly. The Latin1 characters cannot be used in the lineX_name, but can be used in the lineX_shortname and lineX_displayname. If the proxy supports Latin1 characters in the To/From headers, they can be used in the lineX_name parameter as well.

**Supported Protocols**

The Cisco SIP IP phone supports the following standard protocols:

- Domain Name Server (DNS)—Used in the Internet for translating names of network nodes into addresses. SIP uses DNS to resolve the host names of endpoints to IP addresses.

- Dynamic Host Configuration Protocol (DHCP)—Used to dynamically allocate and assign IP addresses. DHCP allows you to move network devices from one subnet to another without administrative attention. If using DHCP, you can connect Cisco SIP IP phones to the network and become operational without having to manually assign an IP address and additional network parameters.

  The Cisco SIP IP phone complies with the DHCP specifications documented in RFC 2131. By default, Cisco SIP IP phones are DHCP-enabled.

- Internet Control Message Protocol (ICMP)—A network layer Internet protocol that enables hosts to send error or control messages to other hosts. ICMP also provides other information relevant to IP packet processing.

  The Cisco SIP IP phone supports ICMP as it is documented in RFC 792.

- Internet Protocol (IP)—A network layer protocol that sends datagram packets between nodes on the Internet. IP also provides features for addressing, type-of-service (ToS) specification, fragmentation and reassembly, and security.

  The Cisco SIP IP phone supports IP as it is defined in RFC 791.

- Real-Time Transport Protocol (RTP)—Transports real-time data (such as voice data) over data networks. RTP also has the ability to obtain quality of service (QoS) information.

  The Cisco SIP IP phone uses RTP as a media channel.

- Session Description Protocol (SDP)—An ASCII-based protocol that describes multimedia sessions and their related scheduling information.

  The Cisco SIP IP phone uses SDP for session description.

- Simple Network Time Protocol (SNTP)—Synchronizes computer clocks on an IP network. The Cisco SIP IP phones use SNTP for their date and time support.

- Transmission Control Protocol (TCP)—Provides a reliable byte-stream transfer service between two endpoints on an internet. The Cisco SIP IP phone supports TCP for Telnet sessions only.
Prerequisites

For the Cisco SIP IP phone to successfully operate as a SIP endpoint in your network, your network must meet the following requirements:

- A working IP network is established.
  For more information about configuring IP, refer to the *Cisco IOS IP Configuration Guide*, Release 12.2.
- VoIP is configured on your Cisco routers.
  For more information about configuring VoIP, refer to the *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2, for the appropriate access platform. For more information about configuring SIP VoIP, refer to the “Configuring SIP for VoIP” chapter.
- VoIP gateways are configured for SIP.
- A TFTP server is active and contains the latest Cisco SIP IP phone firmware image in its root directory.
- A proxy server is active and configured to receive and forward SIP messages.

Cisco SIP IP Phone Connections

The Cisco SIP IP phone has connections for connecting to the data network, for providing power to the phone, and for connecting a headset to the phone. **Figure 1-3** illustrates the connections on the Cisco SIP IP phone.
Connecting to the Network

The Cisco SIP IP phone has two RJ-45 ports that each support 10/100-Mbps half- or full-duplex Ethernet connections to external devices—a network port (labeled 10/100 SW) and an access port (labeled 10/100 PC). You can use either Category 3 or Category 5 cabling for 10-Mbps connections, but use Category 5 for 100-Mbps connections. On both the network port and the access port, use full-duplex mode to avoid collisions.

Network Port (10/100 SW)

Use the network port to connect the phone to the network. You must use a straight-through cable on this port. The phone can also obtain inline power from the Catalyst switch over this connection. See the “Connecting to Power” section on page 1-13 for details.

Access Port (10/100 PC)

Use the access port to connect a network device, such as a computer, to the phone. You must use a straight-through cable on this port.

Connecting to Power

The Cisco SIP IP phone can be powered by the following sources:

- External power source—Optional Cisco AC adapter and power cord for connecting to a standard wall receptacle.
• WS-X6348-RJ45V 10/100 switching module—Provides inline power to the Cisco SIP IP phone when connected to a Catalyst 3500, 4000, or 6000 family 10/100BASE-TX switching module. This module sends power on pins 1 and 2, and 3 and 6.
• WS-PWR-PANEL—Power patch panel provides power to the Cisco SIP IP phone, which allows the Cisco SIP IP phone to be connected to existing Catalyst 4000, 5000, and 6000 family 10/100BASE-TX switching modules. This module sends power on pins 4, 5, 7, and 8.
• WS-X4148-RJ45V—48-port 10/100 Ethernet with inline power module for the Catalyst 4006.
• WS-X4095-PEM—VoIP DC Power Entry module for the Catalyst 4006.
• WS-X4608-2PSU and WS-X4608—External -48VDC power shelf common equipment for the Catalyst 4006 with two AC-to-DC power supply units (PSUs) and one empty bay for redundant option, and the 110V 15A AC-to-48VDC PSU redundant option for the power shelf.
• WS-C3524-PWR-XL-EN—Catalyst 3524-PWR XL switch.

Note
Only the network port (labeled 10/100 SW) supports inline power from the Catalyst switches.

Using a Headset

The Cisco SIP IP phone supports a four- or six-wire headset jack. Specifically, the Cisco SIP IP phone supports the following Plantronics headset models:

• Tristar Monaural
• Encore Monaural H91
• Encore Binaural H101

The volume and mute controls also adjust volume to the earpiece and mute the speech path of the headset. The headset activation key is located on the front of the Cisco SIP IP phone.

Note
When using a headset, an amplifier is not required. However, a coil cord is required to connect the headset to the headset port on the back of your Cisco IP Phone 7960/7940. For information on ordering compatible headsets and coil cords for the Cisco IP Phone 7960/7940, go to the following URL:

http://cisco.getheadsets.com or http://vxicorp.com/cisco

The Cisco SIP IP Phone with a Catalyst Switch

To function in the IP telephony network, the Cisco SIP IP phone must be connected to a networking device, such as a Catalyst switch, to obtain network connectivity.

The Cisco SIP IP phone has an internal Ethernet switch, which enables it to switch traffic coming from the phone, access port, and network port.

If a computer is connected to the access port, packets traveling to and from the computer and to and from the phone share the same physical link to the switch and the same port on the switch.

This configuration has the following implications for the VLAN configuration on the network:
The current VLANs might be configured on an IP subnet basis, and additional IP addresses might not be available to assign the phone to a port so that it belongs to the same subnet as other devices (PC) connected to the same port.

Data traffic present on the VLAN supporting phones might reduce the quality of VoIP traffic.

You can resolve these issues by isolating the voice traffic onto a separate VLAN on each of the ports connected to a phone. The switch port configured for connecting a phone would have separate VLANs configured for carrying the following traffic:

- Voice traffic to and from the Cisco SIP IP phone (auxiliary VLAN).
- Data traffic to and from the PC connected to the switch through the access port of the Cisco SIP IP phone (native VLAN).

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

For redundancy, you can use the Cisco AC adapter even if you are using inline power from the Catalyst switches. The Cisco SIP IP phone can share the power load being used from the inline power and external power source. If either the inline power or the external power goes down, the phone can switch entirely to the other power source.

To use this redundancy feature you must set the inline power mode to auto on the Cisco Catalyst switch. Next, connect the unpowered Cisco SIP IP phone to the network. After the phone powers up, connect the external power supply to the phone.

For more information, refer to the documentation included with the Catalyst switch or available online at the following URL:

http://www.cisco.com/univercd/home/index.htm
Getting Started with Your Cisco SIP IP Phone

This chapter explains the Cisco SIP IP phone initialization and the process that you should follow to install and connect the Cisco SIP IP phone. It provides the following sections:

- Overview of the Initialization Process, page 2-1
- Installing the Cisco SIP IP Phone, page 2-2
- Verifying Startup, page 2-14
- Using the Cisco SIP IP Phone Menu Interface, page 2-15
- Reading the Cisco SIP IP Phone Icons, page 2-15
- Customizing the Cisco SIP IP Phone Ring Types, page 2-17
- Creating Dial Plans, page 2-17

Overview of the Initialization Process

The initialization process of the Cisco SIP IP phone establishes network connectivity and makes the phone operational in your IP network. Once you connect your phone to the network and to an electrical supply, the phone begins its initialization process. During the initialization process, the following events take place:

1. The stored image is loaded.
   The Cisco SIP IP phone has nonvolatile Flash memory in which it stores the firmware images, user-defined preferences, and permanent factory information about the phone.
   During initialization, the phone runs a bootstrap loader that loads and executes the phone image stored in Flash memory.

2. The VLAN is configured.
   If the Cisco SIP IP phone is connected to a Catalyst switch, the switch notifies the phone of the voice VLAN defined on the switch. The phone needs to know its VLAN membership before it can proceed with the Dynamic Host Configuration Protocol (DHCP) request for its IP settings (if using DHCP).

3. An IP address is acquired.
   If the Cisco SIP IP phone is using DHCP to obtain the IP settings, the phone queries the DHCP server. If the phone is not using DHCP, the phone uses IP settings that are stored in Flash memory.
4. The TFTP server is contacted.

The TFTP server contains the latest Cisco SIP IP phone firmware image and the dual boot file (OS79XX.TXT) that enables the phone to automatically determine and initialize the VoIP environment in which it is being installed.

If the phone is using the TFTP server to obtain its SIP parameters, there should also be a configuration file or files on the TFTP server that the phone will request and download. In the configuration file or files, SIP parameters that are required by the phone to operate in a SIP VoIP environment are defined. If the phone is not obtaining its SIP parameters via the TFTP server, the phone uses SIP settings that are stored in Flash memory.

5. The firmware version is verified.

If the phone is obtaining its SIP parameters via a TFTP server, the configuration files are requested. If the phone determines that the image defined in a configuration file differs from the image it has stored in Flash memory, it performs a firmware upgrade. When performing a firmware upgrade, the phone downloads the firmware image from the TFTP server, programs the image into Flash memory, and reboots.

**Installing the Cisco SIP IP Phone**

This section contains information on how to install Cisco SIP IP phones in your IP network. Before getting started, read over the information in this section carefully.

**Installation Task Summary**

To successfully install the Cisco SIP IP phone, complete the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download the required files from Cisco.com to the TFTP server as described in the “Downloading Files to Your TFTP Server” section on page 2-3.</td>
</tr>
<tr>
<td>2</td>
<td>If you are configuring SIP parameters via a TFTP server, create and store the configuration files as described in the “Configuring SIP Parameters Using a TFTP Server” section on page 2-4. If you are not configuring the SIP parameters via a TFTP server, manually configure the required parameters as described in the “Configuring the SIP Parameters Manually” section on page 2-7.</td>
</tr>
<tr>
<td>3</td>
<td>If you are using DHCP to configure the phone network settings, configure the required network parameters on your DHCP server as described in the “Configuring Network Parameters Using a DHCP Server” section on page 2-10. If you are not using DHCP to configure network parameters, manually configure the required network parameters as described in the “Configuring the Network Parameters Manually” section on page 2-10.</td>
</tr>
<tr>
<td>4</td>
<td>Connect the phone to the network and to a power supply as described in the “Connecting the Phone” section on page 2-11.</td>
</tr>
</tbody>
</table>
## Installing the Cisco SIP IP Phone

### Downloading Files to Your TFTP Server

Before installing the Cisco SIP IP phones, copy the following files from Cisco.com to the root directory of your TFTP server.

<table>
<thead>
<tr>
<th>File</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS79XX.TXT</td>
<td>Required</td>
<td>Enables the phone to automatically determine and initialize the VoIP environment in which it is being installed. After downloading this file, you must use an ASCII editor to open it and specify the filename (without the file extension) of the image version that you plan to run on your phones.</td>
</tr>
<tr>
<td>SIPDefault.cnf</td>
<td>Optional</td>
<td>File in which to configure SIP parameters intended for all phones. For more information on using the SIPDefault.cnf file, see the “Creating the Default SIP Configuration File” section on page 2-5.</td>
</tr>
<tr>
<td>SIPConfigGeneric.cnf</td>
<td>Required</td>
<td>File that can be used as a template to configure SIP parameters specific to a phone. When customized for a phone, this file must be renamed to the MAC address of the phone. For more information on custom ring types, see the “Customizing the Cisco SIP IP Phone Ring Types” section on page 2-17.</td>
</tr>
<tr>
<td>RINGLIST.DAT</td>
<td>Optional</td>
<td>Lists audio files that are the custom ring type options for the phones. The audio files listed in the RINGLIST.DAT file must also be in the root directory of the TFTP server. For more information on custom ring types, see the “Customizing the Cisco SIP IP Phone Ring Types” section on page 2-17.</td>
</tr>
</tbody>
</table>
| P0S3xxyy.bin            | Required             | The Cisco SIP IP phone firmware image. The xx variable represents the version number, and the yy variable represents the subversion number.  

**Note** Applies to Cisco SIP IP Phone Release 2.3 and earlier. |
| P0S3-xx-yy-zz.bin       | Required             | The Cisco SIP IP phone firmware image. The xx variable represents the major version number, the yy variable represents the minor version number, and the zz variable represents the subversion number.  

**Note** Applies to Cisco SIP IP Phone Release 3.0 and later. |
| P0S3-xx-yy-zz.sbn       | Required             | Release 5.0 and Release 5.1 secured phone firmware image. |
| dialplan.xml            | Optional             | North American sample dial plan. The dialplan.xml file can be pushed down to the phones using a NOTIFY with a check-sync Event header. |
| syncinfo.xml            | Optional             | Controls the image version and associated synchronization value to be used for remote reboots. |
| SIPPhone Release Notes.4.2.pdf | Optional             | Contains the 4.2 release notes. |
| SIPPhone Release Notes.4.4.pdf | Optional             | Contains the 4.4 release notes. |
| SIPPhone Release Notes.5.0.pdf | Optional             | Contains the 5.0 release notes. |
| SIPPhone Release Notes.5.1.pdf | Optional             | Contains the 5.1 release notes. |
Chapter 2      Getting Started with Your Cisco SIP IP Phone

Installing the Cisco SIP IP Phone

Configuring SIP Parameters

Note

This section describes how to configure the basic SIP parameters that are required for the phone to operate in a SIP VoIP environment. For a complete list of the SIP parameters that you can configure, see the “Modifying the SIP Settings” section on page 3-6.

The SIP parameters are those parameters that a Cisco SIP IP phone needs in order to operate in a SIP VoIP environment. You can configure SIP parameters via a TFTP server, or you can manually configure the parameters on a phone-by-phone basis after connecting the phones.

When the phone initializes, it loads the parameters stored in Flash memory. After loading the parameters stored in Flash memory, the phone requests the default configuration file from the TFTP server. If the default configuration file has been configured and stored in the root directory of the TFTP server, the phone reads the parameters defined in the file and stores those parameters that differ in Flash memory. The phone then requests its phone-specific configuration file.

If the phone-specific configuration file has been configured and placed on the TFTP server (in the root directory or a subdirectory), the phone reads the parameters defined in the file and stores those parameters that differ in Flash memory.

Therefore, when configuring SIP parameters, remember the following:

- Parameters defined in the default configuration file override the values stored in Flash memory.
- Parameters defined in the phone-specific configuration file override the values specified in the default configuration file.
- Parameters entered locally are used by the phone until the next reboot (if a phone-specific configuration file exists).
- If you choose not to configure the phone via a TFTP server, you must manage the phone locally.

Configuring SIP Parameters Using a TFTP Server

If you are configuring SIP parameters using a TFTP server, you must use configuration files.

There are two configuration files that you can use to define the SIP parameters: the default configuration file (optional) and the phone-specific configuration file (required). If you choose to use a default configuration file, you must store the file in the root directory of your TFTP server. Phone-specific configuration files can be stored in the root directory or in a subdirectory in which all phone-specific configuration files are stored.

Except for parameters used to define the lines and users on a phone, all other SIP parameters can be defined in either the default configuration file or the phone-specific configuration file. However, for network control and maintenance purposes, we recommend that you define the parameters that you want to apply to all phones in the default configuration file (SIPDefault.cnf). Phone-specific parameters should only be defined via a phone-specific configuration file or be configured manually. Phone-specific parameters should not be defined in the default configuration file.
Configuration File Guidelines

When modifying the default configuration file and creating the phone-specific configuration files, adhere to the following guidelines and requirements:

- SIP parameters specified in the default configuration file (SIPDefault.cnf) override those parameters stored in Flash memory. Parameters specified in a phone-specific configuration file override those stored in Flash memory and those specified in the default configuration file.

- The name of each phone-specific configuration file is unique and is based on the MAC address of the phone.

The format of the filename must be SIPXXXXYYYYZZZZ.cnf, where XXXXYYYYZZZZ is the MAC address of the phone. The MAC address must be in uppercase, and the cnf extension must be in lowercase (for example, SIP00503EFFD842.cnf).

- The default configuration file must be stored in the root directory of the TFTP server. The phone-specific configuration file can be stored in the root directory or in a subdirectory in which all phone-specific configuration files are located.

- Each line in the configuration files must use the following format:

  variable-name : value ; optional comments

- Use colons to separate variable names and values.

- Only one value can be associated with a variable.

- The variable and value can contain white space before or after them and can contain any characters. However, if white spaces are needed within the value, the value must be enclosed in single or double quotes. If the value is enclosed in quotes, the end quote must be the same as the start quote.

- After the value, you can include optional comments. Use the semicolon (;) and pound (#) delimiters to distinguish the comments.

- Blank lines are allowed.

- Comment lines are allowed.

- Variable names are not case sensitive.

- Only one variable can be set per line.

- Distinguish the end of a line using \(<lf>\) or \(<\cr><lf>\).

- The variable and value must be on the same line and cannot break the line.

- Except for parameters used to defined the lines and users on a phone, all other SIP parameters can be defined in either the default configuration file or the phone-specific configuration file. However, for network control and maintenance purposes, Cisco recommends that you define the parameters that you want to apply to all phones in the default configuration file (SIPDefault.cnf).

Creating the Default SIP Configuration File

In the default configuration file (SIPDefault.cnf), Cisco recommends that you define the SIP parameters that will be common to all of your phones such as the image_version parameter and call environment parameters (for example, you will want to consider if the phones are required to register with a proxy server, and which codec the phones will use when initiating a call).
By maintaining these parameters in the default configuration file, you can perform global changes, such as upgrading the image version, without having to modify the phone-specific configuration file for each phone.

**Before You Begin**

- Ensure that you have downloaded the SIPDefault.cnf file from Cisco.com to the root directory of your TFTP server.
- Review the guidelines documented in the “Configuration File Guidelines” section on page 2-5.
- For a complete list of the SIP parameters that you can configure, see the “Modifying the SIP Settings” section on page 3-6.

**Procedure**

**Step 1** Using an ASCII editor, open the SIPDefault.cnf file and define values for the following SIP global parameters:

- **image_version**—(Required) Firmware version that the Cisco SIP IP phone should run.
  
  Enter the name of the image version (as it is released by Cisco). Do not enter the extension. You cannot change the image version by changing the filename, because the version is also built into the file header. Trying to change the image version by changing the filename causes the firmware to fail when it compares the version in the header against the filename.

- **proxy1_address**—(Required) IP address of the primary SIP proxy server that will be used by the phones.

- **tftp_cfg_dir**—(Required if phone-specific configuration files are located in a subdirectory) Path to the TFTP subdirectory in which phone-specific configuration files are stored.

**Step 2** Save the file with the same filename, SIPDefault.cnf, to the root directory of your TFTP server.

The following is an example of a default SIP configuration file:

```
#Image Version
image_version:PA03-xx-y-zz;

#Proxy server address
proxy1_address: 10.10.1.1;

#Subdirectory config file location
tftp_cfg_dir: /tftpboot/configs/sipphone
```

**Creating the Phone-Specific SIP Configuration File**

In the phone-specific SIP configuration file, define the parameters that are specific to a phone, such as the lines configured on a phone and the users defined for those lines.

**Before You Begin**

- Review the guidelines documented in the “Configuration File Guidelines” section on page 2-5.

- Line parameters (those identified as line\(x\)) define a line on the phone. If you configure a line to use an e-mail address, that line can be called only by using an e-mail address. Similarly, if you configure a line to use a number, that line can be called only by using the number. Each line can have a different proxy configured.
For a complete list of the SIP parameters that you can configure, see the “Modifying the SIP Settings” section on page 3-6.

**Procedure**

### Step 1
Using an ASCII editor, create a phone-specific configuration file for each phone that you plan to install. In the phone-specific configuration file, define values for the following SIP parameters (where \( x \) is a number 1 through 6):

- \( \text{line}_x\text{\_name} \) — (Required) Number or e-mail address used when registering. When entering a number, enter the number without any dashes. For example, enter 555-1212 as 5551212. When entering an e-mail address, enter the e-mail ID without the host name.

- \( \text{line}_x\text{\_authname} \) — (Required when registration is enabled and the proxy server requires authentication) Name used by the phone for authentication if a registration is challenged by the proxy server during initialization. If a value is not configured for the \( \text{line}_x\text{\_authname} \) parameter when registration is enabled, the default name is used. The default name is UNPROVISIONED.

- \( \text{line}_x\text{\_password} \) — (Required when registration is enabled and the proxy server requires authentication) Password used by the phone for authentication if a registration is challenged by the proxy server during initialization. If a value is not configured for the \( \text{line}_x\text{\_password} \) parameter when registration is enabled, the default logical password is used. The default logical password is UNPROVISIONED.

### Step 2
Save the file to your TFTP server (in the root directory or in a subdirectory that contains all the phone-specific configuration files). Name the file SIPXXXXYYYYZZZZ.cnf where XXXXYYYYZZZZ is the MAC address of the phone. The MAC address must be in uppercase and the extension, cnf, must be in lowercase (for example, SIP00503EFFD842.cnf).

The following is an example of a phone-specific SIP configuration file:

```plaintext
; Line 1 phone number
line1_name : 5551212

; Line 1 name for authentication with proxy server
line1_authname : 5551212

; Line 1 authentication name password
line1_password : password
```

### Configuring the SIP Parameters Manually

If you did not configure the SIP parameters via a TFTP server, you must manually configure them after you have connected the phone as described in the “Connecting the Phone” section on page 2-11.

**Before You Begin**

- Connect your phone as described in the “Connecting the Phone” section on page 2-11.
- Unlock configuration mode as described in the “Locking Configuration Mode” section on page 3-3. By default, the SIP parameters are locked to ensure that end users cannot modify settings that might affect their call capabilities.
- Review the guidelines on using the Cisco SIP IP phone menus documented in the “Using the Cisco SIP IP Phone Menu Interface” section on page 2-15.
When configuring the Preferred Codec and Out of Band DTMF parameters, press the **Change** soft key until the option that you desire is displayed and then press the **Save** soft key.

After making your changes, relock configuration mode as described in the “Locking Configuration Mode” section on page 3-3.

For a complete list of the SIP parameters that you can configure, see the “Modifying the SIP Settings” section on page 3-6.

**Procedure**

**Step 1** Press the **settings** key. The Settings menu is displayed.

**Step 2** Highlight **SIP Configuration**. The SIP Configuration menu is displayed.

**Step 3** Highlight **Line 1 Settings**.

**Step 4** Press the **Select** soft key. The Line 1 Configuration menu is displayed.

**Step 5** Highlight and press the **Select** soft key to configure the parameters shown in Table 2-1:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Required</td>
<td>Number or e-mail address used when registering. When entering a number, enter the number without any dashes. For example, enter 555-1212 as 5551212. When entering an e-mail address, enter the e-mail ID without the host name.</td>
</tr>
<tr>
<td>Shortname</td>
<td>Optional</td>
<td>Name or number associated with the linex_name as you want it to display on the phone’s LCD if the linex_name value exceeds the display area. For example, if the linex_name value is the phone number 111-222-333-4444, you can specify 34444 for this parameter to have 34444 display on the LCD instead. Alternately, if the value for the linex_name parameter is the e-mail address “<a href="mailto:username@company.com">username@company.com</a>,” you can specify the “username” to have just the username appear on the LCD instead. This parameter is used for display purposes only. If a value is not specified for this parameter, the value in the Name variable is displayed.</td>
</tr>
<tr>
<td>Authentication Name</td>
<td>Required when registration is enabled</td>
<td>Name used by the phone for authentication if a registration is challenged by the proxy server during initialization. If a value is not configured for the Authentication Name parameter when registration is enabled, the default name is used. The default name is UNPROVISIONED.</td>
</tr>
<tr>
<td>Authentication Password</td>
<td>Required when registration is enabled</td>
<td>Password used by the phone for authentication if a registration is challenged by the proxy server during initialization. If a value is not configured for the Authentication Password parameter when registration is enabled, the default logical password is used. The default password is UNPROVISIONED.</td>
</tr>
</tbody>
</table>
Chapter 2  Getting Started with Your Cisco SIP IP Phone

Installing the Cisco SIP IP Phone

Step 6  Press the Back soft key to exit the Line 1 Configuration menu.

Step 7  To configure additional lines on the phone, highlight the next Line x Settings, press the Select soft key, and repeat Step 5 and Step 6.

Step 8  When done, press the Save soft key to save your changes and exit the SIP Configuration menu.

| Display Name | Optional | Identification as it should appear for caller-identification purposes. For example, instead of jdoe@company.com displaying on phones that have caller ID, you can specify John Doe in this parameter to have John Doe display on the called party end instead. If a value is not specified for this parameter, the Name value is used. |
| Proxy Address | Required for the first line configured on the phone | IP address of the primary SIP proxy server that will be used by the phone. Enter this address in IP dotted-decimal notation or as an FQDN. |
| Proxy Port | Required for the first line configured on the phone | Port of the primary SIP proxy server that is used by the phone. |

Configuring Network Parameters

This section describes how to configure the basic network parameters that are required for the phone to operate on the network. For a complete list of the network parameters that you can configure, see the “Modifying the SIP Settings” section on page 3-6.

The network parameters include those parameters that must be configured on a phone in order for the phone to operate in an IP network. You can configure the required network parameters using DHCP or configure the parameters manually after you have connected the phone to a power supply.

The following parameters must be defined in order for your phone to establish network connectivity:

- Phone IP address
- Subnet mask
- Default gateway for the subnet (use “0.0.0.0” if not required)
- Domain name
- DNS server IP address (use “0.0.0.0” if not required)
- TFTP server IP address
- Backup proxy server

Table 2-1  Manual SIP Configuration Parameters (continued)
When configuring the network parameters of an IP phone, adhere to the following guidelines:

- Use 0.0.0.0 for unused IP addresses.
- You can use 0.0.0.0 for the subnet mask only if the default gateway is also 0.0.0.0.
- The TFTP server must have a nonzero IP address.
- The default gateway must be on the same subnet as the phone.
- The default gateway can be 0.0.0.0 only if the TFTP or DNS server is on the same subnet as the phone.

Note
By default, DHCP is enabled on your phone. Before you can manually configure the network parameters, you must disable DHCP after connecting your phone to a power supply.

Configuring Network Parameters Using a DHCP Server

If you are using DHCP to configure the network parameters, configure the following DHCP options on your DHCP server before you connect your Cisco SIP IP phone:

- dhcp option #50 (IP address)
- dhcp option #1 (IP subnet mask)
- dhcp option #3 (Default IP gateway)
- dhcp option #15 (Domain name)
- dhcp option #6 (DNS server IP address)
- dhcp option #66 (TFTP server IP address)

Configuring the Network Parameters Manually

If you are not using DHCP to configure your network parameters, you must manually configure them.

Before You Begin

- Connect your phone as described in the “Connecting the Phone” section on page 2-11.
- Unlock configuration mode as described in the “Unlocking Configuration Mode” section on page 3-2. By default, the network parameters are locked to ensure that end users cannot modify settings that might affect their network connectivity.
- Review the guidelines on using the Cisco SIP IP phone menus documented in the “Using the Cisco SIP IP Phone Menu Interface” section on page 2-15.
- When configuring a domain name:
  - Press the Number soft key to enter a numerical ID or press the Alpha soft key to enter a name.
  - If entering letters, use the numbers on the dial pad associated with a particular letter. For example, the 2 key has the letters A, B, and C. For a lowercase a, press the 2 key once. To scroll through the available letters and numbers, press the key repeatedly.
  - Press the << soft key to delete any mistakes.
Press the settings key. The Settings menu is displayed.

Highlight Network Configuration.

Press the Select soft key. The Network Configuration menu is displayed.

Highlight DHCP Enabled.

Press the No soft key. DHCP is now disabled.

Highlight and configure each of the following parameters:

- IP Address—IP address of the phone.
- Subnet Mask—IP subnet mask used by the phone.
- TFTP Server—IP address of the TFTP server from which the phone downloads its configuration files and firmware images.
- Default routers 1 through 5—IP address of the default gateway used by the phone. Default routers 2 through 5 are the IP addresses of the gateways that the phone attempts to use as an alternate gateway if the primary gateway is not available.
- Domain Name—Name of the DNS domain in which the phone resides.
- DNS servers 1 through 5—IP address of the DNS server used by the phone to resolve names to IP addresses. The phone attempts to use DNS servers 2 through 5 if DNS server 1 is unavailable.

When done, press the Save soft key. The phone programs the new information into Flash memory and resets.

Connecting the Phone

You must connect the phone to the network and to a power source before using it.

Before You Begin

Refer to Figure 2-1 for a graphical overview of the procedures in this section.
**Figure 2-1  Cisco SIP IP Phone Cable Connections**

- **Power outlet**
- **AC adapter (−48VDC)**
- **RS-232 port**
- **Network port (10/100 SW)**
- **Access port (10/100 PC)**
- **Headset port**
- **Handset port**

**Procedure**

**Step 1** Connect a Category 3 or 5 straight-through Ethernet cable from the switch or hub to the **network** port on the phone.  
See the “Connecting to the Network” section on page 1-13 for more information on the network port.

**Step 2** Connect the handset and headset to their respective ports.  
See the “Using a Headset” section on page 1-14 for more information on the headset port.

**Step 3** Connect a Category 3 or 5 straight-through Ethernet cable from another network device, such as a desktop computer, to the **access** port on the phone (optional).  
See the “Connecting to the Network” section on page 1-13 for more information on the access port.

**Step 4** Connect the power plug to the Cisco AC adapter port (optional).  
See the “Connecting to Power” section on page 1-13 for more information.

---

**Adjusting the Placement of the Cisco SIP Phone**

The Cisco SIP IP phone includes an adjustable footstand. When placing the phone on a desktop surface, you can adjust the tilt height to several different angles in 7.5 degree increments from flat to 60 degrees. Alternatively, you can mount the phone to the wall using the footstand or using the optional locking accessory.
Adjusting the Phone Placement on the Desktop

Adjust the footstand to the height that provides optimum view of the display and use of the buttons and keys as shown in Figure 2-2.

To adjust the phone placement on the desktop:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Push in the footstand adjustment knob.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Adjust the footstand to its desired height and release the knob.</td>
</tr>
</tbody>
</table>

Mounting the Phone to the Wall

You can mount the Cisco SIP IP phone on the wall using the footstand as a mounting bracket or using the optional locking bracket. Use the following procedure to mount the phone on the wall using the standard footstand. To use the optional locking bracket, refer to the Installing the Wall Mount Kit for the Cisco IP Phone document.

Before You Begin

Mounting the Cisco SIP IP phone on the wall requires some tools and equipment that are not provided as standard equipment.

Following are the tools and parts required for a typical Cisco SIP IP phone installation:

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

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Push in the footstand adjustment knob.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Adjust the footstand so that it is flat against the back of the phone, as shown in Figure 2-2.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Modify the handset rest so that the handset remains on the ear-piece rest when the phone is vertically placed.</td>
</tr>
<tr>
<td></td>
<td>a. Remove the handset from the ear-piece rest.</td>
</tr>
<tr>
<td></td>
<td>b. Locate the tab (handset wall hook) at the base of the ear-piece rest.</td>
</tr>
<tr>
<td></td>
<td>c. Slide this tab out, rotate it 180 degrees, and reinsert it.</td>
</tr>
<tr>
<td></td>
<td>d. Place the handset on the ear-piece rest.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Insert two screws into a wall stud, matching them to the two screw holes on the back of the footstand.</td>
</tr>
<tr>
<td></td>
<td>The keyholes fit standard phone jack mounts.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Hang the phone on the wall.</td>
</tr>
</tbody>
</table>
Verifying Startup

After the phone has power connected to it, the phone begins its startup process by cycling through these steps:

1. The following buttons flash on and off in sequence:
   - Headset
   - Mute
   - Speaker

2. The Cisco Systems, Inc. copyright appears on the LCD.

3. The following messages appear as the phone starts up:
   - Configuring VLAN—The phone is configuring the Ethernet connection.
   - Configuring IP—The phone is contacting the DHCP server to obtain network parameters and the IP address of the TFTP server.
   - Requesting Configuration—The phone is contacting the TFTP server to request its configuration files and compare firmware images.
   - Upgrading Software—The Upgrade Software message displays only if the phone has determined that an image upgrade is required. After upgrading the image, the phone automatically reboots to run the new image.

4. The main LCD displays the following:
   - Primary directory number
   - Soft keys

If the phone successfully passes through these stages, it has started up properly.
Using the Cisco SIP IP Phone Menu Interface

As you configure your phone’s settings via the menu interface, follow these guidelines:

- Select a parameter by pressing the down arrow to scroll to and highlight the parameter or by pressing the number that represents the parameter (located to the left of the parameter on the LCD).
- During configuration, use * for dots (periods) or press the “.” soft key when available on the LCD.
- Press Cancel during configuration to cancel all changes and exit a menu.
- When configuring a SIP IP address or ID parameter:
  - Press the Number soft key to enter a numerical value or press the Alpha soft key to enter a name.
  - Use the buttons on the dial pad to enter a new value.
  - If entering letters, use the numbers on the dial pad associated with a particular letter. For example, the 2 key has the letters A, B, and C. For a lowercase a, press the 2 key once. To scroll through the available letters and numbers, press the key repeatedly.
  - Press the << soft key to delete any mistakes.
- When configuring a network IP address or ID parameter:
  - Use the buttons on the dial pad to enter a new value.
  - Press the << soft key to delete any mistakes.
- After editing a parameter, press the Validate soft key to save the value that you have entered and exit the Edit panel.

Reading the Cisco SIP IP Phone Icons

When using the Cisco SIP IP phone, a variety of icons can display on the phone’s LCD. Table 2-2 lists and describes each icon that you might see while using the Cisco SIP IP phone.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![SIP Icon]</td>
<td>The Cisco IP phone that you are using is running SIP.</td>
</tr>
<tr>
<td>![Failure Icon]</td>
<td>The line is configured for E.164 number dialing, and you can enter only numbers when placing the call. The character x displayed to the right of the icon indicates that registration has failed.</td>
</tr>
</tbody>
</table>
The line is configured for E.164 number dialing and is ready for you to place the call. When a line is configured for E.164 number dialing, you can enter only numbers when placing the call.

You can change to URL dialing at any time while dialing on a line by pressing the URL soft key.

The character x displayed to the right of the icon indicates that registration has failed.

The line is configured for URL dialing, and you can enter both numbers and letters when placing the call.

The character x displayed to the right of the icon indicates that registration has failed.

The Cisco SIP IP phone configuration mode is locked. When the phone is locked, the phone’s network or SIP settings cannot be modified.

The Cisco SIP IP phone configuration mode is unlocked. When the phone is unlocked, the phone’s network or SIP settings can be modified.

A normal two-way call is on hold (call display is blinking).

A normal two-way call is connected and communicating.

A three-way call is on hold (call display is blinking).

A three-way call is connected and communicating.
Customizing the Cisco SIP IP Phone Ring Types

The Cisco SIP IP phone ships with two ring types: Chirp1 and Chirp2. By default, your ring type options will be those two choices. However, using the RINGLIST.DAT file, you can customize the ring types that are available to Cisco SIP IP phone users.

Step 1
Create a pulse code modulation (PCM) file of the desired ring types and store the PCM files in the root directory of your TFTP server. PCM files must contain no header information and must comply with the following format guidelines:

- 8000-Hz sampling rate
- 8 bits per sample
- u-law compression

Step 2
Using an ASCII editor, open the RINGLIST.DAT file, and for each of the ring types that you are adding, specify the name as you want it to appear on the Ring Type menu, press Tab, and then specify the filename of the ring type. For example, the format of a pointer in your RINGLIST.DAT file should appear similar to the following:

```
Ring Type 1ringer1.pcm
```

Step 3
After defining pointers for each of the ring types that you are adding, save your modifications and close the RINGLIST.DAT file.

Creating Dial Plans

Dial plans enable the Cisco SIP IP phone to support automatic dialing and automatic generation of a secondary dial tone. If a single dial plan is to be used for a system of phones, the dial plan is best specified in the default configuration file. However, you can create multiple dial plans and specify which phones are to use which dial plan by defining the dial_template parameter in the phone-specific configuration file. If one phone in a system of phones needs to use a different dial plan than the rest, you need to define the differing dial plan by specifying the dial_template parameter in that phone’s phone-specific configuration file.

Note
We recommend that you define the dial_template parameter in the default configuration file for maintenance and control purposes. Specify the dial_template parameter in a phone-specific configuration file only if that phone needs to use a different dial plan than is being used by the other phones in the same system.

When creating a dial plan, remember the following:

- Dial plans must be in an .xml format and must be stored on your TFTP server.
- You must specify which dial plan a phone is to use by specifying the path to the dial plan in the dial_template parameter that you define in either the phone-specific configuration file or the default configuration. We recommend that the dial_template parameter be defined in the default configuration file unless a specific phone must use a dial plan that differs from the one being used by other phones in the same system.
• `<DIALTEMPLATE>` indicates the start of a template and `</DIALTEMPLATE>` indicates the end of a template.

• Rules are matched from start to finish with the longest matching rule taken as the one to use. Matches against a period are not counted for the length to be the longest.

To create your dial plan, perform the following steps:

---

**Step 1**
Using an ASCII editor, open a new file.

**Step 2**
Type `<DIALTEMPLATE>` to indicate the start of the dial-plan template.

**Step 3**
For each of the numbering schemes that you wish to define, add the following string to the template, each starting on a separate line:

```
TEMPLATE MATCH="pattern" Timeout="sec" User="type" Rewrite="xxx" Route="route"
```

Where:

• **MATCH**= “pattern” is the dial pattern to match. When entering the value of `pattern`, use a period (.) to match any character or use an asterisk (*) to match one or more characters. To have the phone generate a secondary dial tone when the part of the template matches, use a comma (,).

• **Timeout**= “sec” is the number of seconds before a timeout occurs, and the number is dialed as entered by the user. To have the number dial immediately, specify 0.

• **User**= “type” is the either IP or Phone. Enter `User=phone` or `User=IP` to have the tag automatically added to the dialed number. This entry is not case sensitive.

• **Rewrite**= “xxx” is the alternate string to be dialed instead of what the user enters.

The rewrite rules are matched from start to finish with the longest matching rule taken as the one to use. Matches against a period are not counted for the length to be the longest. A complete rule is not matched unless it has more nonwildcard matches than an incomplete rule. You can put comments into the file with <!-- to start the comment and --> to end it.

The rules allow for substitution of up to five replacement strings as well as picking off replaced digits one at a time. For example, with a match string of “ab..cd..ef*” and an input string of “ab12cd34ef5678.”

The following replacement strings work, as follows.

<table>
<thead>
<tr>
<th>Rewrite</th>
<th>Output</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>%s</td>
<td>ab12cd34ef5678</td>
<td></td>
</tr>
<tr>
<td>%0</td>
<td>ab12cd34ef5678</td>
<td></td>
</tr>
<tr>
<td>%1</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>%2</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>%3</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>%4</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>%5</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>XYZ....</td>
<td>XYZ1234</td>
<td></td>
</tr>
<tr>
<td>X.YZ...</td>
<td>X1Y2Z345</td>
<td></td>
</tr>
<tr>
<td>919%1%2%3</td>
<td>919123456</td>
<td></td>
</tr>
<tr>
<td>AB...X%1X..</td>
<td>AB123X12X45</td>
<td>Note how “12” appears twice.</td>
</tr>
<tr>
<td>X%1X%1X%1</td>
<td>X12X12X12</td>
<td>You can reuse the string.</td>
</tr>
</tbody>
</table>
Chapter 2      Getting Started with Your Cisco SIP IP Phone

Creating Dial Plans

<table>
<thead>
<tr>
<th>REWRITE</th>
<th>Output</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>X%ss%%</td>
<td>Xab12cd34ef5678% %%</td>
<td>This produces a %.</td>
</tr>
<tr>
<td>919</td>
<td>919</td>
<td>No need to use the input.</td>
</tr>
<tr>
<td>............</td>
<td>12345678</td>
<td>Note that nothing goes in for the extra dots.</td>
</tr>
</tbody>
</table>

- Route= \"route\" is default, emergency, or FQDN. FQDN is treated the same as default proxy. Route indicates which proxy the call is to be routed to. This entry is not case sensitive.

**Step 4** If desired, specify <!--comment--> at the end of each string, where comment defines the type of plan (for example, Long Distance or Corporate Dial Plan).

**Step 5** When completed, enter </DIALTEMPLATE> to indicate the end of the dial-plan template.

**Step 6** Give the file a unique name specific to the dial plan it defines, and save the file with an .xml extension to your TFTP server.

**Step 7** If the dial plan applies to a specific phone, add the path to the dial plan (without specifying the file type of .xml) using the dial_template parameter in the phone-specific configuration file. If the dial plan applies to a system of phones, add the path to the dial plan using the dial_template parameter in the default configuration file. For more information on defining the dial_template parameter, see the “Modifying the SIP Settings” section on page 3-6.

The following is an example of a North American dial plan:

```xml
<DIALTEMPLATE>
  <TEMPLATE MATCH="0*" Timeout="1" User=phone"/> <!-- Local operator -->
  <TEMPLATE MATCH="9,011*" Timeout="6" User=phone"/> <!-- International calls -->
  <TEMPLATE MATCH="9,0" Timeout="2" User=Phone"/> <!-- PSTN Operator -->
  <TEMPLATE MATCH="9,11" Timeout="0" User=Phone" Rewrite="9911"/> <!-- Emergency -->
  <TEMPLATE MATCH="9!" Timeout="1" User="PHONE" Rewrite="9911"/> <!-- 911 when entered in Alpha mode -->
  <TEMPLATE MATCH="9,11" Timeout="0" User=Phone"/> <!-- Service numbers -->
  <TEMPLATE MATCH="9,101..................." Timeout="0" User="Phone"/> <!-- Long Distance Service -->
  <TEMPLATE MATCH="9,10.................." Timeout="0" User=Phone"/> <!-- Long Distance Service -->
  <TEMPLATE MATCH="9,10*" Timeout="6" User=Phone"/> <!-- Long Distance Service -->
  <TEMPLATE MATCH="9,1............" Timeout="0" User=Phone"/> <!-- Long Distance -->
  <TEMPLATE MATCH="9,1............" Timeout="0" User=Phone"/> <!-- Local numbers -->
  <TEMPLATE MATCH="*" Timeout="15"/> <!-- Anything else -->
</DIALTEMPLATE>
```
Updates to the Dial-Plan Template in Release 4.4 and Later

The dial-plan template has been updated so that you can specify the # and * as a dialed digits and the comma (,) can be specified a secondary dial tone.

Specifying the #
Pressing the # is still processed as a “dial now” event and remains the default behavior unless you specify the # in the dial-plan template. If you specify the # in the dial-plan template, the phone does not dial immediately when the # is pressed but does continue to match the dial-plan template that specifies the #. The # is not matched by the wildcard character * or the period (.)

Specifying the *
The * was used as a dial-plan wildcard character, so there was no way to specify it as a dialed digit. Beginning with Release 4.4, an escape sequence was added to indicate that the * should be processed as a dialed digit rather than as a wildcard. The escape sequence is a backward slash (\) and * so that the syntax is \*. The phone automatically strips the \ so that it does not appear in the outgoing dial string. When * is received as a dialed digit, it is matched by the wildcard characters * and period (.)

Specifying the Comma
Prior to this release, specifying a comma (,) in the dial-plan template caused the phone to play the default secondary dial tone (Bellcore-Outside). With this release and later, support is added so that you can specify which tones are played when the comma (,) is specified.

A new XML token named TONE was added to the dial-plan template. If the comma (,) is specified and there is no TONE token present, the phone plays the default secondary dial tone. If the comma (,) is specified and there is a TONE token present, the phone plays the indicated tone instead of the secondary dial tone. If a tone is specified but there is no comma (,) in the match string, the tone is ignored.

Up to 3 different secondary dial tones can be specified in a single dial-plan template. The order in which the tones are listed determines the order in which the tones are played. If multiple commas are specified, they are condensed to a single comma for the purposes of processing the dial-plan template. For example, if the match string is entered as “9,,,234” the phone interprets the string as “9,234” and the 3 commas are treated as a single comma.

The tones are case insensitive and are defined as follows:

- Bellcore-Inside
- Bellcore-Outside
- Bellcore-Busy
- Bellcore-drl
- Bellcore-Reorder
- Bellcore-CallWaiting
- Bellcore-Hold
- Bellcore-Reminder
- Cisco-ZipZip
- Cisco-Zip
- Cisco-BeepBonk
- Bellcore-None
- Bellcore-Confirmation
Chapter 2      Getting Started with Your Cisco SIP IP Phone

Creating Dial Plans

- Bellcore-Permanent

The following are examples of the changes to the dial-plan template:

- Specifying the # in the Dial-Plan Template Example, page 2-21
- Specifying the * in the Dial-Plan Template Example, page 2-21
- Specifying a Secondary Dial Tone in the Dial-Plan Template Example, page 2-21

Specifying the # in the Dial-Plan Template Example

The following is an example using the # as a dialed digit:

```xml
<DIALTEMPLATE>
  <TEMPLATE MATCH="123#45#6" TIMEOUT="0" User="Phone"/> <!-- Match # -->
  <TEMPLATE MATCH="34..." TIMEOUT="0" User="Phone"/> <!-- Match # -->
  <TEMPLATE MATCH="*" TIMEOUT="15" User="Phone"/>
</DIALTEMPLATE>
```

In the example above, the “123#45#6” string is matched if the user dials “123#45#6”. Pressing the # does not cause the phone to dial immediately because the # is specified. However, dialing “1#” or “123#4#” would cause the phone to dial immediately.

Specifying the * in the Dial-Plan Template Example

The following is an example specifying the * as a dialed digit:

```xml
<DIALTEMPLATE>
  <TEMPLATE MATCH="12\*345" TIMEOUT="0" User="Phone"/> <!-- Match * Char -->
  <TEMPLATE MATCH="*" TIMEOUT="10" User="Phone"/> <!-- Wildcard -->
</DIALTEMPLATE>
```

If the user specifies the \ with a digit other than the *, the \ is ignored and \ is matched, for example, specifying \\7 will match the digit 7. The \ is not sent out as part of the dialed digit string because the phone removes it before sending the dial string.

Specifying a Secondary Dial Tone in the Dial-Plan Template Example

The following is an example specifying two different tones:

```xml
<DIALTEMPLATE>
  <TEMPLATE MATCH="7,..." TIMEOUT="0" /> <!-- Default Secondary Dial tone -->
  <TEMPLATE MATCH="9,..." TIMEOUT="0" Tone="Cisco-Zip" /> <!-- Play Zip -->
  <TEMPLATE MATCH="8,..." TIMEOUT="0" Tone="Bellcore-Hold" /> <!-- Play Hold -->
  <TEMPLATE MATCH="8,123,..." TIMEOUT="0" Tone="Bellcore-Hold" Tone="Cisco-Zip" />
      <!--Play Hold after 8, Play Zip Tone after 123-->
</DIALTEMPLATE>
```
Managing Cisco SIP IP Phones

This chapter provides information on the following:

- Changing Your Configuration, page 3-1
- Modifying the Network Settings, page 3-2
- Modifying the SIP Settings, page 3-6
- Modifying Call Preferences, page 3-29
- Setting the Date, Time, and Daylight Saving Time, page 3-30
- Erasing the Locally Defined Settings, page 3-35
- Viewing the Firmware Version, page 3-36
- Upgrading the Cisco SIP IP Phone Firmware, page 3-37
- Performing an Image Upgrade and Remote Reboot, page 3-40

Changing Your Configuration

You can change your Cisco SIP IP phone configuration by any of the following methods:

- Using your phone buttons and soft keys. You must first follow the instructions in the “Entering Configuration Mode” section on page 3-2.
- Editing the default and phone-specific configuration files on the TFTP server. See the “Modifying SIP Parameters via a TFTP Server” section on page 3-9.
- Using Telnet or a console to connect to your Cisco SIP IP phone and using the command-line interface (CLI). You will need to the phone IP address. Press Settings, select Network Configuration, and scroll down to IP Address to find this address. The default Telnet password is “cisco.”

Note: Use the CLI only to debug and troubleshoot your Cisco SIP IP phone.

You can change the following parameters:

- Network settings. See the “Modifying the Network Settings” section on page 3-2.
- SIP settings. See the “Modifying the SIP Settings” section on page 3-6.
Modifying the Network Settings

You can display and configure the network settings of a Cisco SIP IP phone. The network settings include information such as the phone’s Dynamic Host Configuration Protocol (DHCP) server, MAC address, IP address, and domain name.

Entering Configuration Mode

When you access the network configuration information on your Cisco SIP IP phone, you will notice that there is a padlock symbol located in the upper-right corner of your LCD. By default, the network configuration information is locked. Before you can modify any of the network configuration parameters, you must unlock the phone.

Unlocking Configuration Mode

There are two methods to unlock the configuration mode in Cisco SIP IP phones: one method for phones that have Release 4.2 or later and one method for phones that have Release 4.1 or earlier.

In Release 4.2 or Later

In Release 4.2 and later, an “Unlock Config” item displays in the phone settings menu. When the user selects Unlock Config, the user is prompted to enter a phone password using the alphanumeric entry function of the keypad. The phone password is set using the phone_password configuration parameter. When the correct password is entered, the configuration is unlocked and the settings can be changed.

When the Network Configuration or SIP Configuration menus display, the lock icon in the upper-right corner of your LCD will indicate an unlocked state. The unlocked symbol indicates that you can modify the network and SIP configuration settings.

When the Settings menu is exited, the phone will automatically relock the configuration.

In Release 4.1 or Earlier

To unlock the Cisco SIP IP phone for releases before Cisco Release 4.2, press **#.

---

Note

Pressing **# activates the configuration mode for your phone; however there is no indication that an action has taken place.

If the Network Configuration or SIP Configuration panel is displayed, the lock icon in the upper-right corner of your LCD changes to an unlocked state. If you are located elsewhere in the Cisco SIP IP phone menus, the next time you access the Network Configuration or the SIP Configuration menus, the unlocked icon displays, and you can modify the network and SIP configuration settings.
Locking Configuration Mode

There are two methods to lock the configuration mode in Cisco SIP IP phones: one method for phones that have Release 4.2 or later and one method for phones that have Release 4.1 or earlier.

In Release 4.2 or Later

When the configuration has been successfully locked, the menu item displayed is “Lock Config.” If you select this item, the configuration will relock. Also, if you exit the Settings menu the configuration will relock. Refer to the “Unlocking Configuration Mode” section on page 3-2 for more information.

When the Network Configuration or SIP Configuration menus display, the lock icon in the upper-right corner of your LCD will indicate a locked state. The lock symbol indicates that you cannot modify the network and SIP configuration settings.

In Release 4.1 or Earlier

To lock the Cisco SIP IP phone when you are done modifying the settings, press **#. If the Network Configuration or SIP Configuration panel is displayed, the lock icon in the upper-right corner of your LCD changes to a locked state. If you are located elsewhere in the Cisco SIP IP phone menus, the next time you access the Network Configuration or the SIP Configuration panels, the lock icon will be displayed in a locked state. The lock symbol indicates that you cannot modify the network and SIP configuration settings.

Changing the Network Settings

Before You Begin

When configuring network settings, remember the following:

- Unlock configuration mode as described in the “Unlocking Configuration Mode” section on page 3-2. By default, the network parameters are locked to ensure that end users cannot modify settings that might affect their network connectivity.
- Review the guidelines on using the Cisco SIP IP phone menus documented in the “Using the Cisco SIP IP Phone Menu Interface” section on page 2-15.
- After making your changes, relock configuration mode as described in the “Locking Configuration Mode” section on page 3-3.

To change the network settings, perform the following steps:

**Step 1** Press the settings key. The Settings menu displays.

**Step 2** Highlight **Network Configuration**.

**Step 3** Press the Select soft key. The Network Configuration menu displays. Table 3-1 lists the network parameters available from the Network Configuration menu.

**Step 4** When done, press the Save soft key. The phone programs the new information into Flash memory and resets.
When you have completed your changes, ensure that you lock the phone as described in the “Locking Configuration Mode” section on page 3-3.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Can Edit?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin. VLAN Id</td>
<td>Can Edit?</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td>Yes, but if you have an</td>
<td>Unique identifier of the VLAN to which the phone is attached. The value in this field is used only in switched networks that are not Cisco networks.</td>
</tr>
<tr>
<td></td>
<td>administrative VLAN assigned on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the Catalyst switch, that</td>
<td></td>
</tr>
<tr>
<td></td>
<td>setting overrides any</td>
<td></td>
</tr>
<tr>
<td></td>
<td>changes made on the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>phone.</td>
<td></td>
</tr>
<tr>
<td>Alternate TFTP</td>
<td>Yes.</td>
<td>Whether to use an alternate TFTP server. This field enables an administrator to specify the remote TFTP server rather than the local one. Possible values for this parameter are Yes and No. The default is No. When Yes is specified, the IP address in the TFTP Address parameter must be changed to the address of the alternate TFTP server.</td>
</tr>
<tr>
<td>Default Routers 1 through 5</td>
<td>Yes, but DHCP must be disabled.</td>
<td>IP address of the default gateway used by the phone. Default Routers 2 through 5 are the IP addresses of the gateways that the phone attempts to use as an alternate gateway if the primary gateway is unavailable.</td>
</tr>
<tr>
<td>DHCP Address Released</td>
<td>Yes.</td>
<td>Whether the IP address of the phone can be released for reuse in the network. When you set this field to Yes, the phone sends a DHCP release message to the DHCP server and goes into a release state. The release state provides enough time to remove the phone from the network before the phone attempts to acquire another IP address from the DHCP server. When moving the phone to a new network segment, you should first release the DHCP address.</td>
</tr>
<tr>
<td>DHCP Enabled</td>
<td>Yes.</td>
<td>Whether the phone will use DHCP to configure network settings (IP address, subnet mask, domain name, default router list, DNS server list, and TFTP address). Valid values for this field are Yes and No. By default, DHCP is enabled on the phone. To manually configure your IP settings, you must first disable DHCP.</td>
</tr>
<tr>
<td>DNS Servers 1 through 5</td>
<td>Yes, but DHCP must be disabled.</td>
<td>IP address of the DNS server used by the phone to resolve names to IP addresses. The phone attempts to use DNS servers 2 through 5 if DNS server 1 is unavailable.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Yes.</td>
<td>Name of the DNS domain in which the phone resides.</td>
</tr>
</tbody>
</table>
Table 3-1  Network Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Can Edit?</th>
<th>Description</th>
</tr>
</thead>
</table>
| Dynamic DNS Server 1 and 2      | No.       | You can specify the IP address of a new dynamic DNS server. If a new DNS server is specified, it is used for any further DNS requests after the phone uses the initial DNS address upon bootup. The DNS addresses are used in the following order:  
1. dyn_dns_addr_1 (if present)  
2. dyn_dns_add_2 (if present)  
3. DNS Server 1  
4. DNS Server 2  
5. DNS Server 3  
6. DNS Server 4  
7. DNS Server 5  
The dynamic DNS address is not stored in Flash memory. |
| Dynamic TFTP Server             | No.       | You can specify the IP address of a new dynamic TFTP server. After initially querying the default TFTP server, the phone will rerequest the default and MAC-specific configuration files from the new TFTP server. The dynamic TFTP server is not stored in Flash memory. |
| Erase Configuration             | Yes.      | Whether to erase all of the locally defined network settings on the phone and reset the values to the defaults. Selecting Yes reenables DHCP. For more information on erasing the local configuration, see the “Erasing the Locally Defined Settings” section on page 3-35. |
| Host Name                       | No.       | Unique host name assigned to the phone. The value in this field is always SIPmac where mac is the MAC address of the phone. |
| HTTP Proxy Address              | Yes.      | The IP address of the HTTP proxy server. You can use either a dotted IP address or a DNS name (a record only). |
| HTTP Proxy Port                 | Yes.      | The port number of the outbound proxy port. The default is 80. |
| IP Address                      | Yes, but DHCP must be disabled. | IP address of the phone that either was assigned by DHCP or was locally configured. |
| MAC Address                     | No.       | Factory-assigned unique 48-bit hexadecimal MAC address of the phone. |
| Network Media Type              | Yes.      | Ethernet port negotiation mode. Valid values are as follows:  
• Auto—Port is autonegotiated. (This is the default value.)  
• Full-100—Port is configured to be a full-duplex, 100-MB connection.  
• Half-100—Port is configured to be a half-duplex, 100-MB connection.  
• Full-10—Port is configured to be a full-duplex, 10-MB connection.  
• Half-10—Port is configured to be a half-duplex, 10-MB connection. |
You can modify the SIP parameters of a Cisco SIP IP phone. When modifying SIP parameters, remember the following:

- Parameters defined in the default configuration file override the values stored in Flash memory.
- Parameters defined in the phone-specific configuration file override the values specified in the default configuration file.
- Parameters entered locally are used by the phone until the next reboot if a phone-specific configuration file exists.
- If you choose not to configure the phone via a TFTP server, you must manage the phone locally.

Table 3-2 lists each of the SIP parameters that you can configure. In the Configuration File column, the name of a parameter as you would specify it in a configuration file is listed. In the menu columns (SIP Configuration, Network Configuration, Call Preferences, and Time and Date), the name of the same parameter as it would appear on the user interface is listed. If NA appears in a menu column, the parameter cannot be defined using that menu.

### Table 3-2 Summary of SIP Parameters

<table>
<thead>
<tr>
<th>Configuration File</th>
<th>SIP Configuration Menu</th>
<th>Network Configuration Menu</th>
<th>Call Preferences</th>
<th>Time and Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>anonymous_call_block</td>
<td>—</td>
<td>—</td>
<td>Anonymous Call Block</td>
<td>—</td>
</tr>
<tr>
<td>autocomplete</td>
<td>—</td>
<td>—</td>
<td>Auto-Complete Numbers</td>
<td>—</td>
</tr>
<tr>
<td>callerid_blocking</td>
<td>—</td>
<td>—</td>
<td>Caller ID Blocking</td>
<td>—</td>
</tr>
</tbody>
</table>
Table 3-2  Summary of SIP Parameters (continued)

<table>
<thead>
<tr>
<th>Configuration File</th>
<th>SIP Configuration Menu</th>
<th>Network Configuration Menu</th>
<th>Call Preferences</th>
<th>Time and Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>call_hold_ringback</td>
<td></td>
<td>Call Hold Ringback</td>
<td>Call Waiting</td>
<td></td>
</tr>
<tr>
<td>call_waiting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cnf_join_enable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_format</td>
<td></td>
<td></td>
<td></td>
<td>Date Format</td>
</tr>
<tr>
<td>dial_template</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dnd_control</td>
<td></td>
<td></td>
<td>Do Not Disturb</td>
<td></td>
</tr>
<tr>
<td>dst_start_day</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_start_day_of_week</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_start_month</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_start_time</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_start_week_of_month</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_stop_day</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_stop_day_of_week</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_stop_month</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_stop_time</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_stop_week_of_month</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dtmf_avt_payload</td>
<td></td>
<td></td>
<td>Out of Band DTMF</td>
<td></td>
</tr>
<tr>
<td>dtmf_db_level</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dtmf_inband</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dtmf_outofband</td>
<td></td>
<td>End Media Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>enable_vad</td>
<td></td>
<td>Enable VAD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>end_media_port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>image_version</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>language</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>linex_authname (line1 to line6)</td>
<td></td>
<td>Authentication Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linex_displayname (line1 to line6)</td>
<td></td>
<td>Display Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linex_name (line1 to line6)</td>
<td></td>
<td>Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linex_password (line1 to line6)</td>
<td></td>
<td>Authentication Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linex_shortname (line1 to line6)</td>
<td>Shortname</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>messages_uri</td>
<td></td>
<td>Messages URI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nat_address</td>
<td></td>
<td>NAT Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nat_enable</td>
<td></td>
<td>NAT Enabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Table 3-2  Summary of SIP Parameters (continued)

<table>
<thead>
<tr>
<th>Configuration File</th>
<th>SIP Configuration Menu</th>
<th>Network Configuration Menu</th>
<th>Call Preferences</th>
<th>Time and Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>nat_received_processing</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>network_media_type</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>network_port2_type</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>outbound_proxy</td>
<td>Outbound Proxy</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>outbound_proxy_port</td>
<td>Outbound Proxy Port</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>phone_label</td>
<td>Phone Label</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>phone_password</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>phone_prompt</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>preferred_codec</td>
<td>Preferred Codec</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>proxy_backup</td>
<td>Backup Proxy</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>proxy_backup_port</td>
<td>Backup Proxy Port</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>proxy_emergency</td>
<td>Emergency Proxy</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>proxy_emergency_port</td>
<td>Emergency Proxy Port</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>proxy_register</td>
<td>Register with Proxy</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>proxyN_address (N=1 to 6)</td>
<td>Proxy Address</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>proxyN_port (N=1 to 6)</td>
<td>Proxy Port</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>remote_party_id</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>sip_invite_retx</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>sip_retx</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>snntp_mode</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>snntp_server</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>start_media_port</td>
<td>Start Media Port</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>sync</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>tftp_cfg_dir</td>
<td>TFTP Directory</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>time_format_24hr</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>Time format 24-hr</td>
</tr>
<tr>
<td>time_zone</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>Time Zone</td>
</tr>
<tr>
<td>timer_invite_expires</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>timer_register_expires</td>
<td>Register Expires</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>timer_t1</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>timer_t2</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>tos_media</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>
Chapter 3      Managing Cisco SIP IP Phones

Modifying SIP Parameters via a TFTP Server

If you have set up your phones to retrieve their SIP parameters via a TFTP server as described in the “Modifying SIP Parameters via a TFTP Server” section on page 3-9, you can also modify your SIP parameters using the configuration files.

As explained in the “Configuring SIP Parameters” section on page 2-4, there are two configuration files that you can use to define the SIP parameters: the default configuration file and the phone-specific configuration file. If used, the default configuration file must be stored in the root directory of your TFTP server. The phone-specific configuration file can be stored in the root directory of the TFTP server or in a subdirectory in which phone-specific configuration files are stored.

While it is not required, Cisco recommends that you use the default configuration file to define values for SIP parameters that are common to all phones. Doing so will make controlling and maintaining your network easier. You can then define only those parameters that are specific to a phone in the phone-specific configuration file, or they should be manually configured. Phone-specific parameters should not be defined in the default configuration file.

Modifying the Default SIP Configuration File

In the default configuration file (SIPDefault.cnf), Cisco recommends that you maintain the SIP parameters that are common to all your phones. By maintaining these parameters in the default configuration file, you can perform global changes, such as upgrading the image version, without having to modify the phone-specific configuration file for each phone.

Before You Begin

- Ensure that you have downloaded the SIPDefault.cnf file from Cisco.com to the root directory of your TFTP server.
- Review the guidelines documented in the “Configuring SIP Parameters” section on page 2-4.

Note

Refer to the “Setting the Date, Time, and Daylight Saving Time” section on page 3-30 for more information.

Step 1

Using an ASCII editor, open the SIPDefault.cnf file and define or modify values for the SIP parameters shown in Table 3-3, as necessary.

Step 2

Save the file with the same filename, SIPDefault.cnf, to the root directory of your TFTP server.
### Table 3-3  Default SIP Configuration File Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>anonymous_call_block</td>
<td>Optional</td>
<td>Configures anonymous call block. Valid values are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0—Disabled by default, but can be turned on and off using the user interface. When disabled, anonymous calls are received.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1—Enabled by default, but can be turned on and off using the user interface. When enabled, anonymous calls are rejected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2—Disabled permanently and cannot be turned on and off locally using the user interface. Specify this parameter in the phone-specific configuration file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3—Enabled permanently and cannot be turned on and off locally using the user interface. Specify this parameter in the phone-specific configuration file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is 0.</td>
</tr>
<tr>
<td>autocomplete</td>
<td>Optional</td>
<td>Configures automatic completion of numbers. Valid values are 0 (disable autocompletion) or 1 (enable autocompletion). The default is 1.</td>
</tr>
<tr>
<td>call_hold_ringback</td>
<td>Optional</td>
<td>Operates the same way that DND operates. It is selectable by the user in the Services-&gt;Call Preferences menu. When this value is enabled, the phone will ring if the handset is placed on-hook and there is a call currently on hold. If the value is disabled, the phone will not ring in this situation. Acceptable values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0—Off by default, but can be turned on and off locally using the user interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1—On by default, but can be turned on and off locally using the user interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2—Off permanently and cannot be turned on and off locally using the user interface. Specify this parameter in the phone-specific configuration file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3—On permanently and cannot be turned on and off locally using the user interface. Specify this parameter in the phone-specific configuration file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is 0.</td>
</tr>
</tbody>
</table>
Table 3-3  Default SIP Configuration File Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
</table>
| call_waiting    | Optional             | Configures call waiting. Valid values are as follows:  
|                 |                      |   - 0—Disabled by default, but can be turned on and off using the user interface. When disabled, call waiting calls are not received.  
|                 |                      |   - 1—Enabled by default, but can be turned on and off using the user interface. When enabled, call waiting calls are accepted.  
|                 |                      |   - 2—Disabled permanently and cannot be turned on and off locally using the user interface. Specify this parameter in the phone-specific configuration file.  
|                 |                      |   - 3—Enabled permanently and cannot be turned on and off locally using the user interface. Specify this parameter in the phone-specific configuration file.  
| callerid_blocking | Optional             | Configures caller ID blocking. When enabled, the phone blocks its own number or e-mail address from phones that have caller identification enabled. Valid values are as follows:  
|                 |                      |   - 0—Disabled by default, but can be turned on and off using the user interface. When disabled, the caller identification is included in the Request-URI header field.  
|                 |                      |   - 1—Enabled by default, but can be turned on and off using the user interface. When enabled, “Anonymous” is included in place of the user identification in the Request-URI header field.  
|                 |                      |   - 2—Disabled permanently and cannot be turned on and off locally using the user interface. Specify this parameter in the phone-specific configuration file.  
|                 |                      |   - 3—Enabled permanently and cannot be turned on and off locally using the user interface. Specify this parameter in the phone-specific configuration file.  
| cnf_join_enable | Optional             | Specifies whether or not the conference bridge, when the it hangs up, should attempt to join the two leaf nodes. Valid values are as follows:  
|                 |                      |   - 0—Do not join two leaf nodes.  
|                 |                      |   - 1—Join two leaf nodes.  
|                 |                      | The default value is 1.  |
### Table 3-3  Default SIP Configuration File Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
</table>
| date_format     | Optional             | Specifies the format for dates. Valid values are as follows:  
|                 |                      | • M/D/Y—Month/day/year  
|                 |                      | • D/M/Y—Day/month/year  
|                 |                      | • Y/M/D—Year/month/day  
|                 |                      | • Y/D/M—Year/day/month  
|                 |                      | • Y-M-D—Year-month-day  
|                 |                      | • YY-M-D—4-digit year-month-day  
|                 |                      | The default is M/D/Y. |
| directory_url   | Optional             | Specifies the URL of the external directory server. This URL is accessed when the Directory key is pressed and the External Directory option is selected. For example, use directory_url:  
|                 |                      | “http://10.10.10.10/CiscoServices/Directory.asp”. |
| dnd_control     | Optional             | Specifies Do Not Disturb (DND). Valid values are as follows:  
|                 |                      | • 0—Off by default, but can be turned on and off locally using the user interface.  
|                 |                      | • 1—On by default, but can be turned on and off locally using the user interface. The phone blocks all calls placed to the phone and logs those calls in the Missed Calls directory.  
|                 |                      | • 2—Off permanently and cannot be turned on and off locally using the user interface. Specify this parameter in the phone-specific configuration file.  
|                 |                      | • 3—On permanently and cannot be turned on and off locally using the user interface. This setting sets the phone to be a “call out” phone only. Specify this parameter in the phone-specific configuration file.  
|                 |                      | The default value is 0. |
### Table 3-3  Default SIP Configuration File Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dst_auto_adjust</td>
<td>Optional</td>
<td>Configures the date, time, and DST. See the “Setting the Date, Time, and Daylight Saving Time” section on page 3-30 for more information.</td>
</tr>
<tr>
<td>dst_offset</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_start_day</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_start_day_of_week</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_start_month</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_start_time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_start_week_of_month</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_stop_day</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_stop_day_of_week</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_stop_month</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_stop_time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst_stop_week_of_month</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dtmf_avt_payload</td>
<td>Optional</td>
<td>Configures the payload type for Audio/Video Transport (AVT) packets. Range is from 96 to 127. If the value specified exceeds 127, the phone defaults to 101.</td>
</tr>
<tr>
<td>dtmf_db_level</td>
<td>Optional</td>
<td>Specifies the in-band DTMF digit tone level. Valid values are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1—6 dB below nominal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2—3 dB below nominal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3—nominal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 4—3 dB above nominal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 5—6 dB above nominal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is 3.</td>
</tr>
<tr>
<td>dtmf_inband</td>
<td>Optional</td>
<td>Configures the in-band signaling format. Valid values are 1 (generate DTMF digits in-band) and 0 (do not generate DTMF digits in-band). The default is 1.</td>
</tr>
</tbody>
</table>
Table 3-3  Default SIP Configuration File Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dtmf_outofband</td>
<td>Optional</td>
<td>Configures the out-of-band signaling (for tone detection on the IP side of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a gateway). The Cisco SIP IP phone supports out-of-bound signaling using the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AVT tone method.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: The default is avt.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valid values are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• none—Do not generate DTMF digits out-of-band.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• avt—If requested by the remote side, generate DTMF digits out-of-band</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(and disable in-band DTMF signaling); otherwise, do not generate DTMF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>digits out-of-band.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• avt_always—Always generate DTMF digits out-of-band. This option disables</td>
</tr>
<tr>
<td></td>
<td></td>
<td>in-band DTMF signaling.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dyn_dns_addr_1</td>
<td>Optional</td>
<td>Specifies the IP address of a new dynamic DNS server. If a new DNS server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>is specified, it is used for any further DNS requests after the phone uses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the initial DNS address upon bootup. The DNS addresses are used in the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>following order:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. dyn_dns_addr_1 (if present)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. dyn_dns_addr_2 (if present)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. DNS Server 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. DNS Server 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. DNS Server 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. DNS Server 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. DNS Server 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The dynamic DNS address is not stored in Flash memory. Only dotted IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>addresses are accepted. This value can be cleared by removing it from the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configuration file or changing its value to a null value “” or “UNPROVISIONED.”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dyn_dns_addr_2</td>
<td>Optional</td>
<td>Specifies a second dynamic DNS to be used for DNS requests.</td>
</tr>
</tbody>
</table>
Table 3-3  Default SIP Configuration File Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dyn_tftp_addr</td>
<td>Optional</td>
<td>Specifies the IP address of a new dynamic TFTP server. After initially querying the default TFTP server, the phone will rerequest the default and MAC-specific configuration files from the new TFTP server. The dynamic TFTP server is not stored in Flash memory. The number of dyn_tftp_addr values supported by the phone is limited to prevent the phone from bouncing between two TFTP servers. Only dotted IP addresses are accepted. This value can be cleared by removing it from the configuration file or changing its value to a null value “” or “UNPROVISIONED.”</td>
</tr>
<tr>
<td>enable_vad</td>
<td>Optional</td>
<td>Enables or disables VAD. Valid values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0—Disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1—Enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is 0.</td>
</tr>
<tr>
<td>end_media_port</td>
<td>Optional</td>
<td>Configures the Real-Time Transport Protocol (RTP) end range for media. Valid values are from 16,384 to 32,766. Default is 32,766.</td>
</tr>
<tr>
<td>http_proxy_addr</td>
<td>Optional</td>
<td>Specifies the IP address of the HTTP proxy server. You can use either a dotted IP address or a DNS name (a record only).</td>
</tr>
<tr>
<td>http_proxy_port</td>
<td>Optional</td>
<td>Specifies the number of the HTTP proxy port. The default is 80.</td>
</tr>
<tr>
<td>image_version</td>
<td>Required</td>
<td>Specifies the firmware version that the Cisco SIP IP phone should run. Enter the name of the image version (as it is released by Cisco). Do not enter the extension. You cannot change the image version by changing the filename because the version is also built into the file header. Trying to change the image version by changing the filename causes the firmware to fail when it compares the version in the header against the filename.</td>
</tr>
<tr>
<td>language</td>
<td>Optional</td>
<td>This parameter is for future use. English is the only value that is currently supported.</td>
</tr>
</tbody>
</table>
### Table 3-3 Default SIP Configuration File Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logo_url</td>
<td>Optional</td>
<td>Specifies the location of the company logo file. This logo appears on the phone display. The background space allocated for the image is 90 x 56 pixels. Images that are larger than this will automatically be scaled down to 90 x 56 pixels. The recommended file size for the image is from 5 to 15 Kb. For example, use logo_url: “<a href="http://10.10.10.10/companylogo.bmp%E2%80%9D">http://10.10.10.10/companylogo.bmp”</a>. <strong>Note</strong>: This parameter supports Windows 256 color bitmap format only. CMXML PhoneImage objects are not supported for this parameter. Using anything other than a Windows bit-map (.bmp) file can cause unpredictable results.</td>
</tr>
<tr>
<td>messages_uri</td>
<td>Optional</td>
<td>Configures the voice-mail number when the messages button is pressed.</td>
</tr>
<tr>
<td>nat_address</td>
<td>Optional</td>
<td>Specifies the WAN IP address of the NAT or firewall server. You can use either a dotted IP address or a DNS name (a record only).</td>
</tr>
<tr>
<td>nat_enable</td>
<td>Optional</td>
<td>Enables or disables NAT. Valid values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0—Disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1—Enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When NAT is enabled, the Contact header appears as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contact: sip:lineN_name@nat_address:voip_control_port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If nat_address is invalid or UNPROVISIONED, the Contact header appears as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contact: sip:lineN_name@phone_ip_address:voip_control_port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and the Via header appears as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Via: SIP/2.0/UDP phone_ip_address:voip_control_port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If NAT is enabled, the Session Description Protocol (SDP) message uses the nat_address and an RTP port between the start_media_port and the end_media_port range in the C and M fields. All RTP traffic is sourced from the port advertised in the SDP.</td>
</tr>
</tbody>
</table>
Table 3-3  Default SIP Configuration File Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
</table>
| nat_received_processing | Optional             | Enables or disables NAT received processing. Valid values are:  
|                     |                      | 0—Disable  
|                     |                      | 1—Enable  
|                     |                      | The default is 0.  
|                     |                      | If nat_received_processing is enabled, and received= tag is in the Via header of the 200 OK response from a REGISTER, the IP address in the received= tag is used instead of the nat_address in the Contact header. If this switch occurs, the phone unregisters the old IP address and reregisters with the new IP address. |
| network_media_type  | Optional             | Specifies the Ethernet port negotiation mode. Valid values are as follows:  
|                     |                      | • Auto—Port is autonegotiated.  
|                     |                      | • Full100—Port is configured to be a full-duplex, 100-MB connection.  
|                     |                      | • Half100—Port is configured to be a half-duplex, 100-MB connection.  
|                     |                      | • Full10—Port is configured to be a full-duplex, 10-MB connection.  
|                     |                      | • Half10—Port is configured to be a half-duplex, 10-MB connection.  
|                     |                      | The default is Auto. |
| network_port2_type  | Optional             | Configures the device type that is connected to port 2 of the phone. Valid values are as follows:  
|                     |                      | • Hub/Switch (default)  
|                     |                      | • PC  
|                     |                      | **Note** If the value is PC, port 2 can be connected only to a PC. If you are not sure about the connection, use the default value. Using a value of “PC” and connecting port 2 to a switch results in spanning-tree loops and network confusion. |
| outbound_proxy      | Optional             | Specifies the IP address of the outbound proxy server. You can use either a dotted IP address or a DNS name. |
### Table 3-3  Default SIP Configuration File Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
</table>
| outbound_proxy_port     | Optional             | Specifies the port number of the outbound proxy server. The default is 5060. When outbound proxy is enabled, all SIP requests are sent to the outbound proxy server instead of the proxyN_address. All responses continue to reconcile the normal Via processing rules. The media stream is not routed through the outbound proxy. NAT and outbound proxy modes can be independently enabled or disabled. The received= tag is added to the Via header of all responses if there is no received= tag in the uppermost Via header and if the source IP address is different from the IP address in the uppermost Via header. Responses are sent back to the source under the following conditions:  
  - If a received= tag is in the uppermost Via header, the response is sent back to the IP address contained in the received= tag.  
  - If there is no received= tag and the IP address in the uppermost Via header is different from the source IP address, the response is sent back to the source IP. Otherwise, the response is sent back to the IP address in the uppermost Via header. |
| phone_password          | Optional             | Specifies a password to be used for console or Telnet access. The default password is “cisco.”               |
| phone_prompt            | Optional             | Specifies the prompt to be displayed when using Telnet or console access. The default phone prompt is “SIP Phone.” |
| preferred_codec         | Optional             | Specifies the codec to use when a call is initiated. Valid values are g711ulaw, g711ulaw, g729a, and none. The default is g711ulaw. |
| proxy_backup            | Optional             | Specifies the IP address of the backup proxy server or gateway. Enter this address in IP dotted-decimal notation. |
| proxy_backup_port       | Optional             | Specifies the port number of the backup proxy server. Default is 5060.                                         |
| proxy_emergency         | Optional             | Specifies the IP address of the emergency proxy server or gateway. Enter this address in IP dotted-decimal notation. |
| proxy_emergency_port    | Optional             | Specifies the port number of the emergency proxy server. Default is 5060.                                         |
### Table 3-3 Default SIP Configuration File Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proxy_register</td>
<td>Optional</td>
<td>Specifies that the phone must register with a proxy server during initialization. Valid values are 0 and 1. Specify 0 to disable registration during initialization. Specify 1 to enable registration during initialization. The default is 0. After a phone has initialized and registered with a proxy server, changing the value of this parameter, using manual configuration, to 0 unregisters the phone from the proxy server. To reinitiate a registration, change the value of this parameter back to 1. <strong>Note</strong> If you enable registration, and authentication is required, you must specify values for the line_authname and line_password parameters (where x is a number from 1 to 6) in the phone-specific configuration file. For information on configuring the phone-specific configuration file, refer to the “Modifying the Phone-Specific SIP Configuration File” section on page 3-24.</td>
</tr>
<tr>
<td>proxy1_address</td>
<td>Required</td>
<td>Specifies the IP address of the primary SIP proxy server that will be used by the phones. Enter this address in IP dotted-decimal notation.</td>
</tr>
<tr>
<td>proxy1_port</td>
<td>Optional</td>
<td>Specifies the port number of the primary SIP proxy server. This is the port on which the SIP client listens for messages. The default is 5060.</td>
</tr>
<tr>
<td>proxyN_address</td>
<td>Optional</td>
<td>Specifies the IP address or DNS name of the SIP proxy server that will be used by phone lines other than line 1. For IP address, use the IP dotted-decimal notation. If the proxyN_address parameter is provisioned with an FQDN, the phone sends REGISTER and INVITE messages by using the FQDN in the Req-URI, To, and From fields. If you want to use a dotted IP address, the proxyN_address parameters should be configured as dotted IP addresses.</td>
</tr>
<tr>
<td>proxyN_port</td>
<td>Optional</td>
<td>Specifies the port number of the SIP proxy server that will be used by phone lines other than line 1.</td>
</tr>
</tbody>
</table>
### Table 3-3  Default SIP Configuration File Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
</table>
| remote_party_id        | Optional             | Specifies the Remote-Party-ID header supports network verification and screening of a call participant’s identity (for example, name and number) and provides privacy for call participants. Valid values are as follows:  
  - 0—Remote party ID is disabled. The phone does not send or accept the Remote Party ID.  
  - 1—Remote party ID is enabled. The phone sends the Remote Party ID, and can accept the Remote Party ID.  
  The default value is 0. |
| semi_attended_transfer| Optional             | Defines whether or not the caller can transfer the second leg of an attended transfer while the call is ringing. Valid values are as follows:  
  - 0—Semi-attended transfer is disabled.  
  - 1—Semi-attended transfer is enabled.  
  The default value is 1. |
| services_url           | Optional             | Specifies the URL of the services BTXML files. This URL is accessed when the Services button is pressed. For example, use services_url: “http://10.10.10.10/CiscoServices/Services.asp” |
| sip_invite_retx        | Optional             | Specifies the maximum number of times that an INVITE request will be retransmitted. The valid value is any positive integer. The default is 6. |
| sip_retx               | Optional             | Specifies the maximum number of times that a SIP message other than an INVITE request will be retransmitted. The valid value is any positive integer. The default is 10. |
| sntp_mode              | Optional             | See the “Setting the Date, Time, and Daylight Saving Time” section on page 3-30 for more information. |
| sntp_server            | Optional             | Specifies the start RTP range for media. Valid values are from 16,384 to 32,766. Default is 16,384. |
| start_media_port       | Optional             | Specifies the value against which to compare the value in the syncinfo.xml file before a remote reboot is performed. Valid value is a character string up to 32 characters long. |
Table 3-3  Default SIP Configuration File Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>telnet_level</td>
<td>Optional</td>
<td>Enables Telnet for the phone. Valid values are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 0—Telnet is disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 1—Telnet is enabled, no privileged commands.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 2—Telnet is enabled and privileged commands can be executed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is 0.</td>
</tr>
<tr>
<td>tftp_cfg_dir</td>
<td>Required¹</td>
<td>Specifies the path to the TFTP subdirectory in which phone-specific</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configuration files are stored.</td>
</tr>
<tr>
<td>time_format_24hr</td>
<td>Optional</td>
<td>Specifies the whether a 12- or 24-hour time format is displayed by default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>on the user interface. Valid values are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 0—12-hour format is displayed by default but can be changed to a 24-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hour format using the user interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 1—24-hour format is displayed by default but can be changed to a 12-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hour format using the user interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 2—12-hour format is displayed and cannot be changed to a 24-hour</td>
</tr>
<tr>
<td></td>
<td></td>
<td>format using the user interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 3—24-hour format is displayed and cannot be changed to a 12-hour</td>
</tr>
<tr>
<td></td>
<td></td>
<td>format using the user interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is 1.</td>
</tr>
<tr>
<td>time_zone</td>
<td>Optional</td>
<td>See the “Setting the Date, Time, and Daylight Saving Time” section on page</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-30 for more information.</td>
</tr>
<tr>
<td>timer_invite_expires</td>
<td>Optional</td>
<td>Specifies the amount of time, in seconds, after which a SIP INVITE expires.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This value is used in the Expire header field. The valid value is any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>positive number; however, Cisco recommends 180 seconds. The default is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>180.</td>
</tr>
<tr>
<td>timer_register_expires</td>
<td>Optional</td>
<td>Specifies the amount of time, in seconds, after which a REGISTRATION</td>
</tr>
<tr>
<td></td>
<td></td>
<td>request expires. This value is inserted into the Expire header field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The valid value is any positive number; however, Cisco recommends 3600</td>
</tr>
<tr>
<td></td>
<td></td>
<td>seconds. The default is 3600.</td>
</tr>
<tr>
<td>timer_t1</td>
<td>Optional</td>
<td>Specifies the lowest value, in milliseconds, of the retransmission timer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>for SIP messages. The valid value is any positive integer. The default is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>500.</td>
</tr>
<tr>
<td>timer_t2</td>
<td>Optional</td>
<td>Specifies the highest value, in milliseconds, of the retransmission timer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>for SIP messages. The valid value is any positive integer greater than</td>
</tr>
<tr>
<td></td>
<td></td>
<td>timer_t1. The default is 4000.</td>
</tr>
</tbody>
</table>
The following is a sample SIP default configuration file:

```
# Image Version
image_version: "P0S3-xx-y-zz"

# Proxy Server
proxy1_address: "proxy.company.com"
proxy2_address: ""
proxy3_address: ""
proxy4_address: ""
proxy5_address: ""
proxy6_address: ""

# Proxy Server Port (default - 5060)
proxy1_port: "5060"
proxy2_port: ""
proxy3_port: ""
proxy4_port: ""
proxy5_port: ""
proxy6_port: ""

# Emergency Proxy info
proxy_emergency: "1.2.3.4"
proxy_emergency_port: "5060"
```

1. Required if phone-specific configuration files are located in a subdirectory.
# Backup Proxy info
proxy_backup: "1.2.3.4"
proxy_backup_port: "5060"

# Proxy Registration (0-disable (default), 1-enable)
proxy_register: "1"

timer_register_expires: "180"

# Codec for media stream (g711ulaw (default), g711alaw, g729)
preferred_codec: "g711ulaw"

tos_media: "5"

# In-band DTMF Settings (0-disable, 1-enable (default))
dtmf_inband: "1"

# Out-of-band DTMF Settings (none-disable, avt-avt enable (default), avt_always - always avt)
dtmf_outofband: "avt"

dtmf_db_level: "3"

# SIP Timers
timer_t1: "500" ; Default 500 ms
timer_t2: "4000" ; Default 4 sec
sip_retx: "10" ; Default 11
sip_invite_retx: "6" ; Default 7
timer_invite_expires: "180" ; Default 180 sec

# Setting for Message speed dial to Voice mail
messages_uri: "9195551000"

#********* Release 2 new configuration parameters **********

# TFTP Phone Specific Configuration File Directory
tftp_cfg_dir: "/"

dst_offset: "1"
dst_start_month: "April"
dst_start_day: ""
dst_start_day_of_week: "Sun"
dst_start_week_of_month: "1"
dst_start_time: "02"
dst_stop_month: "Oct"
dst_stop_day: ""
dst_stop_day_of_week: "Sunday"
dst_stop_week_of_month: "8"
dst_stop_time: "2"
dst_auto_adjust: "1"

dnd_control: "0" ; Default 0 (Do Not Disturb feature is off)
# Caller ID Blocking (0-disabled, 1-enabled, 2-disabled no user control, 3-enabled no user control)
callerid_blocking: "0" ; Default 0 (Disable sending all calls as anonymous)

# Anonymous Call Blocking (0-disabled, 1-enabled, 2-disabled no user control, 3-enabled no user control)
anonymous_call_block: "0" ; Default 0 (Disable blocking of anonymous calls)

# DTMF AVT Payload (Dynamic payload range for AVT tones - 96-127)
dtmf_avt_payload: "101" ; Default 101

# XML file that specifies the dial plan desired
dial_template: "dialplan"

# Network Media Type (auto, full100, full10, half100, half10)
network_media_type: "auto"

# Autocompletion During Dial (0-off, 1-on [default])
autocomplete: "1"

# Time Format (0-12hr, 1-24hr [default])
time_format_24hr: "1"

# Enable or Disable VAD (0-disabled (default), 1-enabled)
enable_vad: 0
telnet_level: 0
phone_password: "cisco"

# URL for External XML Services and Phone Logo
services_url: "http://www.company.com/phone/services.asp"
directory_url: "http://www.company.com/phone/companydirectory.asp"
logo_url: "http://www.company.com/phone/logo.bmp"

**Modifying the Phone-Specific SIP Configuration File**

Before you begin modifying the configuration file:

- Review the guidelines documented in the “Modifying the Default SIP Configuration File” section on page 3-9.

- Line parameters (those identified as line x) define a line on the phone. If you configure a line to use an e-mail address, that line can be called only by using an e-mail address. Similarly, if you configure a line to use a number, that line can be called only by using the number. Each line can have a different proxy configured.

To modify the phone-specific SIP configuration file, open the file in an ASCII text editor. In the file, define values for the SIP parameters shown in Table 3-4. For all variables, x is a number 1 through 6.
### Table 3-4 Phone-Specific Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>line1_authname</td>
<td>Required¹</td>
<td>Name used by the phone for authentication if a registration is challenged by the proxy server during initialization. If a value is not configured for the line1_authname parameter for a line when registration is enabled, the value defined for line 1 is used. If a value is not defined for line 1, the default line1_authname is UNPROVISIONED.</td>
</tr>
<tr>
<td>line2_displayname</td>
<td>Optional</td>
<td>Identification as it should appear for caller identification purposes. For example, instead of <a href="mailto:jdoe@company.com">jdoe@company.com</a> appearing on phones that have caller ID, you can specify John Doe in this parameter to have John Doe appear on the callee end instead. If a value is not specified for this parameter, nothing is used.</td>
</tr>
<tr>
<td>line2_name</td>
<td>Optional</td>
<td>Number or e-mail address used when registering. When entering a number, enter the number without any dashes. For example, enter 555-1212 as 5551212. When entering an e-mail address, enter the e-mail ID without the host name.</td>
</tr>
<tr>
<td>line2_password</td>
<td>Required¹</td>
<td>Password used by the phone for authentication if a registration is challenged by the proxy server during initialization. If a value is not configured for the line2_password parameter for a line when registration is enabled, the value defined for line 1 is used. If a value is not defined for line 1, the default line1_password is UNPROVISIONED.</td>
</tr>
<tr>
<td>line3_displayname</td>
<td>Optional</td>
<td>Name or number associated with the line3_name as you want it to display on the phone’s LCD if the line3_name length exceeds the allowable space in the display area. For example, if the line3_name value is the phone number 111-222-333-4444, you can specify 34444 for this parameter to have 34444 display on the LCD instead. Alternatively, if the value for the line3_name parameter is the e-mail address “<a href="mailto:username@company.com">username@company.com</a>”, you can specify the “username” to have just the username appear on the LCD instead. This parameter is used for display only. If a value is not specified for this parameter, the value in the line3_name variable is displayed.</td>
</tr>
<tr>
<td>line3_name</td>
<td>Optional</td>
<td>Label to display on the top status line of the LCD. This field is for end-user display only. For example, a phone label can display “John Doe’s phone.” Up to 11 characters can be used to specify the phone label. Save the file to your TFTP server (in the root directory or in a subdirectory that contains all the phone-specific configuration files). Name the file SIPXXXXYYYYZZZZ.cnf where XXXXXXXXX is the MAC address of the phone. The MAC address must be in uppercase, and the extension, cnf, must be in lower case (for example, SIP00503EFFD842.cnf).</td>
</tr>
</tbody>
</table>

¹ Required for line 1 when registration is enabled and the proxy server requires authentication.

The following is a sample phone-specific configuration file:

```bash
line1_displayname: "jdoe43"
line1_name: "43"
line2_displayname: "jdoe44"
line2_name: "44"
line3_displayname: "pgatour"
```
Modifying the SIP Parameters Directly on Your Phone

If you did not configure the SIP parameters using a TFTP server, you can configure them directly on your phone after you have connected the phone.

Before You Begin

- Unlock configuration mode as described in the “Unlocking Configuration Mode” section on page 3-2. By default, the SIP parameters are locked to ensure that end users cannot modify settings that might affect their call capabilities.
- Review the guidelines on using the Cisco SIP IP phone menus documented in the “Using the Cisco SIP IP Phone Menu Interface” section on page 2-15.
- Line parameters (those identified as line x) define a line on the phone. If you configure a line to use an e-mail address, that line can be called only by using an e-mail address. Similarly, if you configure a line to use a number, that line can be called only by using the number.
- When configuring the Preferred Codec and Out of Band DTMF parameters, press the Change soft key until the option that you desire is displayed and then press the Save soft key.
- After making your changes, relock configuration mode as described in the “Locking Configuration Mode” section on page 3-3.

Step 1
Press the settings key. The Settings menu appears.

Step 2
Highlight SIP Configuration. The SIP Configuration menu appears.
Step 3  Highlight **Line 1 Settings**.

Step 4  Press the **Select** soft key. The Line 1 Configuration menu appears.

Step 5  Highlight and press the **Select** soft key to configure the parameters shown in Table 3-5, as necessary.

Step 6  Press the **Back** soft key to exit the Line 1 Configuration menu.

Step 7  To configure additional lines on the phone, highlight the next **Line x Settings**, press the **Select** soft key and repeat Step 5 and Step 6, and then continue with Step 8.

Step 8  In addition to the line settings, you can highlight and press **Select** to configure the parameters on the SIP Configuration menu shown in Table 3-6.

Step 9  When done, press the **Save** soft key to save your changes and exit the SIP Configuration menu.

---

**Caution** When you have completed your changes, ensure that you lock the phone as described in the “Locking Configuration Mode” section on page 3-3.

---

### Table 3-5  SIP Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Password</td>
<td>Required(^1)</td>
<td>Password used by the phone for authentication if a registration is challenged by the proxy server during initialization. If a value is not configured for the Authentication Password parameter when registration is enabled, the default logical password is used. The default logical password is SIPmac-address, where mac-address is the MAC address of the phone.</td>
</tr>
<tr>
<td>Authentication Name</td>
<td>Required(^1)</td>
<td>Name used by the phone for authentication if a registration is challenged by the proxy server during initialization.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Optional</td>
<td>Identification as it should appear for caller identification. For example, instead of <a href="mailto:jdoe@company.com">jdoe@company.com</a> appearing on phones that have caller ID, you can specify John Doe in this parameter to have John Doe appear on the callee end instead. If a value is not specified for this parameter, the Name value is used.</td>
</tr>
<tr>
<td>Name</td>
<td>Required</td>
<td>Description number or e-mail address used when registering. When entering a number, enter the number without any dashes. For example, enter 555-1212 as 5551212. When entering an e-mail address, enter the e-mail ID without the host name.</td>
</tr>
<tr>
<td>Proxy Address</td>
<td>Required</td>
<td>IP address of the primary SIP proxy server that will be used by the phone. Enter this address in IP dotted-decimal notation.</td>
</tr>
</tbody>
</table>
Modifying the SIP Settings

Chapter 3      Managing Cisco SIP IP Phones

Table 3-5    SIP Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Port</td>
<td>Optional</td>
<td>Port number of the primary SIP proxy server. This is the port that the SIP client will use. The default is 5060.</td>
</tr>
<tr>
<td>Short Name</td>
<td>Optional</td>
<td>Name or number associated with the line_name as you want it to display on the phone LCD if the line_name value exceeds the display area. For example, if the line_name value is the phone number 111-222-333-4444, you can specify 34444 for this parameter to have 3444 display on the LCD instead. Alternatively, if the value for the line_name parameter is the e-mail address “<a href="mailto:username@company.com">username@company.com</a>”, you can specify the “username” to have just the username appear on the LCD instead. This parameter is used for display only. If a value is not specified for this parameter, the value in the Name variable is displayed.</td>
</tr>
</tbody>
</table>

1. Required when registration is enabled.

Table 3-6    Additional SIP Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Proxy</td>
<td>Optional</td>
<td>IP address of the backup proxy server or gateway. Enter this address in IP dotted-decimal notation.</td>
</tr>
<tr>
<td>Backup Proxy Port</td>
<td>Optional</td>
<td>Port number of the backup proxy server. Default is 5060.</td>
</tr>
<tr>
<td>Emergency Proxy</td>
<td>Optional</td>
<td>IP address of the emergency proxy server or gateway. Enter this address in IP dotted-decimal notation.</td>
</tr>
<tr>
<td>Emergency Proxy Port</td>
<td>Optional</td>
<td>Port number of the emergency proxy. Default is 5060.</td>
</tr>
<tr>
<td>Enable VAD</td>
<td>Optional</td>
<td>Specifies whether VAD is enabled or disabled.</td>
</tr>
<tr>
<td>End Media Port</td>
<td>Optional</td>
<td>The end RTP range for media. Valid values are 16,384 to 32,766. Default is 32,766.</td>
</tr>
<tr>
<td>Messages URI</td>
<td>Optional</td>
<td>Number to call to check voice mail. This number is called when the Messages key is pressed.</td>
</tr>
<tr>
<td>NAT Address</td>
<td>Optional</td>
<td>The WAN IP address of the NAT or firewall server. You can use either a dotted IP address or a DNS name (a record only).</td>
</tr>
<tr>
<td>NAT Enabled</td>
<td>Optional</td>
<td>Choose No to disable NAT and Yes to enable NAT.</td>
</tr>
</tbody>
</table>
| Out of Band DTMF        | Optional             | Whether to detect and generate the out-of-band signaling (for tone detection on the IP side of a gateway) and if so, when. The Cisco SIP IP phone supports out-of-bound signaling via the AVT tone method. Valid values are as follows:  
  • none—Do not generate DTMF digits out-of-band.  
  • avt—If requested by the remote side, generate DTMF digits out-of-band (and disable in-band DTMF signaling); otherwise, do not generate DTMF digits out-of-band.  
  • avt_always—Always generate DTMF digits out-of-band. This option disables in-band DTMF signaling.  
  The default is avt. |
Chapter 3      Managing Cisco SIP IP Phones

Modifying Call Preferences

The call preferences can be modified only if the configuration variable for each setting has been set to 0 or 1 by the system administrator. If the variables are configured as 2 or 3, the call preferences cannot be modified with the Call Preferences menu. See Table 3-2 on page 3-6 for descriptions of each parameter.

You can modify the call preferences on each phone using the Call Preferences menu as follows:

1. Press the **settings** key. The Settings menu displays.
2. Highlight **Call Preferences**. The Call Preferences configuration menu displays.
3. Press the **Select** soft key.

### Table 3-6 Additional SIP Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound Proxy</td>
<td>Optional</td>
<td>The IP address of the outbound proxy server. You can use either a dotted IP address or a DNS name.</td>
</tr>
<tr>
<td>Outbound Proxy Port</td>
<td>Optional</td>
<td>The port number of the outbound proxy server. The default is 5060.</td>
</tr>
<tr>
<td>Phone Label</td>
<td>Optional</td>
<td>Label to display on the top status line of the LCD. This field is for end-user display only. For example, a phone’s label can display “John Doe’s phone.” Up to 11 characters can be used when specifying the phone label.</td>
</tr>
<tr>
<td>Register Expires</td>
<td>Optional</td>
<td>The amount of time, in seconds, after which a REGISTRATION request expires. This value is used the Expire header field. The valid value is any positive number; however, Cisco recommends 3600 seconds. The default is 3600.</td>
</tr>
<tr>
<td>Register with Proxy</td>
<td>Optional</td>
<td>Whether the phone must register with a proxy server during initialization. Select the <strong>No</strong> soft key to disable registration during initialization. Select the <strong>Yes</strong> soft key to enable registration during initialization. The default is No. After a phone has initialized and registered with a proxy server, changing the value of this parameter to No unregisters the phone from the proxy server. To reinitiate a registration, change the value of this parameter back to Yes.</td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td>If you enable registration, and authentication is required, you must specify values for the Authentication Name and Authentication Password parameters.</td>
</tr>
<tr>
<td>Start Media Port</td>
<td>Optional</td>
<td>The start RTP range for media. Valid values are from 16,384 to 32,766. Default is 16,384.</td>
</tr>
<tr>
<td>TFTP Directory</td>
<td>Required1</td>
<td>Path to the TFTP subdirectory in which phone-specific configuration files are stored.</td>
</tr>
<tr>
<td>VoIP Control Port</td>
<td>Optional</td>
<td>The UDP port used for SIP messages. All SIP REQUESTS use voip_control_port as the UDP source port when nat_enable = 1. Valid values are from 1,025 to 65,535. Default is 5060.</td>
</tr>
</tbody>
</table>

1. Required if phone-specific configuration files are located in a subdirectory.

---

**Modifying Call Preferences**

The call preferences can be modified only if the configuration variable for each setting has been set to 0 or 1 by the system administrator. If the variables are configured as 2 or 3, the call preferences cannot be modified with the Call Preferences menu. See Table 3-2 on page 3-6 for descriptions of each parameter.

You can modify the call preferences on each phone using the Call Preferences menu as follows:

1. Press the **settings** key. The Settings menu displays.
2. Highlight **Call Preferences**. The Call Preferences configuration menu displays.
3. Press the **Select** soft key.
Setting the Date, Time, and Daylight Saving Time

The current date and time is supported on the Cisco SIP IP phone via SNTP and is displayed on the phone’s LCD. In addition to supporting the current date and time, daylight saving time (DST) and time zone settings are also supported. DST can be configured to be obtained via an absolute (for example, starts on April 1 and ends on October 1) or relative (for example, starts on the first Sunday in April and ends on the last day of October) configuration.

The format for the date can be set using the date_format parameter. International time zone abbreviations are supported and are case sensitive (must be in all capital letters). Cisco recommends that date- and time-related parameters be defined in the SIPDefault.cnf file. The time zone parameter can be set manually on the phone or in the configuration file.

Before You Begin
When configuring the date, time, time zone, and DST settings, remember the following:

- Review the guidelines and restrictions documented in the “Modifying the Default SIP Configuration File” section on page 3-9.
- Determine whether you want to configure absolute DST or relative DST.
- The SNTP parameters specify how the phone will obtain the current time from an SNTP server. Review the guidelines in Table 3-7 and Table 3-8 before configuring the SNTP parameters.

Table 3-7 lists the actions that take place when a null value (0.0.0.0) is specified in the sntp_server parameter.
Table 3-7  Actions Based on sntp_mode When the sntp_server Parameter Is Set to a Null Value

<table>
<thead>
<tr>
<th>sntp_server</th>
<th>sntp_mode= unicast</th>
<th>sntp_mode= multicast</th>
<th>sntp_mode= anycast</th>
<th>sntp_mode= directedbroadcast</th>
</tr>
</thead>
<tbody>
<tr>
<td>=0.0.0.0</td>
<td>Sends</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nothing.</td>
<td>No known server with</td>
<td>SNTP packet to the</td>
<td>SNTP packet to the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>which to communicate.</td>
<td>local network</td>
<td>local network broadcast</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>broadcast address.</td>
<td>address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>After the first SNTP</td>
<td>After the first SNTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>response is received,</td>
<td>response is received,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>the phone switches</td>
<td>the phone switches to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>to unicast mode</td>
<td>multicast mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>with the server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>being set as the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>one who first</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>responded.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Receives</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nothing.</td>
<td>No known server with</td>
<td>Unicast SNTP data</td>
<td>SNTP data from the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>which to communicate.</td>
<td>from the SNTP</td>
<td>SNTP/NTP multicast</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>server that first</td>
<td>address and the local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>responded to the</td>
<td>network broadcast address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>network broadcast</td>
<td>from any server on the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>request.</td>
<td>network.</td>
</tr>
<tr>
<td></td>
<td>sntp_server= 192.168.1.9</td>
<td>sntp_mode= unicast</td>
<td>sntp_mode= multicast</td>
<td>sntp_mode= anycast</td>
</tr>
<tr>
<td>Sends</td>
<td>SNTP request to the</td>
<td>Nothing.</td>
<td>SNTP request to the</td>
<td>SNTP packet to the</td>
</tr>
<tr>
<td></td>
<td>SNTP server.</td>
<td></td>
<td>SNTP server.</td>
<td>SNTP server.</td>
</tr>
<tr>
<td>Receives</td>
<td>SNTP response from</td>
<td>SNTP data via the</td>
<td>SNTP response from</td>
<td>SNTP data from the</td>
</tr>
<tr>
<td></td>
<td>the SNTP server and</td>
<td>SNTP/NTP multicast</td>
<td>the SNTP server and</td>
<td>SNTP/NTP multicast</td>
</tr>
<tr>
<td></td>
<td>ignores responses</td>
<td>address from the local</td>
<td>ignores responses</td>
<td>address and the local</td>
</tr>
<tr>
<td></td>
<td>from other SNTP</td>
<td>network broadcast</td>
<td>from other SNTP</td>
<td>network broadcast address</td>
</tr>
<tr>
<td></td>
<td>servers.</td>
<td>address.</td>
<td>servers.</td>
<td>from any server on the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>network.</td>
</tr>
</tbody>
</table>

Table 3-8 lists the actions that take place when a valid IP address is specified in the sntp_server parameter.

**Table 3-8  Actions Based on sntp_mode When the sntp_server Parameter Is Set to an IP Address**

<table>
<thead>
<tr>
<th>sntp_server</th>
<th>sntp_mode= unicast</th>
<th>sntp_mode= multicast</th>
<th>sntp_mode= anycast</th>
<th>sntp_mode= directedbroadcast</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sends</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.1.9</td>
<td>SNTP request to the</td>
<td>SNTP packet to the</td>
<td>SNTP packet to the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNTP server.</td>
<td>local network broadcast address.</td>
<td>SNTP server.</td>
<td></td>
</tr>
<tr>
<td>Receives</td>
<td>SNTP response from</td>
<td>SNTP data via the</td>
<td>SNTP response from</td>
<td>SNTP data from the SNTP</td>
</tr>
<tr>
<td></td>
<td>the SNTP server and</td>
<td>SNTP/NTP multicast</td>
<td>the SNTP server and</td>
<td>server.</td>
</tr>
<tr>
<td></td>
<td>ignores responses</td>
<td>address from the local</td>
<td>ignores responses</td>
<td></td>
</tr>
<tr>
<td></td>
<td>from other SNTP</td>
<td>network broadcast</td>
<td>from other SNTP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>servers.</td>
<td>address.</td>
<td>servers.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 1** Using an ASCII editor, open the SIPDefault.cnf file and define or modify values for the following SNTP-specific SIP parameters as necessary:

- `sntp_mode`—(Required) Mode in which the phone listens for the SNTP server. Valid values are unicast, multicast, anycast, or directedbroadcast.
- `sntp_server`—(Required) IP address of the SNTP server from which the phone will obtain time data.

See Table 3-7 and Table 3-8 for an explanation on how these values work, depending on the `sntp_server` parameter value.
Setting the Date, Time, and Daylight Saving Time

See Table 3-7 and Table 3-8 for an explanation on how these values work, depending on the sntp_server parameter value.

• time_zone—(Required) Time zone in which the phone is located. Valid values are the time zone abbreviations shown in Table 3-9. These abbreviations are case sensitive and must be in all capital letters.

<table>
<thead>
<tr>
<th>Table 3-9</th>
<th>Time Zone Abbreviations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbreviation</td>
<td>GMT Offset</td>
</tr>
<tr>
<td>IDL</td>
<td>GMT-12:00</td>
</tr>
<tr>
<td>NT</td>
<td>GMT-11:00</td>
</tr>
<tr>
<td>AHST</td>
<td>GMT-10:00</td>
</tr>
<tr>
<td>IMT</td>
<td>GMT-09:30</td>
</tr>
<tr>
<td>YST</td>
<td>GMT-09:00</td>
</tr>
<tr>
<td>PST</td>
<td>GMT-08:00</td>
</tr>
<tr>
<td>MST</td>
<td>GMT-07:00</td>
</tr>
<tr>
<td>CST</td>
<td>GMT-06:00</td>
</tr>
<tr>
<td>EST</td>
<td>GMT-05:00</td>
</tr>
<tr>
<td>AST</td>
<td>GMT-04:00</td>
</tr>
<tr>
<td>NST</td>
<td>GMT-03:30</td>
</tr>
<tr>
<td>BST</td>
<td>GMT-03:00</td>
</tr>
<tr>
<td>AT</td>
<td>GMT-02:00</td>
</tr>
<tr>
<td>WAT</td>
<td>GMT-01:00</td>
</tr>
<tr>
<td>GMT</td>
<td>GMT 00:00</td>
</tr>
<tr>
<td>CET</td>
<td>GMT+01:00</td>
</tr>
<tr>
<td>EET</td>
<td>GMT+02:00</td>
</tr>
</tbody>
</table>
Setting the Date, Time, and Daylight Saving Time

### Step 2

To configure common DST settings, specify values for the following parameters:

- **dst_offset**—Offset from the phone’s time when DST is in effect. When DST is over, the specified offset is no longer applied to the phone’s time. Valid values are hour/minute, -hour/minute, +hour/minute, hour, -hour, and +hour.

- **dst_auto_adjust**—Whether or not DST is automatically adjusted on the phones. Valid values are 0 (disable automatic DST adjustment) or 1 (enable automatic DST adjustment). The default is 1.

- **dst_start_month**—Month in which DST starts. Valid values are January, February, March, April, May, June, July, August, September, October, November, and December or 1 through 12 with January being 1 and December being 12. When specifying the name of a month, the value is not case sensitive. In the United States, the default value is April.

- **dst_stop_month**—Month in which DST ends. Valid values are January, February, March, April, May, June, July, August, September, October, November, and December or 1 through 12 with January being 1 and December being 12. When specifying the name of a month, the value is not case sensitive. In the United States, the default value is October.

- **dst_start_time**—Time of day on which DST begins. Valid values are hour/minute (02/00) or hour (02:00). In the United States, the default value is 02:00.

---

**Table 3-9 Time Zone Abbreviations**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>GMT Offset</th>
<th>Cities</th>
<th>Time Zone Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>BT</td>
<td>GMT+03:00</td>
<td>Baghdad, Moscow</td>
<td>BT (Baghdad Time), USSR-zone2</td>
</tr>
<tr>
<td>IT</td>
<td>GMT+03:30</td>
<td>Tehran</td>
<td>IT (Iran Time)</td>
</tr>
<tr>
<td>ZP4</td>
<td>GMT+04:00</td>
<td>Abu Dhabi</td>
<td>USSR-zone3, ZP4 (GMT Plus 4 Hours)</td>
</tr>
<tr>
<td>AFG</td>
<td>GMT+04:30</td>
<td>Kabul</td>
<td>Afghanistan</td>
</tr>
<tr>
<td>ZP5</td>
<td>GMT+05:00</td>
<td>Islamabad</td>
<td>USSR-zone4, ZP5 (GMT Plus 5 Hours)</td>
</tr>
<tr>
<td>IST</td>
<td>GMT+05:30</td>
<td>Bombay, Delhi</td>
<td>IST (Indian Standard Time)</td>
</tr>
<tr>
<td>ZP6</td>
<td>GMT+06:00</td>
<td>Colombo</td>
<td>USSR-zone5, ZP6 (GMT Plus 6 Hours)</td>
</tr>
<tr>
<td>SUM</td>
<td>GMT+06:30</td>
<td>North Sumatra</td>
<td>NST (North Sumatra Time)</td>
</tr>
<tr>
<td>WAST</td>
<td>GMT+07:00</td>
<td>Bangkok, Hanoi</td>
<td>SST (South Sumatra Time), USSR-zone6, WAST (West Australian Standard Time)</td>
</tr>
<tr>
<td>HST</td>
<td>GMT+08:00</td>
<td>Beijing, Hong Kong</td>
<td>CCTV (China Coast Time), HST (Hong Kong Standard Time), USSR-zone7, WADT (West Australian Daylight Time)</td>
</tr>
<tr>
<td>JST</td>
<td>GMT+09:00</td>
<td>Tokyo, Seoul</td>
<td>JST (Japan Standard Time/Tokyo), KST (Korean Standard Time), USSR-zone8</td>
</tr>
<tr>
<td>CAST</td>
<td>GMT+09:30</td>
<td>Darwin</td>
<td>SAST (South Australian Standard Time), CAST (Central Australian Standard Time)</td>
</tr>
<tr>
<td>EAST</td>
<td>GMT+10:00</td>
<td>Brisbane, Guam</td>
<td>GST (Guam Standard Time), USSR-zone9, EAST (East Australian Standard Time)</td>
</tr>
<tr>
<td>EADT</td>
<td>GMT+11:00</td>
<td>Solomon Islands</td>
<td>USSR-zone10, EADT (East Australian Daylight Time)</td>
</tr>
<tr>
<td>NZST</td>
<td>GMT+12:00</td>
<td>Auckland</td>
<td>NZT (New Zealand Time/Auckland), NZST (New Zealand Standard Time), IDLE (International Date Line East)</td>
</tr>
</tbody>
</table>
• dst_stop_time—Time of day on which DST ends. Valid values are hour/minute (02:00) or hour (02:00). In the United States, the default value is 02:00.

**Step 3** To configure absolute DST, specify values for the following parameters, or to configure relative DST, proceed to **Step 4**:

- dst_start_day—Day of the month on which DST begins.
  Valid values are 1 through 31 for the days of the month or 0 when specifying relative DST to indicate that this field be ignored and that the value in the dst_start_day_of_week parameter be used instead.
- dst_stop_day—Day of the month on which DST ends.
  Valid values are 1 through 31 for the days of the month or 0 when specifying relative DST to indicate that this field be ignored and that the value in the dst_stop_day_of_week parameter be used instead.

**Step 4** To configure relative DST, specify values for the following parameters:

- dst_start_day_of_week—Day of the week on which DST begins.
  Valid values are Sunday or Sun, Monday or Mon, Tuesday or Tue, Wednesday or Wed, Thursday or Thu, Friday or Fri, Saturday or Sat, or Sunday or Sun or 1 through 7 with 1 being Sunday and 7 being Saturday. When specifying the name of the day, the value is not case sensitive. In the United States, the default value is Sunday.
- dst_stop_day_of_week—Day of the week on which DST ends.
  Valid values are Sunday or Sun, Monday or Mon, Tuesday or Tue, Wednesday or Wed, Thursday or Thu, Friday or Fri, Saturday or Sat, or Sunday or Sun or 1 through 7, with 1 being Sunday and 7 being Saturday. When specifying the name of the day, the value is not case sensitive. In the United States, the default value is Sunday.
- dst_start_week_of_month—Week of month on which DST begins.
  Valid values are 1 through 6 and 8, with 1 being the first week and each number thereafter being subsequent weeks and 8 specifying the last week in the month regardless of which week the last week is. In the United States, the default value is 1.
- dst_stop_week_of_month—Week of month on which DST ends.
  Valid values are 1 through 6 and 8, with 1 being the first week and each number thereafter being subsequent weeks and 8 specifying the last week in the month regardless of which week the last week is. In the United States, the default value is 8.

**Step 5** Save the file with the same filename, SIPDefault.cnf, to the root directory of your TFTP server.

The following is a sample configuration for an absolute DST configuration:

```
[3-34]
```

```
time_zone : PST
dst_offset : 01/00
dst_start_month : April
dst_start_day : 1
dst_start_time : 02/00
dst_stop_month : October
dst_stop_day : 1
dst_stop_time : 02/00
dst_stop_autoadjust : 1
```

The following is a sample configuration for a relative DST configuration:

```
time_zone : PST
dst_offset : 01/00
dst_start_month : April
dst_start_day : 0
```

---

**Cisco SIP IP Phone Administrator Guide, Release 5.0 and Release 5.1**
Erasing the Locally Defined Settings

You can erase the locally defined network and SIP settings that have been configured in the phone.

Erasing the Locally Defined Network Settings

When you erase the locally defined network settings, the values are reset to the defaults.

**Before You Begin**

- Unlock configuration mode as described in the “Unlocking Configuration Mode” section on page 3-2.
- If DHCP has been disabled on a phone, clearing the phone’s settings reenables it.
- Select the Erase Config parameter by pressing the down arrow to scroll to and highlight the parameter or by pressing the number that represents the parameter (located to the left of the parameter name on the LCD).

<table>
<thead>
<tr>
<th>Step</th>
<th>Action Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Press the settings key. The Settings menu appears.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Highlight <em>Network Configuration</em>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Press the <em>Select</em> soft key. The Network Configuration settings are displayed.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Highlight <em>Erase Configuration</em>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Press the <em>Yes</em> soft key.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Press the <em>Save</em> soft key. The phone programs the new information into Flash memory and resets.</td>
</tr>
</tbody>
</table>

Erasing the Locally Defined SIP Settings

When you erase the locally defined SIP settings, the values are reset to the defaults.

If your system has been set up to have the phones retrieve their SIP parameters using a TFTP server, you must edit the configuration file in which a parameter is defined to delete the parameter. When deleting a parameter, remove the variable in the file or change its value to a null value “” or “UNPROVISIONED”. If both the variable and its value are removed, the phone uses the setting for that variable that it has stored in Flash memory.

dst_start_day_of_week : Sunday
dst_start_week_of_month : 1
dst_start_time : 02/00
dst_stop_month : October
dst_stop_day : 0
dst_stop_day_of_week : Sunday
dst_stop_week_of_month : 8
dst_stop_time : 02/00
dst_stop_autoadjust :
Erasing the Locally Defined Settings

Note
If the telnet_level parameter is set to allow privileged commands to be executed, the entire SIP configuration can be erased. Use the \texttt{erase_protflash} command so that the phone can retrieve its configuration files.

Before You Begin
Unlock configuration mode as described in the “Unlocking Configuration Mode” section on page 3-2.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Press the settings key. The Settings menu appears.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Highlight SIP Configuration.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Press the Select soft key. The SIP Configuration settings are displayed.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Highlight the parameter for which you want to erase the setting.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Press the Edit soft key.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Press the $&lt;$ soft key to delete the current value.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Press the Validate soft key to save your change and exit the Edit panel.</td>
</tr>
<tr>
<td>Step 8</td>
<td>If modifying a line parameter, press the Back soft key to exit the Line Configuration panel.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Press the Save soft key. The phone programs the new information into Flash memory and resets.</td>
</tr>
</tbody>
</table>

Viewing the Firmware Version

To view the firmware version, perform the following steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Press the Settings key. The Settings menu appears.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Highlight Status.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Press the Select soft key. The Setting Status menu appears.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Highlight Firmware Versions.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Press the Select soft key. The Firmware Versions panel appears.</td>
</tr>
<tr>
<td></td>
<td>The following information is displayed on this panel:</td>
</tr>
<tr>
<td></td>
<td>• Application Load ID—Current software image on the phone.</td>
</tr>
<tr>
<td></td>
<td>• Boot Load ID—Bootstrap loader image version that is manufactured on the phone. This image name does not change.</td>
</tr>
<tr>
<td>Step 6</td>
<td>To exit the Firmware Versions panel, press the Exit soft key.</td>
</tr>
</tbody>
</table>
You can use one of two methods to upgrade the firmware on your Cisco SIP IP phones. You can upgrade the firmware on one phone at a time using the phone-specific configuration, or you can upgrade the firmware on a system of phones using the default configuration file.

To upgrade the firmware, you specify the image_version in the phone-specific configuration file. To upgrade the firmware on a system of phones, specify the image_version in the default configuration file and do not define the image_version in the phone-specific configuration files.

**Before You Begin**
- Ensure that the latest version of the Cisco SIP IP phone firmware has been copied from Cisco.com to the root directory of your TFTP server.

See the upgrade scenarios in Table 3-10 to determine how to upgrade.

### Table 3-10 Upgrade Scenarios

<table>
<thead>
<tr>
<th>Image Name</th>
<th>Use Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>P0S3-xx-y-zz</td>
<td>Upgrading to Release 5.0 and Release 5.1, page 3-37</td>
</tr>
<tr>
<td>P0S30202, P0S30203 and P0S3-03-y-xx</td>
<td>Upgrading from Release 2.2 or Later to Current Release, page 3-38</td>
</tr>
<tr>
<td>P0S30100, P0S30200, P0S30201, and P0S3Zxxx</td>
<td>Upgrading from Release 2.1 or Earlier to Current Release, page 3-39</td>
</tr>
<tr>
<td>P003xxxx or P003xxxxxxx (these images are loaded on the Cisco SIP IP phone when it is shipped)</td>
<td>Dual Booting from SCCP or MGCP to a SIP Release, page 3-39</td>
</tr>
<tr>
<td>P0S3-xx-y-zz</td>
<td>Dual Booting from SCCP or MGCP to a SIP Release, page 3-39</td>
</tr>
</tbody>
</table>

### Upgrading to Release 5.0 and Release 5.1

When you upgrade to Release 5.0 or Release 5.1, you will download a ZIP archive instead of a file as in earlier releases. Contained in the archive are the unsigned (.bin) and signed (.sbn) binary images. Specific information for each release is as follows:

**Release 5.0**

Cisco has added image authentication to IP phone protocols, which means that tampering with the binary image before the image is downloaded to the phone is not allowed. Any tampering with the image will cause the phone to fail the authentication process and reject the image. Once you download the Release 5.0 image, you cannot downgrade to any earlier releases.

**Release 5.1**

Release 5.1 is the second release of the signed Cisco IP phone image. Release 5.1 is compatible with Release 5.0 and later releases. Release 5.1 addresses the user interface responsiveness and voice clipping issues.
### Upgrading the Cisco SIP IP Phone Firmware

**Procedure**

**Step 1**
Unzip the ZIP archive to extract the binary images and any notes or readme text files. Read these text files for any special directions regarding the images.

**Step 2**
Using a text editor, open the configuration file and update the image version specified in the `image_version` variable. The version name in the `image_version` variable should match the version name (without the .sbn or .bin extension) of the latest firmware that you downloaded (for example, P0S3-xx-y-zz).

**Step 3**
Reset each phone.

The phone contacts the TFTP server and requests its configuration files. The phone compares the image defined in the file to the image that it has stored in Flash memory. If the phone determines that the image defined in the file differs from the image in Flash memory, it downloads the image defined in the configuration file (which is stored in the root directory on the TFTP server). Once the new image has been downloaded, the phone programs that image into Flash memory and then reboots.

**Note**
If you do not define the `image_version` parameter in the default configuration file, only phones that have an updated phone-specific configuration file with the new image version and that have been restarted use the latest firmware image. All other phones use the older version until their configuration files have been updated with the new image version.

### Upgrading from Release 2.2 or Later to Current Release

**Step 1**
Copy the new image P0S3-xx-y-zz.bin, where `xx` is the release major version, `y` is the release minor version, and `zz` is the maintenance number, from Cisco.com to the root directory of the TFTP server.

**Step 2**
Using a text editor, open the configuration file and update the image version specified in the `image_version` variable. The version name in the `image_version` variable should match the version name (without the .bin extension) of the latest firmware that you downloaded (for example, P0S3-xx-y-zz).

**Step 3**
Reset each phone.

The phone contacts the TFTP server and requests its configuration files. The phone compares the image defined in the file to the image that it has stored in Flash memory. If the phone determines that the image defined in the file differs from the image in Flash memory, it downloads the image defined in the configuration file (which is stored in the root directory on the TFTP server). Once the new image has been downloaded, the phone programs that image into Flash memory and then reboots.

**Note**
If you do not define the `image_version` parameter in the default configuration file, only phones that have an updated phone-specific configuration file with the new image version and that have been restarted use the latest firmware image. All other phones use the older version until their configuration files have been updated with the new image version.
Upgrading from Release 2.1 or Earlier to Current Release

**Step 1**  Copy the P0S30202.bin binary image from Cisco.com to the root directory of the TFTP server.

**Step 2**  If you are dual booting from a Cisco IP phone running the Skinny Client Control Protocol (SCCP) or MGCP protocol, open the OS79XX.TXT file with a text editor and change the file to include P0S30202.

**Step 3**  Open the phone configuration file with a text editor and edit the image_version variable to read P0S30202.

**Step 4**  Reset each phone.

The phone contacts the TFTP server and requests its configuration files. The phone compares the image defined in the file to the image that it has stored in Flash memory. If the phone determines that the image defined in the file differs from the image in Flash memory, it downloads the image defined in the configuration file (which is stored in the root directory on the TFTP server). Once the new image has been downloaded, the phone programs that image into Flash memory and then reboots.

**Step 5**  Copy the new image P0S3-xx-y-zz.bin, where xx is the release major version, y is the release minor version, and zz is the maintenance number, from Cisco.com to the root directory of the TFTP server.

**Step 6**  Using a text editor, open the configuration file and update the image version specified in the image_version variable. The version name in image_version variable should match the version name (without the .bin extension) of the latest firmware that you downloaded (for example, P0S3-xx-y-zz).

**Step 7**  Reset each phone.

---

Dual Booting from SCCP or MGCP to a SIP Release

**Step 1**  Copy the P0S30202.bin binary image from Cisco.com to the root directory of the TFTP server.

**Step 2**  If you are dual booting from a Cisco IP phone running the SCCP or MGCP protocol, open the OS79XX.TXT file with a text editor and change the file to include P0S30202.

**Step 3**  Copy the new image P0S3-xx-y-zz.bin, where xx is the release major version, y is the release minor version, and zz is the maintenance number, from Cisco.com to the root directory of the TFTP server.

**Step 4**  Using a text editor, open the configuration file and update the image version specified in the image_version variable. The version name in image_version variable should match the version name (without the .bin extension) of the latest firmware that you downloaded (for example, P0S3-xx-y-zz).

**Step 5**  Reset each phone.

The phone contacts the TFTP server and requests its configuration files. The phone compares the image defined in the file to the image that it has stored in Flash memory. If the phone determines that the image defined in the file differs from the image in Flash memory, it downloads the image defined in the configuration file (which is stored in the root directory on the TFTP server). Once the new image has been downloaded, the phone programs that image into Flash memory and then reboots.
Performing an Image Upgrade and Remote Reboot

With Version 2.0 and newer of the Cisco SIP IP phone, you can perform an image upgrade and remote reboot using NOTIFY messages and the syncinfo.xml file. The dialplan.xml file can also be pushed down to the phones using a NOTIFY with a check-sync Event header.

Note
To perform an image upgrade and remote reboot, a SIP proxy server and a TFTP server must exist in the phone network.

To upgrade the firmware image and perform a remote reboot, perform the following steps:

Step 1
Using an ASCII editor, open the SIPDefault.cnf file located in the root directory of your TFTP server and change the image_version parameter to the name of the latest image.

Step 2
Using an ASCII editor, open the syncinfo.xml file located in the root directory of your TFTP server and specify values for the image version and sync parameter as follows:

```xml
<IMAGE VERSION="image_version" SYNC="sync_number"/>
```

Where:
- `image_version` is the image version of the phone. The asterisk (*) can be used as a wildcard character.
- `sync_number` is the synchronization level of the phone. The default synchronization level for the phone is 1. A valid value is a character string of up to 32 characters.

Step 3
Send a NOTIFY message to the phone. In the NOTIFY message, ensure that an Event header that is equal to “check-sync” is included. The following is a sample NOTIFY message:

```plaintext
NOTIFY sip:lineX_name@ipaddress:5060 SIP/2.0
Via: SIP/2.0/UDP ipaddress:5060;branch=1
Via: SIP/2.0/UDP ipaddress
From: <sip:webadim@ipaddress>
To: <sip:lineX_name@ipaddress>
Event: check-sync
Date: Mon, 10 Jul 2000 16:28:53 -0700
Call-ID: 1349882@ipaddress
CSeq: 1300 NOTIFY
Contact: <sip:webadmin@ipaddress>
Content-Length: 0
```

After the remote reboot process is initiated on the phone via the NOTIFY message, the following actions take place:

1. If the phone is currently in an idle state, the phone waits 20 seconds and then contacts the TFTP server for the syncinfo.xml file. If the phone is not in an idle state, the phone waits until it is in an idle state for 20 seconds and then contacts the TFTP server for the syncinfo.xml file.

2. The phone reads the syncinfo.xml file and performs the following as appropriate:
   
   a. Determines whether the current image is specified. If so, the phone proceeds to Step c. If not, the phone proceeds to Step b.
   
   b. Determines whether there is a wildcard entry (*) in the image version parameter. If so, the phone proceeds to Step c. If not, the phone proceeds to Step d.
   
   c. Determines if the synchronization value is different than what is stored on the phone. If so, the phone proceeds to Step e. If not, the phone proceeds to Step d.
Performing an Image Upgrade and Remote Reboot

The phone does nothing.

The phone reboots.

The phone does nothing.

The phone reboots.

The phone reboots.

The phone performs a normal reboot process as described in the “Overview of the Initialization Process” section on page 2-1, sees the new image, and upgrades to the new image with a synchronization value of what is specified in the syncinfo.xml file.
Performing an Image Upgrade and Remote Reboot
Monitoring and Maintaining

This chapter provides information on the following:

- Using the Command-Line Interface (CLI), page 4-1
- Accessing Status Information, page 4-7

Using the Command-Line Interface (CLI)

You can use Telnet or a console to connect to your Cisco SIP IP phone and use the command-line interface (CLI) to monitor and maintain the phone. Table 4-1 shows the available CLI commands.

You will need the phone IP address to use the CLI in a Telnet session. To get the IP address of the phone, press Settings and select Network Configuration. You can then scroll down to IP Address and the address displays. The default Telnet password is “cisco.”
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Phone&gt; clear {arp</td>
<td>ethernet</td>
</tr>
<tr>
<td></td>
<td>• arp—Clears the Address Resolution Protocol (ARP) cache.</td>
</tr>
<tr>
<td></td>
<td>• ethernet—Clears the network statistics.</td>
</tr>
<tr>
<td></td>
<td>• ip—Clears the IP statistics.</td>
</tr>
<tr>
<td></td>
<td>• malloc—Clears the memory allocation table.</td>
</tr>
<tr>
<td></td>
<td>• tcp-stats—Clears the TCP statistics.</td>
</tr>
<tr>
<td>SIP Phone&gt; debug {arp</td>
<td>console-stall</td>
</tr>
<tr>
<td></td>
<td>• arp—Shows debug output for the ARP cache.</td>
</tr>
<tr>
<td></td>
<td>• console-stall—Shows debug output for the console-stall driver output mode.</td>
</tr>
<tr>
<td></td>
<td>• strlib—Shows debug output for the string library.</td>
</tr>
<tr>
<td></td>
<td>• malloc—Shows debug output for memory allocation.</td>
</tr>
<tr>
<td></td>
<td>• malloc-table—Enables the population of the memory allocation table. The table can be viewed with the show malloc-table command.</td>
</tr>
<tr>
<td></td>
<td>• sk-platform—Shows debug output for the platform.</td>
</tr>
<tr>
<td></td>
<td>• flash—Shows debug output for the Flash memory.</td>
</tr>
<tr>
<td></td>
<td>• dsp—Shows debug output for DSP accesses.</td>
</tr>
<tr>
<td></td>
<td>• vcm—Shows debug output for the voice channel manager (VCM), including tones, ringing, and volume.</td>
</tr>
<tr>
<td></td>
<td>• dtmf—Shows debug output for DTMF relay.</td>
</tr>
<tr>
<td></td>
<td>• task-socket—Shows socket task debug output.</td>
</tr>
<tr>
<td></td>
<td>• lsm—Shows debug output for the Line State Manager.</td>
</tr>
<tr>
<td></td>
<td>• fsm—Shows debug output for the Feature State Manager.</td>
</tr>
<tr>
<td></td>
<td>• auth—Shows debug output for the SIP authorization state machine.</td>
</tr>
<tr>
<td></td>
<td>• fim—Shows debug output for the Feature Interaction Manager.</td>
</tr>
<tr>
<td></td>
<td>• gsm—Shows debug output for the Global State Manager.</td>
</tr>
<tr>
<td></td>
<td>• cc—Shows debug output for call control.</td>
</tr>
<tr>
<td></td>
<td>• cc-msg—Shows debug output for the call control messages.</td>
</tr>
</tbody>
</table>
debug command keywords (continued)

- **error**—Shows general error debug output.
- **sip-task**—Shows debug output for the SIP task.
- **sip-state**—Shows debug output for the SIP state machine.
- **sip-messages**—Shows debug output for SIP messaging.
- **sip-reg-state**—Shows debug output for the SIP registration state machine.
- **dns**—Shows the DNS command-line interface (CLI) configuration; allows you to clear the cache and set servers.
- **config**—Shows output for the `config system` command.
- **sntp**—Shows debug output for Simple Network Time Protocol (SNTP).
- **sntp-packet**—Displays full SNTP packet data.
- **http**—Shows HTTP requests and responses.
- **arp-broadcast**—Shows ARP broadcast messages.
- **xml-events**—Shows XML events that are posted to the XML application chain.
- **xml-deck**—Shows XML requests for XML cards and decks.
- **xml-vars**—Shows XML content variables.
- **xml-post**—Shows XML post strings.

**Note**  Do not use the `debug all` command because it can cause the phone to become inoperable. This command is for use only by Cisco TAC personnel.

**SIP Phone> dns**

Manipulates the DNS system. The following arguments are used:

- `-p`—Prints out the DNS cache table.
- `-c`—Clears out the DNS cache table.
- `-s ip-address`—Sets the primary DNS server.
- `-b ip-address`—Sets the first backup server.

**SIP Phone> erase protflash**

Erases the protocol area of Flash memory. Forces the phone to reset its IP stack and request its configuration files again. This command can be used only if the telnet_level parameter is set to allow privileged commands to be executed.

**SIP Phone> exit**

Exits the Telnet or console session.
### Table 4-1 CLI Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SIP Phone&gt; ping ip-address number packet-size timeout</strong></td>
<td>Sends an Internet Control Message Protocol (ICMP) ping to a network address. You can use a dotted IP address or an alphanumeric address. The <code>number</code> argument specifies how many pings to send; the default value is 5. The <code>packetsize</code> argument defines the size of the packet; you can send any size packet up to 1480 bytes and the default packet size is 100. The <code>timeout</code> argument is measured in seconds and identifies how long to wait before the request times out; the default is 2.</td>
</tr>
<tr>
<td>**SIP Phone&gt; register {option value</td>
<td>line value}**</td>
</tr>
<tr>
<td><strong>SIP Phone&gt; reset</strong></td>
<td>Resets the phone line. This command can be used only if the <code>telnet_level</code> parameter is set to allow privileged commands to be executed.</td>
</tr>
<tr>
<td>**SIP Phone&gt; show {arp</td>
<td>debug</td>
</tr>
</tbody>
</table>
Using the Command-Line Interface (CLI)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show command keywords continued</strong></td>
<td>• <strong>flash</strong>—Shows Flash memory information.</td>
</tr>
<tr>
<td></td>
<td>• <strong>dspstate</strong>—Shows the DSP status, including whether the DSP is ready, the audio mode, whether keepalive pending is turned on, and the ringer state.</td>
</tr>
<tr>
<td></td>
<td>• <strong>rtp</strong>—Shows packet statistics for the RTP streams.</td>
</tr>
<tr>
<td></td>
<td>• <strong>tcp</strong>—Shows the status of TCP ports, including the state (listen or closed) and the port number.</td>
</tr>
<tr>
<td></td>
<td>• <strong>lsm</strong>—Shows the current status of the Line Manager control blocks.</td>
</tr>
<tr>
<td></td>
<td>• <strong>fsm</strong>—Shows the current status of the Feature State function control blocks.</td>
</tr>
<tr>
<td></td>
<td>• <strong>fsmdef</strong>—Shows the current status of the default Feature State Manager data control blocks.</td>
</tr>
<tr>
<td></td>
<td>• <strong>fsmcnf</strong>—Shows the current status of the Conference Feature State Manager call control blocks.</td>
</tr>
<tr>
<td></td>
<td>• <strong>fsmxfr</strong>—Shows the current status of the Transfer Feature State Manager transfer control blocks.</td>
</tr>
<tr>
<td></td>
<td>• <strong>fim</strong>—Shows the current status of the Feature Interaction Manager control blocks (interface control blocks and state control blocks).</td>
</tr>
<tr>
<td></td>
<td>• <strong>gsm</strong>—Turns on debugging for vcm, lsm, fim, fsm, and gsm.</td>
</tr>
<tr>
<td></td>
<td>• <strong>register</strong>—Shows the current registration status of SIP lines.</td>
</tr>
<tr>
<td></td>
<td>• <strong>network</strong>—Shows network information, such as phone platform, DHCP server, phone IP address and subnet mask, default gateway, address of the TFTP server, phone MAC address, domain name, and phone name.</td>
</tr>
<tr>
<td></td>
<td>• <strong>config</strong>—Shows the current Flash configuration, including network information, phone label and password, SNTP server address, DST information, time and date format, and input and output port numbers.</td>
</tr>
<tr>
<td></td>
<td>• <strong>personaldir</strong>—Displays the current contents of the personal directory. This command can be used only if the telnet_level parameter is set to allow privileged commands to be executed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>dialplan</strong>—Shows the phone dial plan.</td>
</tr>
<tr>
<td></td>
<td>• <strong>timers</strong>—Shows the current status of the platform timers.</td>
</tr>
</tbody>
</table>
Using the Command-Line Interface (CLI)

Chapter 4      Monitoring and Maintaining

SIP Phone> test {open | close | key | onhook | offhook | show | hide}

Accesses the remote call test interface, allowing you to control the phone from a remote site. To use this feature, enter the test open command. To prevent use of this feature, enter the test close command. This command can be used only if the telnet_level parameter is set to allow privileged commands to be executed.

The following commands are available:

- **test key**—When a test session is open, you can simulate key presses using the test key k1 k2 k3...k12 command, where k1 through k13 represent the following key names:
  - voldn—Volume down
  - volup—Volume up
  - headset—Headset
  - spkr—Speaker
  - mute—Mute
  - info—Info
  - msgs—Messages
  - serv—Services
  - dir—Directories
  - set—Settings
  - navup—Navigate up
  - navdn—Navigate down

  The keys 0 through 9, #, and * may be entered in continuous strings to better express typical dialing strings. A typical command would be test ky 23234.

- **test onhook**—Simulates a handset onhook event.
- **test offhook**—Simulates a handset offhook event.
- **test show**—Shows test feedback.
- **test hide**—Hides test feedback.

---

Table 4-1     CLI Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Phone&gt; test open</td>
<td>Accesses the remote call test interface, allowing you to control the phone from a remote site. To use this feature, enter the test open command. To prevent use of this feature, enter the test close command. This command can be used only if the telnet_level parameter is set to allow privileged commands to be executed.</td>
</tr>
<tr>
<td>test close</td>
<td></td>
</tr>
<tr>
<td>test key</td>
<td></td>
</tr>
<tr>
<td>test onhook</td>
<td></td>
</tr>
<tr>
<td>test offhook</td>
<td></td>
</tr>
<tr>
<td>test show</td>
<td></td>
</tr>
<tr>
<td>test hide</td>
<td></td>
</tr>
</tbody>
</table>

Table 4-1 CLI Commands (continued)
Table 4-1 CLI Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Phone&gt; <code>tty</code> {echo {on</td>
<td>off}</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP Phone&gt; <code>trc</code></td>
<td>Initiates a traceroute session from the console or from a Telnet session. Traceroute shows the route that IP datagrams follow from the SIP IP phone to the specified IP address. The arguments are as follows:</td>
</tr>
<tr>
<td><code>traceroute ip-address [ttl]</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP Phone&gt; <code>undebug</code></td>
<td>Turns off debugging.</td>
</tr>
<tr>
<td>`undebug {arp</td>
<td>console-stall</td>
</tr>
</tbody>
</table>

**Accessing Status Information**

There are several types of status information that you can access using the `settings` key. The information that you can obtain using the `settings` key can aid in system management. To access status information, select `settings` and then select `Status` from the Settings menu. From the Status menu, the following three options are available:

- **Status Messages**—Displays diagnostic messages.
- **Network Status**—Displays performance messages.

In addition to the status messages available using the Setting Status menu, you can also obtain status messages for a current call.
## Viewing Status Messages

To view status messages that you can use to diagnose network problems, perform the following steps:

1. Press the **Settings** key. The Settings menu appears.
2. Highlight **Status**.
3. Press the **Select** soft key. The Setting Status menu appears.
4. Highlight **Status Messages**.
5. Press the **Select** soft key. The Status Messages panel appears.
6. To exit the Status Messages panel, press the **Exit** soft key.

## Viewing Network Statistics

To view statistical information about the phone and network performance, perform the following steps:

1. Press the **Settings** key. The Settings menu appears.
2. Highlight **Status**.
3. Press the **Select** soft key. The Setting Status menu appears.
4. Highlight **Network Statistics**.
5. Press the **Select** soft key. The Network Statistics panel appears.

The following information is displayed on this panel:

- **Rcv**—Number of packets received by the phone; not through the switch.
- **Xmit**—Number of packets sent by the phone; not through the switch.
- **REr**—Number of packets received by the phone that contained errors.
- **BCast**—Number of broadcast packets received by the phone.
- **Phone State Message**—TCP messages indicating the state of the phone. Possible messages are:
  - **Phone Initialized**—TCP connection has not gone down since the phone was powered on.
  - **Phone Closed TCP**—TCP connection was closed by the phone.
  - **TCP Timeout**—TCP connection was closed because of a retry timeout.
  - **Error Code**—Error messages indicating unusual reasons the TCP connection was closed.
- **Elapsed Time**—Length of time (in days, hours, minutes, and seconds) since the last power cycle.
- **Port 0 Full, 100**—Indicates that the network is in a linked state and has autonegotiated a full-duplex 100-Mbps connection.
- **Port 0 Half, 100**—Indicates that the network is in a linked state and has autonegotiated a half-duplex 100-Mbps connection.
- **Port 0 Full, 10**—Indicates that the network is in a linked state and has autonegotiated a full-duplex 10-Mbps connection.
- **Port 0 Half, 10**—Indicates that the network is in a linked state and has autonegotiated a half-duplex 10-Mbps connection.
Accessing Status Information

There are several types of status information that you can access via the settings key. The information that you can obtain via the settings key can aid in system management. To access status information, select settings and then select Status from the Settings menu. From the Status menu, the following three options are available:

- **Status Messages**—Displays diagnostic messages.
- **Network Status**—Displays performance messages.
- **Firmware Version**—Displays information about the current firmware version on the phone.

In addition to the status messages available via the Setting Status menu, you can also obtain status messages for a current call.

Viewing Status Messages

To view status messages that you can use to diagnose network problems, perform the following steps:

1. Press the **Settings** key. The Settings menu appears.
2. Highlight **Status**.
3. Press the **Select** soft key. The Setting Status menu appears.
4. Highlight **Status Messages**.
5. Press the **Select** soft key. The Status Messages panel appears.
6. To exit the Status Messages panel, press the **Exit** soft key.
**Viewing Network Statistics**

To view statistical information about the phone and network performance, perform the following steps:

1. **Step 1** Press the **Settings** key. The Settings menu appears.
2. **Step 2** Highlight **Status**.
3. **Step 3** Press the **Select** soft key. The Setting Status menu appears.
4. **Step 4** Highlight **Network Statistics**.
5. **Step 5** Press the **Select** soft key. The Network Statistics panel appears.

The following information is displayed on this panel:

- **Rcv**—Number of packets received by the phone; not through the switch.
- **Xmit**—Number of packets sent by the phone; not through the switch.
- **REr**—Number of packets received by the phone that contained errors.
- **BCast**—Number of broadcast packets received by the phone.
- **Phone State Message**—TCP messages indicating the state of the phone. Possible messages are:
  - Phone Initialized—TCP connection has not gone down since the phone was powered on.
  - Phone Closed TCP—TCP connection was closed by the phone.
  - TCP Timeout—TCP connection was closed because of a retry timeout.
  - Error Code—Error messages indicating unusual reasons the TCP connection was closed.
- **Elapsed Time**—Length of time (in days, hours, minutes, and seconds) since the last power cycle.
- **Port 0 Full, 100**—Indicates that the network is in a linked state and has autonegotiated a full-duplex 100-Mbps connection.
- **Port 0 Half, 100**—Indicates that the network is in a linked state and has autonegotiated a half-duplex 100-Mbps connection.
- **Port 0 Full, 10**—Indicates that the network is in a linked state and has autonegotiated a full-duplex 10-Mbps connection.
- **Port 0 Half, 10**—Indicates that the network is in a linked state and has autonegotiated a half-duplex 10-Mbps connection.
- **Port 1 Full, 100**—Indicates that the network is in a linked state and has autonegotiated a full-duplex 100-Mbps connection.
- **Port 1 Half, 100**—Indicates that the network is in a linked state and has autonegotiated a half-duplex 100-Mbps connection.
- **Port 1 Full, 10**—Indicates that the network is in a linked state and has autonegotiated a full-duplex 10-Mbps connection.
- **Port 1 Half, 10**—Indicates that the network is in a linked state and has autonegotiated a half-duplex 10-Mbps connection.

6. **Step 6** To exit the Network Statistics panel, press the **Exit** soft key.

---

**Note**

To reset the values displayed on the Network Statistics panel, power the phone off and on.
This appendix describes how the Cisco SIP IP phone complies with the IETF definition of SIP as described in RFC 3261. It has compliance information on the following:

- SIP Functions, page A-1
- SIP Methods, page A-2
- SIP Responses, page A-2
- SIP Header Fields, page A-7
- SIP Session Description Protocol Usage, page A-8
- Transport Layer Protocols, page A-9
- SIP Security Authentication, page A-9
- SIP DTMF Digit Transport, page A-9

### SIP Functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>User agent client (UAC)</td>
<td>Yes</td>
</tr>
<tr>
<td>User agent server (UAS)</td>
<td>Yes</td>
</tr>
<tr>
<td>Proxy server</td>
<td>Third-party only</td>
</tr>
<tr>
<td>Redirect server</td>
<td>Third-party only</td>
</tr>
</tbody>
</table>
SIP Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Supported?</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVITE</td>
<td>Yes</td>
<td>The Cisco SIP IP phone supports mid-call changes such as putting a call on hold as signaled by a new INVITE that contains an existing call ID.</td>
</tr>
<tr>
<td>ACK</td>
<td>Yes</td>
<td>None.</td>
</tr>
<tr>
<td>OPTIONS</td>
<td>Response only</td>
<td></td>
</tr>
<tr>
<td>BYE</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CANCEL</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>REGISTER</td>
<td>Yes</td>
<td>The Cisco SIP IP phone supports both user and device registration.</td>
</tr>
<tr>
<td>REFER</td>
<td>Yes</td>
<td>None.</td>
</tr>
<tr>
<td>NOTIFY</td>
<td>Yes</td>
<td>Used for REFER and remote reboot.</td>
</tr>
</tbody>
</table>

SIP Responses

Release 4.0 of the Cisco SIP IP phone supports the following SIP responses:

- **1xx Response**—Information Responses, page A-2
- **2xx Response**—Successful Responses, page A-3
- **3xx Response**—Redirection Responses, page A-3
- **4xx Response**—Request Failure Responses, page A-4
- **5xx Response**—Server Failure Responses, page A-6
- **6xx Response**—Global Responses, page A-7

**1xx Response— Information Responses**

<table>
<thead>
<tr>
<th>1xx Response</th>
<th>Supported?</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 Trying</td>
<td>Yes</td>
<td>The Cisco SIP IP phone generates this response for an incoming INVITE. Upon receiving this response, the phone waits for a 180 Ringing, 183 Session progress, or 200 OK response.</td>
</tr>
<tr>
<td>180 Ringing</td>
<td>Yes</td>
<td>None</td>
</tr>
</tbody>
</table>
### 1xx Response

<table>
<thead>
<tr>
<th>Response</th>
<th>Supported?</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>181 Call Is Being Forwarded</td>
<td>See comments</td>
<td>The Cisco SIP IP phone does not generate these responses; however, the phone does receive them. The phone processes these responses the same way that it processes the 100 Trying response.</td>
</tr>
<tr>
<td>182 Queued</td>
<td></td>
<td></td>
</tr>
<tr>
<td>183 Session Progress</td>
<td></td>
<td>The SIP IP phone does not generate this message. Upon receiving this response, the phone provides early media cut-through and then waits for a 200 OK response.</td>
</tr>
</tbody>
</table>

### 2xx Response—Successful Responses

<table>
<thead>
<tr>
<th>Response</th>
<th>Supported?</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 OK</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>202 Accepted</td>
<td>Yes</td>
<td>None</td>
</tr>
</tbody>
</table>

### 3xx Response—Redirection Responses

<table>
<thead>
<tr>
<th>Response</th>
<th>Supported?</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>300 Multiple Choices</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>301 Moved Permanently</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>302 Moved Temporarily</td>
<td>Yes</td>
<td>The Cisco SIP IP phone does not generate this response at this time. Upon receiving this response, the phone sends an INVITE containing the contact information received in the 302 Moved temporarily response.</td>
</tr>
<tr>
<td>305 Use Proxy</td>
<td>Yes</td>
<td>The phone does not generate these responses. The gateway contacts the new address in the Contact header field.</td>
</tr>
<tr>
<td>380 Alternate Service</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
# 4xx Response—Request Failure Responses

<table>
<thead>
<tr>
<th>4xx Response</th>
<th>Supported?</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>400 Bad Request</td>
<td>Yes</td>
<td>The phone generates a 400 Bad Request response for an erroneous request. For an incoming response, the phone initiates a graceful call disconnect (during which the caller hears a busy or fast busy tone) before clearing the call request.</td>
</tr>
<tr>
<td>401 Unauthorized</td>
<td>Yes</td>
<td>This response is received only in this release. If a 401 Unauthorized response is received during registration, the phone accepts the response and sends a new request that contains the user’s authentication information in the format of the HTTP digest as modified by RFC 3261.</td>
</tr>
<tr>
<td>402 Payment Required</td>
<td>Yes</td>
<td>The phone does not generate the 402 Payment Required response.</td>
</tr>
<tr>
<td>403 Forbidden</td>
<td>Yes</td>
<td>This response is received only in this release. If the phone receives a 403 Forbidden response, it notifies the user of the response. This response indicates that the SIP server has the request but will not provide service.</td>
</tr>
<tr>
<td>404 Not Found</td>
<td>Yes</td>
<td>The Cisco SIP IP phone generates this response if it is unable to locate the callee. Upon receiving this response, the phone notifies the user.</td>
</tr>
<tr>
<td>405 Method Not Allowed</td>
<td>See comments</td>
<td>This response is received only in this release. If the phone receives a 405 Method Not Allowed response, it notifies the user of the response.</td>
</tr>
<tr>
<td>406 Not Acceptable</td>
<td>See comments</td>
<td>The SIP phone does not generate a 406 Not Acceptable response. For an incoming response, the gateway initiates a graceful call disconnect (during which the caller hears a busy or fast busy tone) before clearing the call request.</td>
</tr>
<tr>
<td>407 Proxy Authentication Required</td>
<td>See comments</td>
<td>This response is received only in this release. The 407 Proxy Authentication Required response indicates that the phone must first authenticate itself with the proxy server. If received by the phone, the phone may repeat the INVITE request with a suitable Proxy-Authorization field. This field should contain the authentication information of the user agent for the next outbound proxy or gateway.</td>
</tr>
<tr>
<td>4xx Response</td>
<td>Supported?</td>
<td>Comments</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>408 Request Timeout</td>
<td>See comments</td>
<td>The SIP phone does not generate a 408 Request Timeout response. For an incoming response, the gateway initiates a graceful call disconnect (during which the caller hears a busy or fast busy tone) before clearing the call request.</td>
</tr>
<tr>
<td>409 Conflict</td>
<td>See comments</td>
<td>This response is received only by the phone in this release. The 409 Conflict response indicates that the INVITE request could not be processed because of a conflict with the current state of the resource. If this response is received, the user is notified.</td>
</tr>
<tr>
<td>410 Gone</td>
<td>See comments</td>
<td>This response is received by the phone only in this release. The 410 Gone response indicates that a resource is no longer available at the server and no forwarding address is known.</td>
</tr>
<tr>
<td>411 Length Required</td>
<td>See comments</td>
<td>This response is received only by the phone in this release. If a retry after header field is contained in this response, then the user can attempt the call once again in the retry time provided.</td>
</tr>
<tr>
<td>413 Request—URL Too Long</td>
<td>See comments</td>
<td>This response is received only by the phone in this release. The user is notified if this response is received. If the phone does not understand the protocol extension specified in the Require field, the 420 Bad Extension response is generated.</td>
</tr>
<tr>
<td>414 Bad Extension</td>
<td>See comments</td>
<td>This response is received only by the phone in this release. The user is notified if this response is received. If the phone does not understand the protocol extension specified in the Require field, the 420 Bad Extension response is generated.</td>
</tr>
<tr>
<td>480 Temporarily Unavailable</td>
<td>See comments</td>
<td>The phone sends this response if Do Not Disturb (DND) is active on the phone.</td>
</tr>
</tbody>
</table>
## 4xx Response—Server Failure Responses

<table>
<thead>
<tr>
<th>4xx Response</th>
<th>Supported?</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>481 Call Leg/Transaction Does Not Exist</td>
<td>See comments</td>
<td>This response is received only by the phone in this release. The user is notified if this response is received.</td>
</tr>
<tr>
<td>482 Loop Detected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>483 Too Many Hops</td>
<td></td>
<td></td>
</tr>
<tr>
<td>484 Address Incomplete</td>
<td></td>
<td></td>
</tr>
<tr>
<td>485 Ambiguous</td>
<td>See comments</td>
<td>This response is received only by the phone in this release. If a new contact is received, the phone might reinitiate the call.</td>
</tr>
<tr>
<td>486 Busy Here</td>
<td>Yes</td>
<td>The Cisco SIP IP phone generates this response if the called party is off-hook and the call cannot be presented as a call-waiting call. Upon receiving this response, the phone notifies the user and generates a busy tone.</td>
</tr>
<tr>
<td>487 Request Canceled</td>
<td>Yes</td>
<td>This response indicates that the initial request is terminated with a BYE or CANCEL request.</td>
</tr>
<tr>
<td>488 Not Acceptable</td>
<td>Yes</td>
<td>The Cisco SIP IP phone receives and generates this response.</td>
</tr>
</tbody>
</table>

## 5xx Response—Server Failure Responses

<table>
<thead>
<tr>
<th>5xx Response</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>500 Internal Server Error</td>
<td>The Cisco SIP IP phone does not generate these 5xx responses. For an incoming response, the SIP IP phone initiates a graceful call disconnect.</td>
</tr>
<tr>
<td>501 Not Implemented</td>
<td></td>
</tr>
<tr>
<td>502 Bad Gateway</td>
<td></td>
</tr>
<tr>
<td>503 Service Unavailable</td>
<td></td>
</tr>
<tr>
<td>504 Gateway Timeout</td>
<td></td>
</tr>
<tr>
<td>505 Version Not Supported</td>
<td></td>
</tr>
</tbody>
</table>
6xx Response—Global Responses

<table>
<thead>
<tr>
<th>6xx Response</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>600 Busy Everywhere</td>
<td>The Cisco SIP IP phone does not generate these 6xx responses. For an incoming response, the SIP IP phone initiates a graceful call disconnect.</td>
</tr>
<tr>
<td>603 Decline</td>
<td></td>
</tr>
<tr>
<td>604 Does Not Exist Anywhere</td>
<td></td>
</tr>
<tr>
<td>606 Not Acceptable</td>
<td></td>
</tr>
</tbody>
</table>

SIP Header Fields

<table>
<thead>
<tr>
<th>Header Field</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>Yes</td>
</tr>
<tr>
<td>Accept-Encoding</td>
<td>Yes</td>
</tr>
<tr>
<td>Accept-Language</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow</td>
<td>Yes</td>
</tr>
<tr>
<td>Also</td>
<td>Yes</td>
</tr>
<tr>
<td>Authorization</td>
<td>Yes</td>
</tr>
<tr>
<td>Call-ID</td>
<td>Yes</td>
</tr>
<tr>
<td>Contact</td>
<td>Yes</td>
</tr>
<tr>
<td>Content-Encoding</td>
<td>Yes</td>
</tr>
<tr>
<td>Content-Length</td>
<td>Yes</td>
</tr>
<tr>
<td>Content-Type</td>
<td>Yes</td>
</tr>
<tr>
<td>Cseq</td>
<td>Yes</td>
</tr>
<tr>
<td>Date</td>
<td>Yes</td>
</tr>
<tr>
<td>Encryption</td>
<td>No</td>
</tr>
<tr>
<td>Expires</td>
<td>Yes</td>
</tr>
<tr>
<td>From</td>
<td>Yes</td>
</tr>
<tr>
<td>Hide</td>
<td>No</td>
</tr>
<tr>
<td>Max-Forwards</td>
<td>Yes</td>
</tr>
<tr>
<td>Organization</td>
<td>No</td>
</tr>
<tr>
<td>Priority</td>
<td>No</td>
</tr>
<tr>
<td>Proxy-Authenticate</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## SIP Session Description Protocol Usage

<table>
<thead>
<tr>
<th>Header Field</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy-Authorization</td>
<td>Yes</td>
</tr>
<tr>
<td>Proxy-Require</td>
<td>Yes</td>
</tr>
<tr>
<td>Record-Route</td>
<td>Yes</td>
</tr>
<tr>
<td>Referred-By</td>
<td>Yes</td>
</tr>
<tr>
<td>Referred-To</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote-Party-ID</td>
<td>Yes</td>
</tr>
<tr>
<td>Replaces</td>
<td>Yes</td>
</tr>
<tr>
<td>Requested-By</td>
<td>Yes</td>
</tr>
<tr>
<td>Require</td>
<td>Yes</td>
</tr>
<tr>
<td>Response-Key</td>
<td>No</td>
</tr>
<tr>
<td>Retry-After</td>
<td>Yes</td>
</tr>
<tr>
<td>Route</td>
<td>Yes</td>
</tr>
<tr>
<td>Server</td>
<td>Yes</td>
</tr>
<tr>
<td>Subject</td>
<td>No</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Yes</td>
</tr>
<tr>
<td>To</td>
<td>Yes</td>
</tr>
<tr>
<td>Unsupported</td>
<td>Yes</td>
</tr>
<tr>
<td>User-Agent</td>
<td>Yes</td>
</tr>
<tr>
<td>Via</td>
<td>Yes</td>
</tr>
<tr>
<td>Warning</td>
<td>Yes</td>
</tr>
<tr>
<td>WWW-Authenticate</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### SDP Headers

<table>
<thead>
<tr>
<th>SDP Headers</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>v—Protocol version</td>
<td>Yes</td>
</tr>
<tr>
<td>o—Owner or creator and session identifier</td>
<td>Yes</td>
</tr>
<tr>
<td>s—Session name</td>
<td>Yes</td>
</tr>
<tr>
<td>t—Time description</td>
<td>Yes</td>
</tr>
<tr>
<td>c—Connection information</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Transport Layer Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unicast UDP</td>
<td>Yes</td>
</tr>
<tr>
<td>Multicast UDP</td>
<td>No</td>
</tr>
<tr>
<td>TCP</td>
<td>No</td>
</tr>
</tbody>
</table>

### SIP Security Authentication

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>No</td>
</tr>
<tr>
<td>Digest</td>
<td>Yes</td>
</tr>
<tr>
<td>Proxy</td>
<td>No</td>
</tr>
<tr>
<td>PGP</td>
<td>No</td>
</tr>
</tbody>
</table>

### SIP DNS Records Usage

<table>
<thead>
<tr>
<th>DNS Resource Record Type</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type A</td>
<td>Yes</td>
</tr>
<tr>
<td>Type SRV</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### SIP DTMF Digit Transport

<table>
<thead>
<tr>
<th>Transport Type</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2833</td>
<td>Yes</td>
</tr>
<tr>
<td>In-band tones</td>
<td>Yes</td>
</tr>
</tbody>
</table>
SIP Call Flows

This appendix includes the following sections:

- Call Flow Scenarios for Successful Calls, page B-1
- Call Flow Scenarios for Failed Calls, page B-52

SIP uses the following request methods:

- INVITE—Indicates that a user or service is being invited to participate in a call session.
- ACK—Confirms that the client has received a final response to an INVITE request.
- BYE—Terminates a call and can be sent by either the caller or the callee.
- CANCEL— Cancels any pending searches but does not terminate a call that has already been accepted.
- OPTIONS—Queries the capabilities of servers.
- REGISTER—Registers the address listed in the To header field with a SIP server.
- REFER—Indicates that the user (recipient) should contact a third party for use in transferring parties.
- NOTIFY—Notifies the user of the status of a transfer using REFER. Also used for remote reset.

The following types of responses are used by SIP and generated by the Cisco SIP gateway:

- SIP 1xx—Informational Responses
- SIP 2xx—Successful Responses
- SIP 3xx—Redirection Responses
- SIP 4xx—Client Failure Responses
- SIP 5xx—Server Failure Responses
- SIP 6xx—Global Failure Responses

Call Flow Scenarios for Successful Calls

This section describes successful call flows scenarios, which are as follows:

- Gateway to Cisco SIP IP Phone, page B-2
- Cisco SIP IP Phone to Cisco SIP IP Phone, page B-7
Gateway to Cisco SIP IP Phone

The following scenarios describe and illustrate successful calls in a gateway to a Cisco SIP IP phone:

- Call Setup and Disconnect, page B-2
- Call Setup and Hold, page B-4
- Call to a Gateway Acting as an Emergency Proxy from a Cisco SIP IP Phone, page B-6

Call Setup and Disconnect

Figure B-1 illustrates a successful phone call setup and disconnect. In this scenario, the two end users are User A and User B. User A is located at PBX A. PBX A is connected to Gateway 1 (SIP Gateway) via a T1/E1. User B is located at a Cisco SIP IP phone. Gateway 1 is connected to the Cisco SIP IP phone over an IP network.

The call flow is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B hangs up.

Figure B-1  Successful Setup and Disconnect
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Setup—PBX A to Gateway 1</td>
<td>Call Setup is initiated between PBX A and Gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.</td>
</tr>
</tbody>
</table>
| 2.   | INVITE—Gateway 1 to Cisco SIP IP phone | Gateway 1 maps the SIP URL phone number to a dial peer. The dial peer includes the IP address and the port number of the SIP-enabled entity to contact. Gateway 1 sends a SIP INVITE request to the address it receives as the dial peer, which, in this scenario, is the Cisco SIP IP phone. In the INVITE request:  
  - The IP address of the Cisco SIP IP phone is inserted in the Request-URI field.  
  - PBX A is identified as the call session initiator in the From field.  
  - A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.  
  - The transaction number within a single call leg is identified in the CSeq field.  
  - The media capability User A is ready to receive is specified.  
  - The port on which the Gateway is prepared to receive the RTP data is specified. |
| 3.   | Call Proceeding—Gateway 1 to PBX A | Gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request. |
| 4.   | 100 Trying—Cisco SIP IP phone to Gateway 1 | The Cisco SIP IP phone sends a SIP 100 Trying response to Gateway 1. The 100 Trying response indicates that the INVITE request has been received by the Cisco SIP IP phone. |
| 5.   | 180 Ringing—Cisco SIP IP phone to Gateway 1 | The Cisco SIP IP phone sends a SIP 180 Ringing response to Gateway 1. The 180 Ringing response indicates that the user is being alerted. |
| 6.   | Alerting—Gateway 1 to PBX A | Gateway 1 sends an Alert message to User A. The Alert message indicates that Gateway 1 has received a 180 Ringing response from the Cisco SIP IP phone. User A hears the ringback tone that indicates that User B is being alerted. |
| 7.   | 200 OK—Cisco SIP IP phone to Gateway 1 | The Cisco SIP IP phone sends a SIP 200 OK response to Gateway 1. The 200 OK response notifies Gateway 1 that the connection has been made. |
| 8.   | Connect—Gateway 1 to PBX A | Gateway 1 sends a Connect message to PBX A. The Connect message notifies PBX A that the connection has been made. |
| 9.   | Connect ACK—PBX A to Gateway 1 | PBX A acknowledges Gateway 1’s Connect message. |
| 10.  | ACK—Gateway 1 to Cisco SIP IP phone | Gateway 1 sends a SIP ACK to the Cisco SIP IP phone. The ACK confirms that Gateway 1 has received the 200 OK response. The call session is now active. |
| 11.  | BYE—Cisco SIP IP phone to Gateway 1 | User B terminates the call session at his Cisco SIP IP phone and the phone sends a SIP BYE request to Gateway 1. The BYE request indicates that User B wants to release the call. |
| 12.  | Disconnect—Gateway 1 to PBX A | Gateway 1 sends a Disconnect message to PBX A. |
| 13.  | Release—PBX A to Gateway 1 | PBX A sends a Release message to Gateway 1. |
Call Flow Scenarios for Successful Calls

**Figure B-2** illustrates a successful phone call setup and call hold. In this scenario, the two end users are User A and User B. User A is located at PBX A, PBX A is connected to gateway 1 (SIP Gateway) via a T1/E1. User B is located at a Cisco SIP IP phone. Gateway 1 is connected to the Cisco SIP IP phone over an IP network.

The call flow is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B puts User A on hold.
4. User B takes User A off hold.

**Figure B-2  Successful Call Setup and Hold**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.</td>
<td>200 OK—Gateway 1 to Cisco SIP IP phone</td>
<td>Gateway 1 sends a SIP 200 OK response to the Cisco SIP IP phone. The 200 OK response notifies the phone that Gateway 1 has received the BYE request.</td>
</tr>
<tr>
<td>15.</td>
<td>Release Complete—Gateway 1 to PBX A</td>
<td>Gateway 1 sends a Release Complete message to PBX A and the call session is terminated.</td>
</tr>
</tbody>
</table>
### Call Flow Scenarios for Successful Calls

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Setup—PBX A to Gateway 1</td>
<td>Call setup is initiated between PBX A and Gateway 1. The call setup includes the standard transactions that take place as User A attempts to call User B.</td>
</tr>
</tbody>
</table>
| 2.   | INVITE—Gateway 1 to Cisco SIP IP phone | Gateway 1 maps the SIP URL phone number to a dial peer. The dial peer includes the IP address and the port number of the SIP enabled entity to contact. Gateway 1 sends a SIP INVITE request to the address it receives as the dial peer, which, in this scenario, is the Cisco SIP IP phone.  
In the INVITE request:  
- The IP address of the Cisco SIP IP phone is inserted in the Request-URI field.  
- PBX A is identified as the call session initiator in the From field.  
- A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.  
- The transaction number within a single call leg is identified in the CSeq field.  
- The media capability User A is ready to receive is specified.  
- The port on which the gateway is prepared to receive the RTP data is specified. |
| 3.   | Call Proceeding—Gateway 1 to PBX A | Gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request. |
| 4.   | 100 Trying—Cisco SIP IP phone to Gateway 1 | The Cisco SIP IP phone sends a SIP 100 Trying response to Gateway 1. The 100 Trying response indicates that the INVITE request has been received by the Cisco SIP IP phone. |
| 5.   | 180 Ringing—Cisco SIP IP phone to Gateway 1 | The Cisco SIP IP phone sends a SIP 180 Ringing response to Gateway 1. The 180 Ringing response indicates that the user is being alerted. |
| 6.   | Alerting—Gateway 1 to PBX A | Gateway 1 sends an Alert message to User A. The Alert message indicates that Gateway 1 has received a 180 Ringing response from the Cisco SIP IP phone. User A hears the ringback tone that indicates that User B is being alerted. |
| 7.   | 200 OK—Cisco SIP IP phone to Gateway 1 | The Cisco SIP IP phone sends a SIP 200 OK response to Gateway 1. The 200 OK response notifies Gateway 1 that the connection has been made. |
| 8.   | Connect—Gateway 1 to PBX A | Gateway 1 sends a Connect message to PBX A. The Connect message notifies PBX A that the connection has been made. |
| 9.   | ACK—Gateway 1 to Cisco SIP IP phone | Gateway 1 sends a SIP ACK to the Cisco SIP IP phone. The ACK confirms that User A has received the 200 OK response. The call session is now active. |
| 10.  | Connect ACK—PBX A to Gateway 1 | PBX A acknowledges Gateway 1’s Connect message. |
| 11.  | INVITE—Cisco SIP IP phone to Gateway 1 | User B puts User A on hold. The Cisco SIP IP phone sends a SIP INVITE request to Gateway 1. |
| 12.  | 200 OK—Gateway 1 to Cisco SIP IP phone | Gateway 1 sends a SIP 200 OK response to the Cisco SIP IP phone. The 200 OK response notifies the Cisco SIP IP phone that the INVITE was successfully processed. |
| 13.  | ACK—Cisco SIP IP phone to Gateway 1 | The Cisco SIP IP phone sends a SIP ACK to Gateway 1. The ACK confirms that the Cisco SIP IP phone has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent. |
Call to a Gateway Acting as an Emergency Proxy from a Cisco SIP IP Phone

Figure B-3 illustrates a successful call from a Cisco SIP IP phone to a gateway acting as an emergency proxy.

14. INVITE—Cisco SIP IP phone to Gateway 1
   User B takes User A off hold. The Cisco SIP IP phone sends a SIP INVITE request to Gateway 1.

15. 200 OK—Gateway 1 to Cisco SIP IP phone
   Gateway 1 sends a SIP 200 OK response to the Cisco SIP IP phone. The 200 OK response notifies the Cisco SIP IP phone that the INVITE was successfully processed.

16. ACK—Cisco SIP IP phone to Gateway 1
   The Cisco SIP IP phone sends a SIP ACK to Gateway 1. The ACK confirms that the Cisco SIP IP phone has received the 200 OK response. The call session is now active.

---

Figure B-3  Successful Call from Cisco SIP IP Phone to Gateway (Emergency Proxy)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>INVITE—Cisco SIP IP phone to</td>
<td>User B takes User A off hold. The Cisco SIP IP phone sends a SIP INVITE</td>
</tr>
<tr>
<td></td>
<td>Gateway 1</td>
<td>request to Gateway 1.</td>
</tr>
<tr>
<td>15</td>
<td>200 OK—Gateway 1 to Cisco SIP</td>
<td>Gateway 1 sends a SIP 200 OK response to the Cisco SIP IP phone. The 200</td>
</tr>
<tr>
<td></td>
<td>IP phone</td>
<td>OK response notifies the Cisco SIP IP phone that the INVITE was successfully</td>
</tr>
<tr>
<td></td>
<td></td>
<td>processed.</td>
</tr>
<tr>
<td>16</td>
<td>ACK—Cisco SIP IP phone to</td>
<td>The Cisco SIP IP phone sends a SIP ACK to Gateway 1. The ACK confirms that</td>
</tr>
<tr>
<td></td>
<td>Gateway 1</td>
<td>the Cisco SIP IP phone has received the 200 OK response. The call session</td>
</tr>
<tr>
<td></td>
<td></td>
<td>is now active.</td>
</tr>
</tbody>
</table>

Step Action Description

1. INVITE (Matches dial template for emergency route)
2. Setup
3. Call Proceeding
4. 100 Trying
5. Alerting
6. 180 Ringing
7. Connect
8. 200 OK
9. ACK
10. Connect ACK
11. BYE
12. Disconnect
13. Release
14. 200 OK
15. Release Complete

2-way voice path
Call Flow Scenarios for Successful Calls

### Call Flow Scenarios for Successful Calls

#### Cisco SIP IP Phone to Cisco SIP IP Phone

The following sections describe and illustrate successful calls from Cisco SIP IP phone to Cisco SIP IP phone:

- **Simple Call Hold, page B-8**
- **Call Hold with Consultation, page B-10**
- **Call Waiting, page B-14**
- **Call Transfer Without Consultation, page B-18**
- **Call Transfer Without Consultation Using Failover, page B-22**
- **Call Transfer with Consultation, page B-25**
- **Call Transfer with Consultation Using Failover, page B-30**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>INVITE—Cisco SIP IP phone to gateway (emergency proxy)</td>
<td>Cisco SIP IP phone tries to connect to the gateway (emergency proxy) by sending out the INVITE message. The dial template for the emergency route is matched.</td>
</tr>
<tr>
<td>2.</td>
<td>Setup—Gateway to PBX</td>
<td>Call setup is initiated between the gateway and PBX. The call setup includes the standard transactions that take place as User A attempts to call User B.</td>
</tr>
<tr>
<td>3.</td>
<td>Call Proceeding—PBX to gateway</td>
<td>PBX sends a Call Proceeding message to gateway to acknowledge the Call Setup request.</td>
</tr>
<tr>
<td>4.</td>
<td>100 Trying—Gateway to Cisco SIP IP phone (User A)</td>
<td>Gateway sends a SIP 100 Trying response to User A. The 100 Trying response indicates that the INVITE request has been received by the gateway.</td>
</tr>
<tr>
<td>5.</td>
<td>Alerting—PBX to gateway</td>
<td>PBX sends an Alert message to the gateway. The Alert message indicates that the PBX has received a 100 Trying Ringing response from the gateway.</td>
</tr>
<tr>
<td>6.</td>
<td>180 Ringing—Gateway to Cisco SIP IP phone (User A)</td>
<td>The gateway sends a SIP 180 Ringing response to User A. The 180 Ringing response indicates that the gateway is being alerted.</td>
</tr>
<tr>
<td>7.</td>
<td>Connect—PBX to gateway</td>
<td>PBX sends a Connect message to gateway. The Connect message notifies the gateway that the connection has been made.</td>
</tr>
<tr>
<td>8.</td>
<td>200 OK—Gateway to Cisco SIP IP phone (User A)</td>
<td>Gateway sends a SIP 200 OK response to the User A. The 200 OK response notifies User A that the connection has been made.</td>
</tr>
<tr>
<td>9.</td>
<td>ACK—Cisco SIP IP phone (User A) to gateway</td>
<td>User A sends a SIP ACK to the gateway. The ACK confirms that User A has received the 200 OK response. The call session is now active.</td>
</tr>
<tr>
<td>10.</td>
<td>Connect ACK—Gateway to PBX</td>
<td>Gateway acknowledges PBX’s Connect message.</td>
</tr>
<tr>
<td>11.</td>
<td>BYE—Cisco SIP IP phone (User A) to gateway</td>
<td>User A terminates the call session and sends a SIP BYE request to gateway. The BYE request indicates that User A wants to release the call.</td>
</tr>
<tr>
<td>12.</td>
<td>Disconnect—Gateway to PBX</td>
<td>Gateway sends a Disconnect message to PBX.</td>
</tr>
<tr>
<td>13.</td>
<td>Release—PBX to gateway</td>
<td>PBX sends a Release message to the gateway.</td>
</tr>
<tr>
<td>14.</td>
<td>200 OK—Gateway to Cisco SIP IP phone (User A)</td>
<td>Gateway sends a SIP 200 OK response to User A. The 200 OK response notifies User A that the gateway has received the BYE request.</td>
</tr>
<tr>
<td>15.</td>
<td>Release Complete—Gateway to PBX</td>
<td>Gateway sends a Release Complete message to the PBX and the call session is terminated.</td>
</tr>
</tbody>
</table>
Simple Call Hold

Figure B-4 illustrates a successful call between Cisco SIP IP phones in which one of the participants places the other on hold and then returns to the call. In this call flow scenario, the two end users are User A and User B. User A and User B are both using Cisco SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B places User A on hold.
4. User B takes User A off hold.
5. The call continues.

**Figure B-4 Simple Call Hold**

<table>
<thead>
<tr>
<th>Step</th>
<th>Message/Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User A sends INVITE to User B</td>
</tr>
<tr>
<td>2</td>
<td>User B sends 180 RINGING to User A</td>
</tr>
<tr>
<td>3</td>
<td>User B sends 200 OK to User A</td>
</tr>
<tr>
<td>4</td>
<td>User A sends ACK to User B</td>
</tr>
<tr>
<td>5</td>
<td>User B sends INVITE with c=IN IP4 0.0.0.0 to User A</td>
</tr>
<tr>
<td>6</td>
<td>User A sends 200 OK to User B</td>
</tr>
<tr>
<td>7</td>
<td>User B sends ACK to User A</td>
</tr>
<tr>
<td>8</td>
<td>User B sends INVITE with c=IN IP4 IP-User B to User A</td>
</tr>
<tr>
<td>9</td>
<td>User A sends 200 OK to User B</td>
</tr>
<tr>
<td>10</td>
<td>User B sends ACK to User A</td>
</tr>
</tbody>
</table>

- User A is taken off hold. The RTP channel between A and B is reestablished.
- User A is on hold. The RTP channel between A and B is torn down.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B</td>
<td>Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session. &lt;br&gt;<strong>In the INVITE request:</strong>&lt;br&gt;• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an e-mail address (<em>user@host</em>, where <em>user</em> is the telephone number and <em>host</em> is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as “INVITE sip:<a href="mailto:555-0002@companyb.com">555-0002@companyb.com</a>; user=phone.” The “user=phone” parameter distinguishes that the Request-URI address is a telephone number rather than a username.&lt;br&gt;• Cisco SIP IP phone A is identified as the call session initiator in the From field.&lt;br&gt;• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.&lt;br&gt;• The transaction number within a single call leg is identified in the CSeq field.&lt;br&gt;• The media capability User A is ready to receive is specified.</td>
</tr>
<tr>
<td>2.</td>
<td>180 Ringing—Cisco SIP IP phone B to Cisco SIP IP phone A</td>
<td>Cisco SIP IP phone B sends a SIP 180 Ringing response to Cisco SIP IP phone A.</td>
</tr>
<tr>
<td>3.</td>
<td>200 OK—Cisco SIP IP phone B to Cisco SIP IP phone A</td>
<td>Cisco SIP IP phone B sends a SIP 200 OK response to Cisco SIP IP phone A. The 200 OK response notifies Cisco SIP IP phone A that the connection has been made. &lt;br&gt;<strong>If Cisco SIP IP phone B supports the media capability advertised in the INVITE message sent by Cisco SIP IP phone A, it advertises the intersection of its own and Cisco SIP IP phone A’s media capability in the 200 OK response. If Cisco SIP IP phone B does not support the media capability advertised by Cisco SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field.</strong></td>
</tr>
<tr>
<td>4.</td>
<td>ACK—Cisco SIP IP phone A to Cisco SIP IP phone B</td>
<td>Cisco SIP IP phone A sends a SIP ACK to Cisco SIP IP phone B. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone B. &lt;br&gt;The ACK might contain a message body with the final session description to be used by Cisco SIP IP phone B. If the message body of the ACK is empty, Cisco SIP IP phone B uses the session description in the INVITE request.</td>
</tr>
<tr>
<td>5.</td>
<td>INVITE—Cisco SIP IP phone B to Cisco SIP IP phone A</td>
<td>Cisco SIP IP phone B sends a mid-call INVITE to Cisco SIP IP phone A with new Session Description Protocol (SDP) session parameters (IP address), which are used to place the call on hold. &lt;br&gt;<strong>Call-ID=1</strong>&lt;br&gt;<strong>SDP:</strong> c=IN IP4 0.0.0.0 &lt;br&gt;The c= SDP field of the SIP INVITE contains an 0.0.0.0. This places the call in hold.</td>
</tr>
</tbody>
</table>

A two-way RTP channel is established between Cisco SIP IP phone A and Cisco SIP IP phone B.
Call Flow Scenarios for Successful Calls

Call Hold with Consultation

Figure B-5 illustrates a successful call between Cisco SIP IP phones in which one of the participants places the other on hold, calls a third party (consultation), and then returns to the original call. In this call flow scenario, the end users are User A, User B, and User C. They are all using Cisco SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B places User A on hold.
4. User B calls User C.
5. User B disconnects from User C.
6. User B takes User A off hold.
7. The original call continues.
Figure B-5  Call Hold with Consultation

1. INVITE B
2. 180 Ringing
3. 200 OK
4. ACK

A is put on hold. The RTP channel between A and B is torn down.

5. INVITE (c=IN IP4 0.0.0.0)
6. 200 OK
7. ACK

2-way RTP channel

14. INVITE (c=IN IP4 IP-User B)
15. 200 OK
16. ACK

A is taken off hold. The RTP channel between A and B is reestablished.

8. INVITE C
9. 180 Ringing
10. 200 OK
11. ACK
12. BYE
13. 200 OK

B is disconnected from C.

SIP IP Phone User A
IP Network
SIP IP Phone User B
SIP IP Phone User C

IP Network
SIP IP Phone User A
IP Network
SIP IP Phone User B
SIP IP Phone User C

14. INVITE (c=IN IP4 IP-User B)
15. 200 OK
16. ACK

A is taken off hold. The RTP channel between A and B is reestablished.
## Call Flow Scenarios for Successful Calls

### Step 1
**Action:** INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B

Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.

*In the INVITE request:*

- The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an e-mail address (user@host, where user is the telephone number and host is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as “INVITE sip:555-0002@companyb.com; user=phone.” The “user=phone” parameter distinguishes that the Request-URI address is a telephone number rather than a username.
- Cisco SIP IP phone A is identified as the call session initiator in the From field.
- A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
- The transaction number within a single call leg is identified in the CSeq field.
- The media capability User A is ready to receive is specified.

### Step 2
**Action:** 180 Ringing—Cisco SIP IP phone B to Cisco SIP IP phone A

Cisco SIP IP phone B sends a SIP 180 Ringing response to Cisco SIP IP phone A.

### Step 3
**Action:** 200 OK—Cisco SIP IP phone B to Cisco SIP IP phone A

Cisco SIP IP phone B sends a SIP 200 OK response to Cisco SIP IP phone A. The 200 OK response notifies Cisco SIP IP phone A that the connection has been made.

If Cisco SIP IP phone B supports the media capability advertised in the INVITE message sent by Cisco SIP IP phone A, it advertises the intersection of its own and Cisco SIP IP phone A's media capability in the 200 OK response. If Cisco SIP IP phone B does not support the media capability advertised by Cisco SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field.

### Step 4
**Action:** ACK—Cisco SIP IP phone A to Cisco SIP IP phone B

Cisco SIP IP phone A sends a SIP ACK to Cisco SIP IP phone B. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone B.

The ACK might contain a message body with the final session description to be used by Cisco SIP IP phone B. If the message body of the ACK is empty, Cisco SIP IP phone B uses the session description in the INVITE request.

A two-way RTP channel is established between Cisco SIP IP phone A and Cisco SIP IP phone B.

### Step 5
**Action:** INVITE—Cisco SIP IP phone B to Cisco SIP IP phone A

Cisco SIP IP phone B sends a mid-call INVITE to Cisco SIP IP phone A with new SDP session parameters (IP address), which are used to place the call on hold.

| Call_ID=1  
| SDP: c=IN IP4 0.0.0.0 |

The c= SDP field of the SIP INVITE contains 0.0.0.0. This places the call in hold.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>200 OK—Cisco SIP IP phone A to Cisco SIP IP phone B</td>
<td>Cisco SIP IP phone A sends a SIP 200 OK response to Cisco SIP IP phone B.</td>
</tr>
<tr>
<td>7.</td>
<td>ACK—Cisco SIP IP phone B to Cisco SIP IP phone A</td>
<td>Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone A. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone A.</td>
</tr>
<tr>
<td>8.</td>
<td>INVITE—Cisco SIP IP phone B to Cisco SIP IP phone C</td>
<td>Cisco SIP IP phone B sends a SIP INVITE request to Cisco SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session.</td>
</tr>
<tr>
<td>9.</td>
<td>180 Ringing—Cisco SIP IP phone C to Cisco SIP IP phone B</td>
<td>Cisco SIP IP phone C sends a SIP 180 Ringing response to Cisco SIP IP phone B.</td>
</tr>
<tr>
<td>10.</td>
<td>200 OK—Cisco SIP IP phone C to Cisco SIP IP phone B</td>
<td>Cisco SIP IP phone C sends a SIP 200 OK response to Cisco SIP IP phone B. The 200 OK response notifies Cisco SIP IP phone B that the connection has been made. If Cisco SIP IP phone B supports the media capability advertised in the INVITE message sent by Cisco SIP IP phone A, it advertises the intersection of its own and Cisco SIP IP phone A's media capability in the 200 OK response. If Cisco SIP IP phone B does not support the media capability advertised by Cisco SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field.</td>
</tr>
<tr>
<td>11.</td>
<td>ACK—Cisco SIP IP phone B to Cisco SIP IP phone C</td>
<td>Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone C. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone C. The ACK might contain a message body with the final session description to be used by Cisco SIP IP phone C. If the message body of the ACK is empty, Cisco SIP IP phone C uses the session description in the INVITE request.</td>
</tr>
<tr>
<td>12.</td>
<td>BYE—Cisco SIP IP phone B to Cisco SIP IP phone C</td>
<td>The call continues and then User B hangs up. Cisco SIP IP phone B sends a SIP BYE request to Cisco SIP IP phone C. The BYE request indicates that User B wants to release the call.</td>
</tr>
<tr>
<td>13.</td>
<td>200 OK—Cisco SIP IP phone C to Cisco SIP IP phone B</td>
<td>Cisco SIP IP phone C sends a SIP 200 OK message to Cisco SIP IP phone B. The 200 OK response notifies Cisco SIP IP phone B that the BYE request has been received. The call session between User A and User B is now terminated.</td>
</tr>
<tr>
<td>14.</td>
<td>INVITE—Cisco SIP IP phone B to Cisco SIP IP phone A</td>
<td>Cisco SIP IP phone B sends a mid-call INVITE to Cisco SIP IP phone A with the same call ID as the previous INVITE and new SDP session parameters (IP address), which are used to reestablish the call.</td>
</tr>
<tr>
<td>15.</td>
<td>200 OK—Cisco SIP IP phone A to Cisco SIP IP phone B</td>
<td>Cisco SIP IP phone A sends a SIP 200 OK response to Cisco SIP IP phone B.</td>
</tr>
</tbody>
</table>

The RTP channel between Cisco SIP IP phone A and Cisco SIP IP phone B is torn down.

The RTP channel between Cisco SIP IP phone B and Cisco SIP IP phone C is torn down.

To reestablish the call between phone A and phone B, the IP address of phone B is inserted into the c= SDP field.
Call Flow Scenarios for Successful Calls

Call Waiting

Figure B-6 illustrates a successful call between Cisco SIP IP phones in which two parties are in a call, one of the participants receives a call from a third party, and then returns to the original call. In this call flow scenario, the end users are User A, User B, and User C. They are all using Cisco SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User C calls User B.
4. User B accepts the call from User C.
5. User B switches back to User A.
6. User B hangs up, ending the call with User A.
7. User B is notified of the remaining call with User C.
8. User B answers the notification and continues the call with User C.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.</td>
<td>ACK—Cisco SIP IP phone B to Cisco SIP IP phone A</td>
<td>Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone A. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone A. A two-way RTP channel is reestablished between Cisco SIP IP phone A and Cisco SIP IP phone B.</td>
</tr>
</tbody>
</table>
Figure B-6  Call Waiting

1. INVITE B
2. 180 Ringing
3. 200 OK
4. ACK
5. INVITE C
6. 180 Ringing

2-way RTP channel

7. INVITE (c=IN IP4 0.0.0.0)
8. 200 OK
10. 200 OK
12. INVITE (c=IN IP4 0.0.0.0)
13. 200 OK
14. ACK

A is put on hold. The RTP channel between A and B is torn down.

15. INVITE (c=IN IP4 IP-User B)
16. 200 OK
17. ACK
18. INVITE (c=IN IP4 IP-User B)
19. 200 OK
20. INVITE (c=IN IP4 IP-User B)
21. 200 OK
22. ACK

C is taken off hold. The RTP channel between B and C is reestablished.

B is on hold. The RTP channel between B and C is torn down.

A is taken off hold. The RTP channel between A and B is reestablished.
## Call Flow Scenarios for Successful Calls

### Step 1: INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B

Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.

In the INVITE request:

- The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an e-mail address (user@host, where user is the telephone number and host is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as “INVITE sip:555-0002@companyb.com; user=phone.” The “user=phone” parameter distinguishes that the Request-URI address is a telephone number rather than a username.
- Cisco SIP IP phone A is identified as the call session initiator in the From field.
- A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
- The transaction number within a single call leg is identified in the CSeq field.
- The media capability User A is ready to receive is specified.

### Step 2: 180 Ringing—Cisco SIP IP phone B to Cisco SIP IP phone A

Cisco SIP IP phone B sends a SIP 180 Ringing response to Cisco SIP IP phone A.

### Step 3: 200 OK—Cisco SIP IP phone B to Cisco SIP IP phone A

Cisco SIP IP phone B sends a SIP 200 OK response to Cisco SIP IP phone A. The 200 OK response notifies Cisco SIP IP phone A that the connection has been made.

If Cisco SIP IP phone B supports the media capability advertised in the INVITE message sent by Cisco SIP IP phone A, it advertises the intersection of its own and Cisco SIP IP phone A’s media capability in the 200 OK response. If Cisco SIP IP phone B does not support the media capability advertised by Cisco SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field.

### Step 4: ACK—Cisco SIP IP phone A to Cisco SIP IP phone B

Cisco SIP IP phone A sends a SIP ACK to Cisco SIP IP phone B. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone B.

The ACK might contain a message body with the final session description to be used by Cisco SIP IP phone B. If the message body of the ACK is empty, Cisco SIP IP phone B uses the session description in the INVITE request.

A two-way RTP channel is established between Cisco SIP IP phone A and Cisco SIP IP phone B.

### Step 5: INVITE—Cisco SIP IP phone C to Cisco SIP IP phone B

Cisco SIP IP phone C sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.

### Step 6: 180 Ringing—Cisco SIP IP phone B to Cisco SIP IP phone C

Cisco SIP IP phone B sends a SIP 180 Ringing response to Cisco SIP IP phone C.

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request:  
- The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an e-mail address (user@host, where user is the telephone number and host is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as “INVITE sip:555-0002@companyb.com; user=phone.” The “user=phone” parameter distinguishes that the Request-URI address is a telephone number rather than a username.  
- Cisco SIP IP phone A is identified as the call session initiator in the From field.  
- A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.  
- The transaction number within a single call leg is identified in the CSeq field.  
- The media capability User A is ready to receive is specified. |
| 2.   | 180 Ringing—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a SIP 180 Ringing response to Cisco SIP IP phone A. |
| 3.   | 200 OK—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a SIP 200 OK response to Cisco SIP IP phone A. The 200 OK response notifies Cisco SIP IP phone A that the connection has been made. If Cisco SIP IP phone B supports the media capability advertised in the INVITE message sent by Cisco SIP IP phone A, it advertises the intersection of its own and Cisco SIP IP phone A’s media capability in the 200 OK response. If Cisco SIP IP phone B does not support the media capability advertised by Cisco SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field. |
| 4.   | ACK—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP ACK to Cisco SIP IP phone B. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone B. The ACK might contain a message body with the final session description to be used by Cisco SIP IP phone B. If the message body of the ACK is empty, Cisco SIP IP phone B uses the session description in the INVITE request. A two-way RTP channel is established between Cisco SIP IP phone A and Cisco SIP IP phone B. |
| 5.   | INVITE—Cisco SIP IP phone C to Cisco SIP IP phone B | Cisco SIP IP phone C sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session. |
| 6.   | 180 Ringing—Cisco SIP IP phone B to Cisco SIP IP phone C | Cisco SIP IP phone B sends a SIP 180 Ringing response to Cisco SIP IP phone C. |
### Call Flow Scenarios for Successful Calls

#### Call Flow Scenarios for Successful Calls

**7.** **INVITE**—Cisco SIP IP phone B to Cisco SIP IP phone A

Cisco SIP IP phone B sends a mid-call INVITE to Cisco SIP IP phone A with new SDP session parameters (IP address), which are used to place the call on hold.

- **Call_ID=1**
- **SDP: c=IN IP4 0.0.0.0**

The c= SDP field of the SIP INVITE contains 0.0.0.0. This places the call in hold.

**8.** **200 OK**—Cisco SIP IP phone A to Cisco SIP IP phone B

Cisco SIP IP phone A sends a SIP 200 OK response to Cisco SIP IP phone B.

**9.** **ACK**—Cisco SIP IP phone B to Cisco SIP IP phone A

Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone A. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone A.

The RTP channel between Cisco SIP IP phone A and Cisco SIP IP phone B is torn down.

**10.** **200 OK**—Cisco SIP IP phone B to Cisco SIP IP phone C

Cisco SIP IP phone B sends a SIP 200 OK response to Cisco SIP IP phone C. The 200 OK response notifies Cisco SIP IP phone C that the connection has been made.

**11.** **ACK**—Cisco SIP IP phone C to Cisco SIP IP phone B

Cisco SIP IP phone C sends a SIP ACK to Cisco SIP IP phone B. The ACK confirms that Cisco SIP IP phone C has received the 200 OK response from Cisco SIP IP phone B.

The ACK might contain a message body with the final session description to be used by Cisco SIP IP phone B. If the message body of the ACK is empty, Cisco SIP IP phone B uses the session description in the INVITE request.

The two-way RTP channel is established between Cisco SIP IP phone B and Cisco SIP IP phone C.

**12.** **INVITE**—Cisco SIP IP phone B to Cisco SIP IP phone C

Cisco SIP IP phone B sends a mid-call INVITE to Cisco SIP IP phone C with new SDP session parameters (IP address), which are used to place the call on hold.

- **Call_ID=2**
- **SDP: c=IN IP4 0.0.0.0**

To establish the call between phone B and phone C, the IP address of phone B is inserted into the c= SDP field.

**13.** **200 OK**—Cisco SIP IP phone C to Cisco SIP IP phone B

Cisco SIP IP phone C sends a SIP 200 OK response to Cisco SIP IP phone B.

**14.** **ACK**—Cisco SIP IP phone B to Cisco SIP IP phone C

Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone C. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone C.

The RTP channel between Cisco SIP IP phone B and Cisco SIP IP phone C is torn down.

**15.** **INVITE**—Cisco SIP IP phone B to Cisco SIP IP phone A

Cisco SIP IP phone B sends a mid-call INVITE to Cisco SIP IP phone A with the same call ID as the previous INVITE (sent to Cisco SIP IP phone A) and new SDP session parameters (IP address), which are used to reestablish the call.

- **Call_ID=1**
- **SDP: c=IN IP4 10.10.10.0**

**16.** **200 OK**—Cisco SIP IP phone A to Cisco SIP IP phone B

Cisco SIP IP phone A sends a SIP 200 OK response to Cisco SIP IP phone B.
### Call Flow Scenarios for Successful Calls

#### Call Transfer Without Consultation

*Figure B-7* illustrates a successful call between Cisco SIP IP phones in which two parties are in a call and then one of the participants transfers the call to a third party without first contacting the third party. This is called a blind or unattended transfer. In this call flow scenario, the end users are User A, User B, and User C. They are all using Cisco SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B transfers the call to User C.

### Call Flow Scenarios for Successful Calls

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.</td>
<td>ACK—Cisco SIP IP phone B to Cisco SIP IP phone A</td>
<td>Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone A. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone A.</td>
</tr>
<tr>
<td>18.</td>
<td>BYE—Cisco SIP IP phone B to Cisco SIP IP phone A</td>
<td>The call continues and then User B hangs up. Cisco SIP IP phone B sends a SIP BYE request to Cisco SIP IP phone A. The BYE request indicates that User B wants to release the call.</td>
</tr>
<tr>
<td>19.</td>
<td>200 OK—Cisco SIP IP phone A to Cisco SIP IP phone B</td>
<td>Cisco SIP IP phone A sends a SIP 200 OK message to Cisco SIP IP phone B. The 200 OK response notifies Cisco SIP IP phone B that the BYE request has been received. The call session between User A and User B is now terminated.</td>
</tr>
</tbody>
</table>
| 20.  | INVITE—Cisco SIP IP phone B to Cisco SIP IP phone C | Cisco SIP IP phone B sends a mid-call INVITE to Cisco SIP IP phone C with the same call ID as the previous INVITE (sent to Cisco SIP IP phone C) and new SDP session parameters (IP address), which are used to reestablish the call.  
   Call_ID=2  
   SDP: c=IN IP4 10.10.10.0 |
| 21.  | 200 OK—Cisco SIP IP phone C to Cisco SIP IP phone B | Cisco SIP IP phone C sends a SIP 200 OK response to Cisco SIP IP phone B. |
| 22.  | ACK—Cisco SIP IP phone B to Cisco SIP IP phone C | Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone C. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone A. |

The RTP channel between Cisco SIP IP phone A and Cisco SIP IP phone B is torn down.

### Call Transfer Without Consultation

A two-way RTP channel is reestablished between Cisco SIP IP phone B and Cisco SIP IP phone C.
**Figure B-7 Call Transfer without Consultation**

1. INVITE
2. 100 TRYING
3. 180 RINGING
4. 200 OK
5. ACK

User B presses blind transfer.

6. INVITE (c=0.0.0.0)
7. 200 OK
8. ACK

User B dials user C.

9. REFER (Refer-To: C, Referred-By: B)
10. 202 ACCEPTED
11. BYE
12. 200 OK
13. INVITE (Referred-By: B)
14. 100 TRYING
15. 180 RINGING
16. 200 OK
17. ACK
18. NOTIFY (Event: Refer)
19. 200 OK

2-way voice path

User B presses blind transfer.

6. INVITE (c=0.0.0.0)
7. 200 OK
8. ACK

User B dials user C.

9. REFER (Refer-To: C, Referred-By: B)
10. 202 ACCEPTED
11. BYE
12. 200 OK
13. INVITE (Referred-By: B)
14. 100 TRYING
15. 180 RINGING
16. 200 OK
17. ACK
18. NOTIFY (Event: Refer)
19. 200 OK

2-way voice path
## Call Flow Scenarios for Successful Calls

### Step 1: INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B

Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.

In the INVITE request:

- The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an e-mail address (`user@host`, where `user` is the telephone number and `host` is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as “INVITE sip:555-0002@companyb.com; user=phone.” The “user=phone” parameter distinguishes that the Request-URI address is a telephone number rather than a username.
- Cisco SIP IP phone A is identified as the call session initiator in the From field.
- A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
- The transaction number within a single call leg is identified in the CSeq field.
- The media capability User A is ready to receive is specified.

### Step 2: 100 Trying—Cisco SIP IP phone B to Cisco SIP IP phone A

The Cisco SIP IP phone B sends a SIP 100 Trying response to Cisco SIP IP phone A. The 100 Trying response indicates that the INVITE request has been received by Cisco SIP IP phone B.

### Step 3: 180 Ringing—Cisco SIP IP phone B to Cisco SIP IP phone A

Cisco SIP IP phone B sends a SIP 180 Ringing response to Cisco SIP IP phone A.

### Step 4: 200 OK—Cisco SIP IP phone B to Cisco SIP IP phone A

Cisco SIP IP phone B sends a SIP 200 OK response to Cisco SIP IP phone A. The 200 OK response notifies Cisco SIP IP phone A that the connection has been made.

If Cisco SIP IP phone B supports the media capability advertised in the INVITE message sent by Cisco SIP IP phone A, it advertises the intersection of its own and Cisco SIP IP phone A’s media capability in the 200 OK response. If Cisco SIP IP phone B does not support the media capability advertised by Cisco SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field.

### Step 5: ACK—Cisco SIP IP phone A to Cisco SIP IP phone B

Cisco SIP IP phone A sends a SIP ACK to Cisco SIP IP phone B. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone B.

The ACK might contain a message body with the final session description to be used by Cisco SIP IP phone B. If the message body of the ACK is empty, Cisco SIP IP phone B uses the session description in the INVITE request.

A two-way RTP channel is established between Cisco SIP IP phone A and Cisco SIP IP phone B. User B then selects the option to blind transfer the call to User C.
6. **INVITE**—Cisco SIP IP phone B to Cisco SIP IP phone A

Cisco SIP IP phone B sends a mid-call INVITE to Cisco SIP IP phone A with new SDP session parameters (IP address), which are used to place the call on hold.

- **Call_ID=1**
- **SDP:** c=IN IP4 0.0.0.0

The c= SDP field of the SIP INVITE contains an 0.0.0.0. This places the call in hold.

7. **200 OK**—Cisco SIP IP phone A to Cisco SIP IP phone B

Cisco SIP IP phone A sends a SIP 200 OK response to Cisco SIP IP phone B.

8. **ACK**—Cisco SIP IP phone B to Cisco SIP IP phone A

Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone A. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone A.

User B dials User C.

9. **REFER**—Cisco SIP IP phone B to Cisco SIP IP phone A

Cisco SIP IP phone B sends a REFER message to Cisco SIP IP phone A. The REFER message contains the following information:

- **Refer-To:** C
- **Referred-By:** B

The REFER message indicates that Cisco SIP IP phone A should send an INVITE request to Cisco SIP IP phone C.

10. **202 ACCEPTED**—Cisco SIP IP phone A to Cisco SIP IP phone B

Cisco SIP IP phone A sends a SIP 202 ACCEPTED message to Cisco SIP IP phone B. The 202 ACCEPTED confirms that the REFER message has been received.

11. **BYE**—Cisco SIP IP phone B to Cisco SIP IP phone A

Cisco SIP IP phone B sends a BYE message to Cisco SIP IP phone A. This message indicates that Cisco SIP IP phone B will be disconnecting from the call.

12. **200 OK**—Cisco SIP IP phone A to Cisco SIP IP phone B

Cisco SIP IP phone A sends a SIP 200 OK response to Cisco SIP IP phone B. The 200 OK response notifies Cisco SIP IP phone B that the BYE message was received.

13. **INVITE**—Cisco SIP IP phone A to Cisco SIP IP phone C

Because of the REFER message from Cisco SIP IP phone B, Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session. The INVITE request contains the following information:

- **Referred-By:** B

This message indicates that the INVITE was referred by Cisco SIP IP phone B.

14. **100 Trying**—Cisco SIP IP phone C to Cisco SIP IP phone A

The Cisco SIP IP phone C sends a SIP 100 Trying response to Cisco SIP IP phone A. The 100 Trying response indicates that the INVITE request has been received by Cisco SIP IP phone C.

15. **180 Ringing**—Cisco SIP IP phone C to Cisco SIP IP phone A

Cisco SIP IP phone C sends a SIP 180 Ringing response to Cisco SIP IP phone A. The 180 Ringing response notifies Cisco SIP IP phone A that the connection has been made.

16. **200 OK**—Cisco SIP IP phone C to Cisco SIP IP phone A

Cisco SIP IP phone C sends a SIP 200 OK response to Cisco SIP IP phone A. The 200 OK response notifies Cisco SIP IP phone A that the connection has been made.

17. **ACK**—Cisco SIP IP phone A to Cisco SIP IP phone C

Cisco SIP IP phone A sends a SIP ACK to Cisco SIP IP phone C. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone C.
Call Transfer Without Consultation Using Failover

Figure B-7 illustrates a successful call between Cisco SIP IP phones in which two parties are in a call and then one of the participants transfers the call to a third party without first contacting the third party. This is called a blind or unattended transfer. In this call flow scenario, the end users are User A, User B, and User C. They are all using Cisco SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B transfers the call to User C.

A two-way RTP channel is established between Cisco SIP IP phone A and Cisco SIP IP phone C.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.  
   In the INVITE request:  
   - The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an e-mail address (user@host, where user is the telephone number and host is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as “INVITE sip:555-0002@companyb.com; user=phone.” The “user=phone” parameter distinguishes that the Request-URI address is a telephone number rather than a username.  
   - Cisco SIP IP phone A is identified as the call session initiator in the From field.  
   - A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.  
   - The transaction number within a single call leg is identified in the CSeq field.  
   - The media capability User A is ready to receive is specified. |
| 2.   | 100 Trying—Cisco SIP IP phone B to Cisco SIP IP phone A | The Cisco SIP IP phone B sends a SIP 100 Trying response to Cisco SIP IP phone A. The 100 Trying response indicates that the INVITE request has been received by Cisco SIP IP phone B. |
| 3.   | 180 Ringing—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a SIP 180 Ringing response to Cisco SIP IP phone A. |
| 4.   | 200 OK—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a SIP 200 OK response to Cisco SIP IP phone A. The 200 OK response notifies Cisco SIP IP phone A that the connection has been made.  
   If Cisco SIP IP phone B supports the media capability advertised in the INVITE message sent by Cisco SIP IP phone A, it advertises the intersection of its own and Cisco SIP IP phone A’s media capability in the 200 OK response. If Cisco SIP IP phone B does not support the media capability advertised by Cisco SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field. |
| 5.   | ACK—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP ACK to Cisco SIP IP phone B. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone B.  
   The ACK might contain a message body with the final session description to be used by Cisco SIP IP phone B. If the message body of the ACK is empty, Cisco SIP IP phone B uses the session description in the INVITE request.  
   A two-way RTP channel is established between Cisco SIP IP phone A and Cisco SIP IP phone B.  
   User B then selects the option to blind transfer the call to User C. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 6.   | INVITE—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a mid-call INVITE to Cisco SIP IP phone A with new SDP session parameters (IP address), which are used to place the call on hold.  
\[
\text{Call_ID}=1  
\text{SDP: c=IN IP4 0.0.0.0}  
\]  
The c= SDP field of the SIP INVITE contains an 0.0.0.0. This places the call in hold. |
| 7.   | 200 OK—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP 200 OK response to Cisco SIP IP phone B. |
| 8.   | ACK—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone A. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone A. |
| 9.   | REFER—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a REFER message to Cisco SIP IP phone A. The REFER message contains the following information:  
- Refer-To: C  
- Referred-By: B  
The REFER message indicates that Cisco SIP IP phone A should send an INVITE request to Cisco SIP IP phone C. |
| 10.  | 501 Not Implemented—Cisco SIP IP Phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a 501 Not Implemented message to Cisco SIP IP phone B. This message indicates that the REFER message is not supported and that Cisco SIP IP phone B should failover to Bye/Also. |
| 11.  | BYE—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a BYE message to Cisco SIP IP phone A. The BYE message includes the following information:  
- Also: C  
The message indicates that the 501 Not Implemented message was received in response to a REFER message. |
| 12.  | 200 OK—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP 200 OK response to Cisco SIP IP phone B. The 200 OK response notifies Cisco SIP IP phone B that the BYE message was received. |
| 13.  | INVITE—Cisco SIP IP phone A to Cisco SIP IP phone C | Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session. The INVITE request contains the following information:  
- Requested-By: B  
This message indicates that the INVITE was requested by Cisco SIP IP phone B. |
| 14.  | 100 Trying—Cisco SIP IP phone C to Cisco SIP IP phone A | The Cisco SIP IP phone C sends a SIP 100 Trying response to Cisco SIP IP phone A. The 100 Trying response indicates that the INVITE request has been received by Cisco SIP IP phone C. |
| 15.  | 180 Ringing—Cisco SIP IP phone C to Cisco SIP IP phone A | Cisco SIP IP phone C sends a SIP 180 Ringing response to Cisco SIP IP phone A. |
| 16.  | 200 OK—Cisco SIP IP phone C to Cisco SIP IP phone A | Cisco SIP IP phone C sends a SIP 200 OK response to Cisco SIP IP phone A. The 200 OK response notifies Cisco SIP IP phone A that the connection has been made. |
Call Transfer with Consultation

Figure B-9 illustrates a successful call between Cisco SIP IP phones in which two parties are in a call, one of the participants contacts a third party, and then that participant transfers the call to the third party. This is called an attended transfer. In this call flow scenario, the end users are User A, User B, and User C. They are all using Cisco SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B calls User C, and User C consents to take the call.
4. User B transfers the call to User C.
5. User B disconnects with User C.
6. User C and User A connect to each other.

A two-way RTP channel is established between Cisco SIP IP phone A and Cisco SIP IP phone C.
Call Flow Scenarios for Successful Calls

Figure B-9 Call Transfer with Consultation

1. INVITE

2. 100 TRYING

3. 180 RINGING

4. 200 OK

5. ACK

6. INVITE (c=0.0.0.0)

7. 200 OK

8. ACK

9. INVITE C

10. 100 TRYING

11. 180 RINGING

12. 200 OK

13. ACK

14. INVITE (c=0.0.0.0)

15. 200 OK

16. ACK

17. REFER (Refer-To: C, Replaces: B, Referred-By: B)

User B presses transfer.

18. 202 ACCEPTED

19. INVITE (Referred by: B, Replaces: B)

20. 200 OK

21. ACK

22. BYE

23. 200 OK

24. NOTIFY (Event: Refer)

25. 200 OK

26. BYE

27. 200 OK

28. 200 OK

User B presses transfer.

2-way voice path

2-way voice path

2-way voice path

2-way voice path

SIP IP Phone User A

SIP IP Phone User B

SIP IP Phone User C
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.  

In the INVITE request:

- The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an e-mail address (user@host, where user is the telephone number and host is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as “INVITE sip:555-0002@companyb.com; user=phone.” The “user=phone” parameter distinguishes that the Request-URI address is a telephone number rather than a username.
- Cisco SIP IP phone A is identified as the call session initiator in the From field.
- A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
- The transaction number within a single call leg is identified in the CSeq field.
- The media capability User A is ready to receive is specified. |
| 2.   | 100 Trying—Cisco SIP IP phone B to Cisco SIP IP phone A | The Cisco SIP IP phone B sends a SIP 100 Trying response to Cisco SIP IP phone A. The 100 Trying response indicates that the INVITE request has been received by Cisco SIP IP phone B. |
| 3.   | 180 Ringing—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a SIP 180 Ringing response to Cisco SIP IP phone A. |
| 4.   | 200 OK—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a SIP 200 OK response to Cisco SIP IP phone A. The 200 OK response notifies Cisco SIP IP phone A that the connection has been made. 

If Cisco SIP IP phone B supports the media capability advertised in the INVITE message sent by Cisco SIP IP phone A, it advertises the intersection of its own and Cisco SIP IP phone A’s media capability in the 200 OK response. If Cisco SIP IP phone B does not support the media capability advertised by Cisco SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field. |
| 5.   | ACK—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP ACK to Cisco SIP IP phone B. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone B. 

The ACK might contain a message body with the final session description to be used by Cisco SIP IP phone B. If the message body of the ACK is empty, Cisco SIP IP phone B uses the session description in the INVITE request. |
| 6.   | INVITE—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a mid-call INVITE to Cisco SIP IP phone A with new SDP session parameters (IP address), which are used to place the call on hold.  

Call_ID=1  
SDP: c=IN IP4 0.0.0.0 |

A two-way RTP channel is established between Cisco SIP IP phone A and Cisco SIP IP phone B. User B then selects the option to transfer the call to User C.
## Call Flow Scenarios for Successful Calls

### 7. 200 OK—Cisco SIP IP phone A to Cisco SIP IP phone B
Cisco SIP IP phone A sends a SIP 200 OK response to Cisco SIP IP phone B.

### 8. ACK—Cisco SIP IP phone B to Cisco SIP IP phone A
Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone A. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone A.

User B dials User C.

### 9. INVITE—Cisco SIP IP phone B to Cisco SIP IP phone C
Cisco SIP IP phone B sends a SIP INVITE request to Cisco SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session.

### 10. 100 Trying—Cisco SIP IP phone C to Cisco SIP IP phone B
The Cisco SIP IP phone C sends a SIP 100 Trying response to Cisco SIP IP phone B. The 100 Trying response indicates that the INVITE request has been received by Cisco SIP IP phone C.

### 11. 180 Ringing—Cisco SIP IP phone C to Cisco SIP IP phone B
Cisco SIP IP phone C sends a SIP 180 Ringing response to Cisco SIP IP phone B.

### 12. 200 OK—Cisco SIP IP phone C to Cisco SIP IP phone B
Cisco SIP IP phone C sends a SIP 200 OK response to Cisco SIP IP phone B. The 200 OK response notifies Cisco SIP IP phone B that the connection has been made.

The Cisco SIP IP phone C sends a SIP 100 Trying response to Cisco SIP IP phone B. The 100 Trying response indicates that the INVITE request has been received by Cisco SIP IP phone C.

### 13. ACK—Cisco SIP IP phone B to Cisco SIP IP phone C
Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone C. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone C.

The ACK might contain a message body with the final session description to be used by Cisco SIP IP phone C. If the message body of the ACK is empty, Cisco SIP IP phone C uses the session description in the INVITE request.

A two-way RTP channel is established between Cisco SIP IP phone B and Cisco SIP IP phone C.

User B then selects the option to transfer the call to User C.

### 14. INVITE—Cisco SIP IP phone B to Cisco SIP IP phone A
Cisco SIP IP phone B sends a mid-call INVITE to Cisco SIP IP phone A with new SDP session parameters (IP address), which are used to place the call on hold.

Call_ID=1
SDP: c=IN IP4 0.0.0.0

The c= SDP field of the SIP INVITE contains an 0.0.0.0. This places the call in hold.

### 15. 200 OK—Cisco SIP IP phone A to Cisco SIP IP phone B
Cisco SIP IP phone A sends a SIP 200 OK response to Cisco SIP IP phone B.

### 16. ACK—Cisco SIP IP phone B to Cisco SIP IP phone C
Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone C. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone C.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 17.  | REFER—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a REFER message to Cisco SIP IP phone A. The REFER message contains the following information:  
  - Refer-To: C  
  - Replaces: B  
  - Referred-By: B  
  The REFER message indicates that the user (recipient) should contact a third party for use in transferring parties. |
| 18.  | 202 ACCEPTED—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP 202 ACCEPTED message to Cisco SIP IP phone B. The 202 ACCEPTED confirms that the REFER message has been received. |
| 19.  | INVITE—Cisco SIP IP phone A to Cisco SIP IP phone C | Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone C. The INVITE request contains the following information:  
  - Referred-By: B  
  - Replaces: B |
| 20.  | 200 OK—Cisco SIP IP phone C to Cisco SIP IP phone A | Cisco SIP IP phone C sends a SIP 200 OK message to Cisco SIP IP phone A. The 200 OK response notifies Cisco SIP IP phone A that the INVITE request has been received. |
| 21.  | ACK—Cisco SIP IP phone A to Cisco SIP IP phone C | Cisco SIP IP phone A sends a SIP ACK to Cisco SIP IP phone C. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone C. |
| 22.  | BYE—Cisco SIP IP phone C to Cisco SIP IP phone B | Cisco SIP IP phone C sends a SIP BYE request to Cisco SIP IP phone B. |
| 23.  | 200 OK—Cisco SIP IP phone B to Cisco SIP IP phone C | Cisco SIP IP phone B sends a SIP 200 OK message to Cisco SIP IP phone C. The 200 OK response notifies Cisco SIP IP phone C that the BYE request has been received. |
| 25.  | 200 OK—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a SIP 200 OK message to Cisco SIP IP phone A. The 200 OK response notifies Cisco SIP IP phone A that the NOTIFY request has been received. |
| 26.  | BYE—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a SIP BYE request to Cisco SIP IP phone A. |
| 27.  | 200 OK—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP 200 OK message to Cisco SIP IP phone B. The 200 OK response notifies Cisco SIP IP phone A that the BYE request has been received. |

A two-way RTP channel is established between Cisco SIP IP phone A and Cisco SIP IP phone C.
Call Transfer with Consultation Using Failover

Figure B-10 illustrates a successful call between Cisco SIP IP phones in which two parties are in a call, one of the participants contacts a third party, and then that participant transfers the call to the third party. This is called an attended transfer. In this call flow scenario, the end users are User A, User B, and User C. They are all using Cisco SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B calls User C, and User C consents to take the call.
4. User B transfers the call to User C.
5. User B disconnects with User C.
6. User C and User A connect to each other.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.  
     In the INVITE request:  
     - The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an e-mail address (user@host, where user is the telephone number and host is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as “INVITE sip:555-0002@companyb.com; user=phone.” The “user=phone” parameter distinguishes that the Request-URI address is a telephone number rather than a username.  
     - Cisco SIP IP phone A is identified as the call session initiator in the From field.  
     - A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.  
     - The transaction number within a single call leg is identified in the CSeq field.  
     - The media capability User A is ready to receive is specified. |
| 2.   | 100 Trying—Cisco SIP IP phone B to Cisco SIP IP phone A | The Cisco SIP IP phone B sends a SIP 100 Trying response to Cisco SIP IP phone A. The 100 Trying response indicates that the INVITE request has been received by Cisco SIP IP phone B. |
| 3.   | 180 Ringing—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a SIP 180 Ringing response to Cisco SIP IP phone A. |
| 4.   | 200 OK—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a SIP 200 OK response to Cisco SIP IP phone A. The 200 OK response notifies Cisco SIP IP phone A that the connection has been made.  
     If Cisco SIP IP phone B supports the media capability advertised in the INVITE message sent by Cisco SIP IP phone A, it advertises the intersection of its own and Cisco SIP IP phone A’s media capability in the 200 OK response. If Cisco SIP IP phone B does not support the media capability advertised by Cisco SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field. |
| 5.   | ACK—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP ACK to Cisco SIP IP phone B. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone B.  
     The ACK might contain a message body with the final session description to be used by Cisco SIP IP phone B. If the message body of the ACK is empty, Cisco SIP IP phone B uses the session description in the INVITE request. |
| 6.   | INVITE—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a mid-call INVITE to Cisco SIP IP phone A with new SDP session parameters (IP address), which are used to place the call on hold.  
     Call_ID=1  
     SDP: c=IN IP4 0.0.0.0 |

A two-way RTP channel is established between Cisco SIP IP phone A and Cisco SIP IP phone B.  
User B then selects the option to transfer the call to User C.
## Call Flow Scenarios for Successful Calls

### 7. 200 OK—Cisco SIP IP phone A to Cisco SIP IP phone B
Cisco SIP IP phone A sends a SIP 200 OK response to Cisco SIP IP phone B.

### 8. ACK—Cisco SIP IP phone B to Cisco SIP IP phone A
Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone A. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone A.

User B dials User C.

### 9. INVITE—Cisco SIP IP phone B to Cisco SIP IP phone C
Cisco SIP IP phone B sends a SIP INVITE request to Cisco SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session.

### 10. 100 Trying—Cisco SIP IP phone C to Cisco SIP IP phone B
The Cisco SIP IP phone C sends a SIP 100 Trying response to Cisco SIP IP phone B. The 100 Trying response indicates that the INVITE request has been received by the Cisco SIP IP phone.

### 11. 180 Ringing—Cisco SIP IP phone C to Cisco SIP IP phone B
Cisco SIP IP phone C sends a SIP 180 Ringing response to Cisco SIP IP phone B.

### 12. 200 OK—Cisco SIP IP phone C to Cisco SIP IP phone B
Cisco SIP IP phone C sends a SIP 200 OK response to Cisco SIP IP phone B. The 200 OK response notifies Cisco SIP IP phone B that the connection has been made.

If Cisco SIP IP phone B supports the media capability advertised in the INVITE message sent by Cisco SIP IP phone A, it advertises the intersection of its own and Cisco SIP IP phone A’s media capability in the 200 OK response. If Cisco SIP IP phone B does not support the media capability advertised by Cisco SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field.

### 13. ACK—Cisco SIP IP phone B to Cisco SIP IP phone C
Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone C. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone C.

The ACK might contain a message body with the final session description to be used by Cisco SIP IP phone C. If the message body of the ACK is empty, Cisco SIP IP phone C uses the session description in the INVITE request.

A two-way RTP channel is established between Cisco SIP IP phone B and Cisco SIP IP phone C.

User B then selects the option to transfer the call to User C.

### 14. INVITE—Cisco SIP IP phone B to Cisco SIP IP phone A
Cisco SIP IP phone B sends a mid-call INVITE to Cisco SIP IP phone A with new SDP session parameters (IP address), which are used to place the call on hold.

<table>
<thead>
<tr>
<th>Call_ID=1</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDP: c=IN IP4 0.0.0.0</td>
</tr>
</tbody>
</table>

The c= SDP field of the SIP INVITE contains an 0.0.0.0. This places the call in hold.

### 15. 200 OK—Cisco SIP IP phone A to Cisco SIP IP phone B
Cisco SIP IP phone A sends a SIP 200 OK response to Cisco SIP IP phone B.

### 16. ACK—Cisco SIP IP phone B to Cisco SIP IP phone C
Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone C. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone C.
### Call Flow Scenarios for Successful Calls

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 17.  | REFER—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a REFER message to Cisco SIP IP phone A. The REFER message contains the following information:  
  - Refer-To: C  
  - Replaces: B  
  - Referred-By: B  
The REFER message indicates that the user (recipient) should contact a third party for use in transferring parties. |
| 18.  | 501 Not Implemented—Cisco SIP IP Phone A to Cisco SIP IP Phone B | Cisco SIP IP phone A sends a 501 Not Implemented message to Cisco SIP IP phone B. This message indicates that the REFER message is not supported and that Cisco SIP IP phone B should failover to Bye/Also. |
| 19.  | BYE—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a BYE message to Cisco SIP IP phone A. The BYE message includes the following information:  
  - Also: C  
This message indicates that the 501 Not Implemented message was received in response to a REFER message. |
| 20.  | 200 OK—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP 200 OK message to Cisco SIP IP phone B. The 200 OK response notifies Cisco SIP IP phone B that the BYE request has been received. |
| 21.  | BYE—Cisco SIP IP phone B to Cisco SIP IP phone C | Cisco SIP IP phone B sends a SIP BYE request to Cisco SIP IP phone C. |
| 22.  | 200 OK—Cisco SIP IP phone C to Cisco SIP IP phone B | Cisco SIP IP phone C sends a SIP 200 OK message to Cisco SIP IP phone B. The 200 OK response notifies Cisco SIP IP phone B that the BYE request has been received. |
| 23.  | INVITE—Cisco SIP IP phone A to Cisco SIP IP phone C | Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone C. The INVITE request contains the following information:  
  - Requested-By: B  
This message indicates that the INVITE was requested by Cisco SIP IP phone B. |
| 24.  | 100 Trying—Cisco SIP IP phone C to Cisco SIP IP phone A | The Cisco SIP IP phone C sends a SIP 100 Trying response to Cisco SIP IP phone A. The 100 Trying response indicates that the INVITE request has been received by Cisco SIP IP phone C. |
| 26.  | 200 OK—Cisco SIP IP phone C to Cisco SIP IP phone A | Cisco SIP IP phone C sends a SIP 200 OK response to Cisco SIP IP phone A. The 200 OK response notifies Cisco SIP IP phone A that the connection has been made. |
| 27.  | ACK—Cisco SIP IP phone A to Cisco SIP IP phone C | Cisco SIP IP phone A sends a SIP ACK to Cisco SIP IP phone C. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone C. |

A two-way RTP channel is established between Cisco SIP IP phone A and Cisco SIP IP phone C.
Network Call Forwarding (Unconditional)

Figure B-11 illustrates successful call forwarding between Cisco SIP IP phones in which User B has requested unconditional call forwarding from the network. When User A calls User B, the call is immediately transferred to Cisco SIP IP phone C. In this call flow scenario, the end users are User A, User B, and User C. They are all using Cisco SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B requests that the network forward all calls to Cisco SIP IP phone C.
2. User A calls User B.
3. The network transfers the call to Cisco SIP IP phone C.

Figure B-11  Network Call Forwarding (Unconditional)
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | INVITE—Cisco SIP IP phone A to SIP proxy server | Cisco SIP IP phone A sends a SIP INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request:  
- The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an e-mail address (user@host, where user is the telephone number and host is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as “INVITE sip:555-0002@companyb.com; user=phone.” The “user=phone” parameter distinguishes that the Request-URI address is a telephone number rather than a username.  
- Cisco SIP IP phone A is identified as the call session initiator in the From field.  
- A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.  
- The transaction number within a single call leg is identified in the CSeq field.  
- The media capability User A is ready to receive is specified. |
| 2.   | INVITE—SIP proxy server to SIP redirect server | SIP proxy server sends the SIP INVITE request to the SIP redirect server. |
| 3.   | 302 Moved Temporarily—SIP redirect server to SIP proxy server | SIP redirect server sends a SIP 302 Moved temporarily message to the SIP proxy server. The message indicates that User B is not available at SIP phone B and includes instructions to locate User B at Cisco SIP IP phone C. |
| 4.   | INVITE—SIP proxy server to Cisco SIP IP phone C | SIP proxy server sends a SIP INVITE request to Cisco SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session. |
| 5.   | 180 Ringing—Cisco SIP IP phone C to SIP proxy server | Cisco SIP IP phone C sends a SIP 180 Ringing response to the SIP proxy server. |
| 6.   | 200 OK—Cisco SIP IP phone C to SIP proxy server | Cisco SIP IP phone C sends a SIP 200 OK response to the SIP proxy server. |
| 7.   | 200 OK—SIP proxy server to Cisco SIP IP phone A | SIP proxy server forwards the SIP 200 OK response to Cisco SIP IP phone A. |
| 8.   | ACK—Cisco SIP IP phone A to SIP proxy server | Cisco SIP IP phone A sends a SIP ACK to the SIP proxy server. The ACK confirms that the SIP proxy server has received the 200 OK response from Cisco SIP IP phone C. |
| 9.   | ACK—SIP proxy server to Cisco SIP IP phone C | SIP proxy server forwards the SIP ACK to the Cisco SIP IP phone C. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone C. |
Network Call Forwarding (Busy)

Figure B-12 illustrates successful call forwarding between Cisco SIP IP phones in which User B has requested call forwarding from the network in the event the phone is busy. When User A calls User B, the SIP proxy server tries to place the call to Cisco SIP IP phone B and, if the line is busy, the call is transferred to Cisco SIP IP phone C. In this call flow scenario, the end users are User A, User B, and User C. They are all using Cisco SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B requests that if their phone (Cisco SIP IP phone B) is busy, the network should forward incoming calls to Cisco SIP IP phone C.
2. User A calls User B.
3. User B’s phone is busy.
4. The network transfers the call to Cisco SIP IP phone C.

![Network Call Forwarding (Busy) Diagram]

- 1. INVITE B
- 2. INVITE B
- 3. 300 Multiple Choices
- 4. ACK
- 5. INVITE B
- 6. 486 Busy Here
- 7. ACK
- 8. INVITE C
- 9. 180 Ringing
- 10. 200 OK
- 11. 200 OK
- 12. ACK
- 13. ACK

SIP IP Phone User A
Proxy Server
Redirect Server
SIP IP Phone User B
SIP IP Phone User C

Network Call Forwarding (Busy)
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | INVITE—Cisco SIP IP phone A to SIP proxy server | Cisco SIP IP phone A sends a SIP INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request:  
  - The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an e-mail address (user@host, where user is the telephone number and host is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as “INVITE sip:555-0002@companyb.com; user=phone.” The “user=phone” parameter distinguishes that the Request-URI address is a telephone number rather than a username.  
  - Cisco SIP IP phone A is identified as the call session initiator in the From field.  
  - A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.  
  - The transaction number within a single call leg is identified in the CSeq field.  
  - The media capability User A is ready to receive is specified. |
| 2.   | INVITE—SIP proxy server to SIP redirect server | SIP proxy server sends the SIP INVITE request to the SIP redirect server. |
| 3.   | 300 Multiple Choices—SIP redirect server to SIP proxy server | SIP redirect server sends a SIP 300 Multiple choices message to the SIP proxy server. The message indicates that User B can be reached either at SIP phone B or Cisco SIP IP phone C. |
| 4.   | INVITE—SIP proxy server to Cisco SIP IP phone B | SIP proxy server sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session. |
| 5.   | 486 Busy Here—Cisco SIP IP phone B to SIP proxy server | Cisco SIP IP phone B sends a 486 Busy here message to the SIP proxy server. The message indicates that Cisco SIP IP phone B is in use and the user is not willing or able to take additional calls. |
| 6.   | ACK—SIP proxy server to Cisco SIP IP phone B | SIP proxy server forwards the SIP ACK to the Cisco SIP IP phone B. The ACK confirms that the SIP proxy server has received the 486 Busy here response from Cisco SIP IP phone B. |
| 7.   | INVITE—SIP proxy server to Cisco SIP IP phone C | SIP proxy server sends a SIP INVITE request to Cisco SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session. |
| 8.   | 180 Ringing—Cisco SIP IP phone C to SIP proxy server | Cisco SIP IP phone C sends a SIP 180 Ringing response to the SIP proxy server. |
| 10.  | 200 OK—SIP proxy server to Cisco SIP IP phone A | SIP proxy server forwards the SIP 200 OK response to Cisco SIP IP phone A. |
Call Flow Scenarios for Successful Calls

Network Call Forwarding (No Answer)

Figure B-13 illustrates successful call forwarding between Cisco SIP IP phones in which User B has requested call forwarding from the network in the event that there is no answer. When User A calls User B, the proxy server tries to place the call to Cisco SIP IP phone B and, if there is no answer, the call is transferred to Cisco SIP IP phone C. In this call flow scenario, the end users are User A, User B, and User C. They are all using Cisco SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User B requests that if the phone (Cisco SIP IP phone B) is not answered within a set amount of time, the network should forward incoming calls to Cisco SIP IP phone C.
2. User A calls User B.
3. User B’s phone is not answered.
4. The network transfers the call to Cisco SIP IP phone C.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.</td>
<td>ACK—Cisco SIP IP phone A to SIP proxy server</td>
<td>Cisco SIP IP phone A sends a SIP ACK to the SIP proxy server. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone C.</td>
</tr>
<tr>
<td>12.</td>
<td>ACK—SIP proxy server to Cisco SIP IP phone C</td>
<td>SIP proxy server forwards the SIP ACK to the Cisco SIP IP phone C. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone C.</td>
</tr>
</tbody>
</table>
Figure B-13 Network Call Forwarding (No Answer)

1. INVITE B

2. INVITE B

3. 300 Multiple Choices

4. ACK

5. INVITE B

6. 180 Ringing

7. 180 Ringing

8. CANCEL

9. 200 OK

10. INVITE C

11. 180 Ringing

12. 200 OK

13. 200 OK

14. ACK

15. ACK

2-way RTP channel
## Call Flow Scenarios for Successful Calls

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | INVITE—Cisco SIP IP phone A to SIP proxy server | Cisco SIP IP phone A sends a SIP INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request:  
- The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an e-mail address (user@host, where user is the telephone number and host is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as “INVITE sip:555-0002@companyb.com; user=phone.” The “user=phone” parameter distinguishes that the Request-URI address is a telephone number rather than a username.  
- Cisco SIP IP phone A is identified as the call session initiator in the From field.  
- A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.  
- The transaction number within a single call leg is identified in the CSeq field.  
- The media capability User A is ready to receive is specified. |
| 2.   | INVITE—SIP proxy server to SIP redirect server | SIP proxy server sends the SIP INVITE request to the SIP redirect server. |
| 3.   | 300 Multiple Choices—SIP redirect server to SIP proxy server | SIP redirect server sends a SIP 300 Multiple choices message to the SIP proxy server. The message indicates that User B can be reached either at SIP phone B or Cisco SIP IP phone C. |
| 4.   | INVITE—SIP proxy server to Cisco SIP IP phone B | Cisco SIP IP phone B sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session. |
| 5.   | 180 Ringing—Cisco SIP IP phone B to SIP proxy server | SIP proxy server sends a SIP 180 Ringing response to the SIP proxy server. The timeout expires before the phone is answered. |
| 6.   | 180 Ringing—SIP proxy server to Cisco SIP IP phone A | SIP proxy server sends a SIP 180 Ringing response to Cisco SIP IP phone A. |
| 7.   | CANCEL (Ring Timeout)—SIP proxy server to Cisco SIP IP phone B | SIP proxy server sends a CANCEL request to Cisco SIP IP phone B to cancel the invitation. |
| 8.   | 200 OK—Cisco SIP IP phone B to SIP proxy server | Cisco SIP IP phone B sends a SIP 200 OK response to the SIP proxy server. The response confirms receipt of the cancellation request. |
| 9.   | INVITE—SIP proxy server to Cisco SIP IP phone C | SIP proxy server sends a SIP INVITE request to Cisco SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session. |
| 10.  | 180 Ringing—Cisco SIP IP phone C to SIP proxy server | Cisco SIP IP phone C sends a SIP 180 Ringing response to the SIP proxy server. |
| 11.  | 200 OK—Cisco SIP IP phone C to SIP proxy server | Cisco SIP IP phone C sends a SIP 200 OK response to the SIP proxy server. |
| 12.  | 200 OK—SIP proxy server to Cisco SIP IP phone A | SIP proxy server forwards the SIP 200 OK response to Cisco SIP IP phone A. |
Call Flow Scenarios for Successful Calls

Three-Way Calling

Figure B-14 illustrates successful three-way calling between Cisco SIP IP phones in which User B mixes two RTP channels and therefore establishes a conference bridge between User A and User C. In this call flow scenario, the end users are User A, User B, and User C. They are all using Cisco SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.
3. User B puts User A on hold.
4. User B calls User C.
5. User C answers the call.
6. User B takes User A off hold.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.</td>
<td>ACK—Cisco SIP IP phone A to SIP proxy server</td>
</tr>
<tr>
<td></td>
<td>Cisco SIP IP phone A sends a SIP ACK to the SIP proxy server. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone C.</td>
</tr>
<tr>
<td>14.</td>
<td>ACK—SIP proxy server to Cisco SIP IP phone C</td>
</tr>
<tr>
<td></td>
<td>SIP proxy server forwards the SIP ACK to the Cisco SIP IP phone C. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone C.</td>
</tr>
</tbody>
</table>
Figure B-14 Three-Way Calling

1. INVITE B (Call-ID=1)
2. 180 Ringing
3. 200 OK
4. ACK

User A is on hold. The RTP channel 1 between User A and B is torn down.

5. INVITE (Call-ID=1, c=IN IP4 0.0.0.0)
6. 200 OK
7. ACK

2-way RTP channel 1 between Users A and B established

8. INVITE A (Call-ID=1, c=IN IP4 0.0.0.0)
9. 200 OK
10. ACK

User B mixes the RTP channels 1 and 2 and establishes a conference bridge between Users A and C.

11. INVITE B (Call-ID=2)
12. 200 OK
13. ACK

2-way RTP channel 1 between User B and C is established
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request:  
   - The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an e-mail address (user@host, where user is the telephone number and host is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as “INVITE sip:555-0002@companyb.com; user=phone.” The “user=phone” parameter distinguishes that the Request-URI address is a telephone number rather than a username.  
   - Cisco SIP IP phone A is identified as the call session initiator in the From field.  
   - A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.  
   - The transaction number within a single call leg is identified in the CSeq field.  
   - The media capability User A is ready to receive is specified. |
| 2.   | 180 Ringing—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a SIP 180 Ringing response to Cisco SIP IP phone A. |
| 3.   | 200 OK—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a SIP 200 OK response to Cisco SIP IP phone A. The 200 OK response notifies Cisco SIP IP phone A that the connection has been made.  
   If Cisco SIP IP phone B supports the media capability advertised in the INVITE message sent by Cisco SIP IP phone A, it advertises the intersection of its own and Cisco SIP IP phone A's media capability in the 200 OK response. If Cisco SIP IP phone B does not support the media capability advertised by Cisco SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field. |
| 4.   | ACK—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP ACK to Cisco SIP IP phone B. The ACK confirms that Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone B.  
   The ACK might contain a message body with the final session description to be used by Cisco SIP IP phone B. If the message body of the ACK is empty, Cisco SIP IP phone B uses the session description in the INVITE request. |
| 5.   | INVITE—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a mid-call INVITE to Cisco SIP IP phone A with new SDP session parameters (IP address), which are used to place the call on hold.  
   Call_ID=1  
   SDP: c=IN IP4 0.0.0.0  
   The c= SDP field of the SIP INVITE contains an 0.0.0.0. This places the call in hold. |
| 6.   | 200 OK—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP 200 OK response to Cisco SIP IP phone B. |

A two-way RTP channel is established between Cisco SIP IP phone A and Cisco SIP IP phone B.
### Call Flow Scenarios for Successful Calls

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>ACK—Cisco SIP IP phone B to Cisco SIP IP phone A</td>
<td>Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone A. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone A. The RTP channel between Cisco SIP IP phone A and Cisco SIP IP phone B is torn down. User A is put on hold.</td>
</tr>
</tbody>
</table>
| 8.   | INVITE—Cisco SIP IP phone B to Cisco SIP IP phone C | Cisco SIP IP phone B sends a SIP INVITE request to Cisco SIP IP phone C. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request:  
  - The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an e-mail address (user@host, where user is the telephone number and host is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User C appears as “INVITE sip:555-0002@companyb.com; user=phone.” The “user=phone” parameter distinguishes that the Request-URI address is a telephone number rather than a username.  
  - Cisco SIP IP phone B is identified as the call session initiator in the From field.  
  - A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.  
  - The transaction number within a single call leg is identified in the CSeq field.  
  - The media capability User B is ready to receive is specified. |
| 9.   | 180 Ringing—Cisco SIP IP phone C to Cisco SIP IP phone B | Cisco SIP IP phone C sends a SIP 180 Ringing response to Cisco SIP IP phone B.                                                                                                                                 |
| 10.  | 200 OK—Cisco SIP IP phone C to Cisco SIP IP phone B | Cisco SIP IP phone C sends a SIP 200 OK response to Cisco SIP IP phone B. The 200 OK response notifies Cisco SIP IP phone B that the connection has been made.  
  - If Cisco SIP IP phone C supports the media capability advertised in the INVITE message sent by Cisco SIP IP phone B, it advertises the intersection of its own and Cisco SIP IP phone B’s media capability in the 200 OK response. If Cisco SIP IP phone C does not support the media capability advertised by Cisco SIP IP phone B, it sends back a 400 Bad Request response with a 304 Warning header field. |
| 11.  | ACK—Cisco SIP IP phone B to Cisco SIP IP phone C | Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone C. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone C.  
  - The ACK might contain a message body with the final session description to be used by Cisco SIP IP phone C. If the message body of the ACK is empty, Cisco SIP IP phone C uses the session description in the INVITE request.  
  - A two-way RTP channel is established between SIP IP phone B and SIP IP phone C. |
### Call Flow Scenarios for Successful Calls

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.  | INVITE—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a mid-call INVITE to Cisco SIP IP phone A with the same call ID as the previous INVITE and new SDP session parameters (IP address), which are used to reestablish the call.  
   
   **Call_ID=1**  
   **SDP:** c=IN IP4 10.10.10.10  
   
   To reestablish the call between phone A and phone B, the IP address of phone B is inserted into the c= SDP field. |
| 13.  | 200 OK—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP 200 OK response to Cisco SIP IP phone B. |
| 14.  | ACK—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a SIP ACK to Cisco SIP IP phone A. The ACK confirms that Cisco SIP IP phone B has received the 200 OK response from Cisco SIP IP phone A.  
   
   SIP IP phone B acts as a bridge mixing the RTP channel between User A and User B with the channel between User B and User C; establishing a conference bridge between User A and User C. |
Call from a Cisco SIP IP Phone to a Gateway Acting as a Backup Proxy

Figure B-15 illustrates a successful call from a Cisco SIP IP phone to a gateway acting as a backup proxy.

Figure B-15 Call from a Cisco SIP IP Phone to a Gateway Acting as a Backup Proxy

1. INVITE
2. INVITE (retry)
3. INVITE (retry)
4. INVITE (retry)
5. INVITE (retry)
6. INVITE (retry)
7. INVITE (retry)
8. INVITE (retry)
9. Setup
10. Call Proceeding
11. 100 Trying
12. Alerting
13. 180 Ringing
14. Connect
15. 200 OK
16. ACK
17. Connect ACK
18. Bye
19. Disconnect
20. Release
21. 200 OK
22. Release Complete

IP
SIP IP Phone
User A
Primary
GW
PBX
User B

2-way voice path
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>INVITE—Cisco SIP IP phone to primary proxy</td>
<td>Cisco SIP IP phone tries to connect to the proxy by sending out the INVITE message.</td>
</tr>
<tr>
<td>2.</td>
<td>INVITE—Cisco SIP IP phone to primary proxy (second try)</td>
<td>Cisco SIP IP phone retries a second time to connect to the proxy by sending out the INVITE message.</td>
</tr>
<tr>
<td>3.</td>
<td>INVITE—Cisco SIP IP phone to primary proxy (third try)</td>
<td>Cisco SIP IP phone retries a third time to connect to the proxy by sending out the INVITE message.</td>
</tr>
<tr>
<td>4.</td>
<td>INVITE—Cisco SIP IP phone to primary proxy (fourth try)</td>
<td>Cisco SIP IP phone retries a fourth time to connect to the proxy by sending out the INVITE message.</td>
</tr>
<tr>
<td>5.</td>
<td>INVITE—Cisco SIP IP phone to primary proxy (fifth try)</td>
<td>Cisco SIP IP phone retries a fifth time to connect to the proxy by sending out the INVITE message. If the connection is not successful after this trial, “Network Delay, Trying Backup” message displays on the Phone.</td>
</tr>
<tr>
<td>6.</td>
<td>INVITE—Cisco SIP IP phone to primary proxy (sixth try)</td>
<td>Cisco SIP IP phone retries a sixth time to connect to the proxy by sending out the INVITE message.</td>
</tr>
<tr>
<td>7.</td>
<td>INVITE—Cisco SIP IP phone to primary proxy (seventh try)</td>
<td>Cisco SIP IP phone retries a seventh time to connect to the proxy.</td>
</tr>
<tr>
<td>8.</td>
<td>Setup—Gateway to PBX</td>
<td>Call Setup is initiated between gateway to PBX. The Call Setup includes the standard transactions that take place as User A attempts to call User B.</td>
</tr>
<tr>
<td>9.</td>
<td>Call Proceeding—PBX to gateway</td>
<td>PBX sends a Call Proceeding message to gateway to acknowledge the Call Setup request.</td>
</tr>
<tr>
<td>10.</td>
<td>100 Trying—Gateway to Cisco SIP IP phone (User A)</td>
<td>Gateway sends a SIP 100 Trying response to User A. The 100 Trying response indicates that the INVITE request has been received by the gateway.</td>
</tr>
<tr>
<td>11.</td>
<td>Alerting—PBX to gateway</td>
<td>PBX sends an Alert message to gateway. The Alert message indicates that PBX has received a 100 Trying Ringing response from the gateway.</td>
</tr>
<tr>
<td>12.</td>
<td>180 Ringing—Gateway to Cisco SIP IP phone (User A)</td>
<td>The gateway sends a SIP 180 Ringing response to User A. The 180 Ringing response indicates that the gateway is being alerted.</td>
</tr>
<tr>
<td>13.</td>
<td>Connect—PBX to gateway</td>
<td>PBX sends a Connect message to gateway. The Connect message notifies the gateway that the connection has been made.</td>
</tr>
<tr>
<td>14.</td>
<td>200 OK—Gateway to Cisco SIP IP phone (User A)</td>
<td>Gateway sends a SIP 200 OK response to the User A. The 200 OK response notifies User A that the connection has been made.</td>
</tr>
<tr>
<td>15.</td>
<td>ACK—Cisco SIP IP phone (User A) to gateway</td>
<td>User A sends a SIP ACK to the gateway. The ACK confirms that User A has received the 200 OK response. The call session is now active.</td>
</tr>
<tr>
<td>17.</td>
<td>BYE—Cisco SIP IP phone (User A) to gateway</td>
<td>User A terminates the call session and sends a SIP BYE request to gateway. The BYE request indicates that User A wants to release the call.</td>
</tr>
<tr>
<td>18.</td>
<td>Disconnect—Gateway to PBX</td>
<td>Gateway sends a Disconnect message to PBX.</td>
</tr>
</tbody>
</table>
Call from a Cisco SIP IP Phone to a Cisco SIP IP Phone By Way of a Backup Proxy

Figure B-16 illustrates a successful call from a Cisco SIP IP phone to a Cisco SIP IP phone via a backup proxy.

Figure B-16  A Successful Call from a Cisco SIP IP Phone to a Cisco SIP IP Phone By Way of a Backup Proxy

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21.</td>
<td>200 OK—Gateway to Cisco SIP IP phone (User A)</td>
<td>Gateway sends a SIP 200 OK response to User A. The 200 OK response notifies User A that the gateway has received the BYE request.</td>
</tr>
<tr>
<td>22.</td>
<td>Release Complete—Gateway to PBX</td>
<td>Gateway sends a Release Complete message to PBX and the call session is terminated.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>1.</td>
<td>INVITE—Cisco SIP IP phone (User A) to primary proxy</td>
<td>Cisco SIP IP Phone tries to connect to the primary proxy by sending out the INVITE message.</td>
</tr>
<tr>
<td>2.</td>
<td>INVITE—Cisco SIP IP phone (User A) to primary proxy (second try)</td>
<td>Cisco SIP IP phone retries a second time to connect to the primary proxy by sending out the INVITE message.</td>
</tr>
<tr>
<td>3.</td>
<td>INVITE—Cisco SIP IP phone (User A) to primary proxy (third try)</td>
<td>Cisco SIP IP phone retries a third time to connect to the primary proxy by sending out the INVITE message.</td>
</tr>
<tr>
<td>4.</td>
<td>INVITE—Cisco SIP IP phone (User A) to primary proxy (fourth try)</td>
<td>Cisco SIP IP phone retries a fourth time to connect to the primary proxy by sending out the INVITE message.</td>
</tr>
<tr>
<td>5.</td>
<td>INVITE—Cisco SIP IP phone (User A) to primary proxy (fifth try)</td>
<td>Cisco SIP IP phone retries a fifth time to connect to the primary proxy by sending out the INVITE message.</td>
</tr>
<tr>
<td>6.</td>
<td>INVITE—Cisco SIP IP phone (User A) to primary proxy (sixth try)</td>
<td>Cisco SIP IP phone retries a sixth time to connect to the primary proxy by sending out the INVITE message.</td>
</tr>
<tr>
<td>7.</td>
<td>INVITE—Cisco SIP IP phone (User A) to primary proxy (seventh try)</td>
<td>Cisco SIP IP phone retries a seventh time to connect to the primary proxy. If the connection is not successful after this trial, the “Network Delay, Trying Backup” message displays on the Phone.</td>
</tr>
<tr>
<td>8.</td>
<td>INVITE—Backup proxy to Cisco SIP IP phone (User B)</td>
<td>Backup proxy tries to connect to User B by sending out the INVITE message.</td>
</tr>
<tr>
<td>9.</td>
<td>100 Trying—Backup proxy to Cisco SIP IP phone (User A)</td>
<td>Backup proxy sends a SIP 100 Trying response to Cisco SIP IP phone. The 100 Trying response indicates that the INVITE request has been received by the backup proxy.</td>
</tr>
<tr>
<td>10.</td>
<td>100 Trying—Backup proxy to Cisco SIP IP phone (User B)</td>
<td>User B sends a SIP 100 Trying response to backup proxy. The 100 Trying response indicates that the INVITE request has been received by User B.</td>
</tr>
<tr>
<td>11.</td>
<td>180 Ringing—Cisco SIP IP phone (User B) to backup proxy</td>
<td>User B sends a SIP 180 Ringing response to the backup proxy. The 180 Ringing response indicates that User B is being alerted.</td>
</tr>
<tr>
<td>12.</td>
<td>180 Ringing—Backup proxy to Cisco SIP IP phone (User A)</td>
<td>The backup proxy sends a SIP 180 Ringing response to User A. The 180 Ringing response indicates that the backup proxy is being alerted.</td>
</tr>
<tr>
<td>13.</td>
<td>200 OK—Cisco SIP IP phone (User B) to backup proxy</td>
<td>User B sends a SIP 200 OK response to the backup proxy. The 200 OK response notifies the backup proxy that the connection has been made.</td>
</tr>
<tr>
<td>14.</td>
<td>200 OK—Backup proxy to Cisco SIP IP phone (User A)</td>
<td>Backup proxy sends a SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.</td>
</tr>
<tr>
<td>15.</td>
<td>ACK—Cisco SIP IP phone (User A) to backup proxy</td>
<td>User A acknowledges backup proxy’s Connect message.</td>
</tr>
<tr>
<td>16.</td>
<td>ACK—Backup proxy to Cisco SIP IP phone (User B)</td>
<td>Backup proxy acknowledges User B’s Connect message.</td>
</tr>
<tr>
<td>17.</td>
<td>BYE—Cisco SIP IP phone (User A) to backup proxy</td>
<td>User A terminates the call session and sends a SIP BYE request to backup proxy. The BYE request indicates that User A wants to release the call.</td>
</tr>
</tbody>
</table>
Call from Cisco SIP IP Phone to Cisco SIP IP Phone Using an Emergency Proxy

Figure B-17 illustrates a successful call from a Cisco SIP IP phone to a Cisco SIP IP phone via emergency proxy. User B is the extension of the dial template with the “Route” attribute as “emergency” in the dialplan.xml file.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.</td>
<td>BYE—Backup proxy to Cisco SIP IP phone (User B)</td>
<td>Backup proxy terminates the call session and sends a SIP BYE request to User B. The BYE request indicates that the backup proxy wants to release the call.</td>
</tr>
<tr>
<td>20.</td>
<td>200 OK—Cisco SIP IP phone (User B) to backup proxy</td>
<td>User B sends a SIP 200 OK response to the backup proxy. The 200 OK response notifies the backup proxy that User B has received the BYE request.</td>
</tr>
<tr>
<td>21.</td>
<td>200 OK—Backup proxy to Cisco SIP IP phone (User A)</td>
<td>Backup proxy sends a SIP 200 OK response to User A. The 200 OK response notifies User A that the backup proxy has received the BYE request.</td>
</tr>
</tbody>
</table>

Figure B-17  Successful Call from a Cisco SIP IP Phone to a Cisco SIP IP Phone Using an Emergency Proxy

1. INVITE (Matches dial template for emergency route)

2. 100 Trying

6. 180 Ringing

8. 200 OK

9. ACK

11. BYE

14. 200 OK

3. INVITE

4. 100 Trying

5. 180 Ringing

7. 200 OK

10. ACK

12. BYE

13. 200 OK
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>INVITE—Cisco SIP IP phone (User A) to emergency proxy</td>
<td>Cisco SIP IP phone tries to connect to the emergency proxy by sending out the INVITE message. The dial template for the emergency route is matched.</td>
</tr>
<tr>
<td>2.</td>
<td>100 Trying—Emergency proxy to Cisco SIP IP phone (User A)</td>
<td>Emergency proxy sends a SIP 100 Trying response to User A. The 100 Trying response indicates that the INVITE request has been received by the emergency proxy.</td>
</tr>
<tr>
<td>3.</td>
<td>INVITE—Emergency proxy to Cisco SIP IP phone (User B)</td>
<td>Backup proxy tries to connect to User B by sending out the INVITE message.</td>
</tr>
<tr>
<td>4.</td>
<td>100 Trying—Cisco SIP IP phone (User B) to emergency proxy</td>
<td>User B sends a SIP 100 Trying response to the emergency proxy. The 100 Trying response indicates that the INVITE request has been received by User B.</td>
</tr>
<tr>
<td>5.</td>
<td>180 Ringing—Cisco SIP IP phone (User B) to emergency proxy</td>
<td>User B sends a SIP 180 Ringing response to the emergency proxy. The 180 Ringing response indicates that User B is being alerted.</td>
</tr>
<tr>
<td>6.</td>
<td>180 Ringing—Emergency proxy to Cisco SIP IP phone (User A)</td>
<td>The emergency proxy sends a SIP 180 Ringing response to User A. The 180 Ringing response indicates that the emergency proxy is being alerted.</td>
</tr>
<tr>
<td>7.</td>
<td>200 OK—Cisco SIP IP phone (User B) to emergency proxy</td>
<td>User B sends a SIP 200 OK response to the emergency proxy. The 200 OK response notifies the emergency proxy that the connection has been made.</td>
</tr>
<tr>
<td>8.</td>
<td>200 OK—Emergency proxy to Cisco SIP IP phone (User A)</td>
<td>Emergency proxy sends a SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.</td>
</tr>
<tr>
<td>9.</td>
<td>ACK—Cisco SIP IP phone (User A) to emergency proxy</td>
<td>User A acknowledges the emergency proxy’s Connect message.</td>
</tr>
<tr>
<td>11.</td>
<td>BYE—Cisco SIP IP phone (User A) to emergency proxy</td>
<td>User A terminates the call session and sends a SIP BYE request to the emergency proxy. The BYE request indicates that User A wants to release the call.</td>
</tr>
<tr>
<td>12.</td>
<td>BYE—Emergency proxy to Cisco SIP IP phone (User B)</td>
<td>Emergency proxy terminates the call session and sends a SIP BYE request to User B. The BYE request indicates that the emergency proxy wants to release the call.</td>
</tr>
<tr>
<td>13.</td>
<td>200 OK—Cisco SIP IP phone (User B) to emergency proxy</td>
<td>User B sends a SIP 200 OK response to the emergency proxy. The 200 OK response notifies the emergency proxy that User B has received the BYE request.</td>
</tr>
<tr>
<td>14.</td>
<td>200 OK—Emergency proxy to Cisco SIP IP phone (User A)</td>
<td>Emergency proxy sends a SIP 200 OK response to User A. The 200 OK response notifies User A that the emergency proxy has received the BYE request.</td>
</tr>
</tbody>
</table>
Call Flow Scenarios for Failed Calls

This section describes call flows for the following scenarios, which illustrate unsuccessful calls:

- Gateway to Cisco SIP IP Phone, page B-52
- Cisco SIP IP Phone to Cisco SIP IP Phone, page B-57

Gateway to Cisco SIP IP Phone

The following scenarios are failed calls in the gateway to a Cisco SIP IP phone:

- Called User Is Busy, page B-52
- Called User Does Not Answer, page B-54
- Client, Server, or Global Error, page B-55

Called User Is Busy

Figure B-18 illustrates an unsuccessful call in which User A initiates a call to User B, but User B is on the phone and is unable or unwilling to take another call.

![Figure B-18 Called User is Busy](image-url)
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Setup—PBX A to Gateway 1</td>
<td>Call Setup is initiated between PBX A and Gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.</td>
</tr>
</tbody>
</table>
| 2.   | INVITE—Gateway 1 to Cisco SIP IP phone | Gateway 1 maps the SIP URL phone number to a dial peer. The dial peer includes the IP address and the port number of the SIP enabled entity to contact. Gateway 1 sends a SIP INVITE request to the address it receives as the dial peer which, in this scenario, is the Cisco SIP IP phone.  
In the INVITE request:  
• The IP address of the Cisco SIP IP phone is inserted in the Request-URI field.  
• PBX A is identified as the call session initiator in the From field.  
• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.  
• The transaction number within a single call leg is identified in the CSeq field.  
• The media capability User A is ready to receive is specified.  
• The port on which the gateway is prepared to receive the RTP data is specified. |
| 3.   | Call Proceeding—Gateway 1 to PBX A | Gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request. |
| 4.   | 100 Trying—Cisco SIP IP phone to Gateway 1 | The Cisco SIP IP phone sends a SIP 100 Trying response to Gateway 1. The 100 Trying response indicates that the INVITE request has been received by the Cisco SIP IP phone. |
| 5.   | 486 Busy Here—Cisco SIP IP phone to Gateway 1 | The Cisco SIP IP phone sends a SIP 486 Busy Here response to Gateway 1. The 486 Busy Here response is a client error response that indicates that User B was successfully contacted but that User B was not willing or was unable to take the call. |
| 6.   | Disconnect (Busy)—Gateway 1 to PBX A | Gateway 1 sends a Disconnect message to PBX A. |
| 7.   | Release—PBX A to Gateway 1 | PBX A sends a Release message to Gateway 1. |
| 8.   | ACK—Gateway 1 to Cisco SIP IP phone | Gateway 1 sends a SIP ACK to the Cisco SIP IP phone. The ACK confirms that User A has received the 486 Busy Here response. The call session attempt is now being terminated. |
| 9.   | Release Complete—Gateway 1 to PBX A | Gateway 1 sends a Release Complete message to PBX A and the call session attempt is terminated. |
## Called User Does Not Answer

Figure B-19 illustrates the call flow in which User A initiates a call to User B but User B does not answer.

![Figure B-19 Called User Does Not Answer](image)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Setup—PBX A to Gateway 1</td>
<td>Call Setup is initiated between PBX A and Gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.</td>
</tr>
</tbody>
</table>
| 2.   | INVITE—Gateway 1 to Cisco SIP IP phone | Gateway 1 maps the SIP URL phone number to a dial peer. The dial peer includes the IP address and the port number of the SIP enabled entity to contact. Gateway 1 sends a SIP INVITE request to the address it receives as the dial peer which, in this scenario, is the Cisco SIP IP phone. In the INVITE request:  
  - The IP address of the Cisco SIP IP phone is inserted in the Request-URI field.  
  - PBX A is identified as the call session initiator in the From field.  
  - A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.  
  - The transaction number within a single call leg is identified in the CSeq field.  
  - The media capability User A is ready to receive is specified.  
  - The port on which the Gateway is prepared to receive the RTP data is specified. |
| 3.   | Call Proceeding—Gateway 1 to PBX A | Gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request. |
| 4.   | 100 Trying—Cisco SIP IP phone to Gateway 1 | The Cisco SIP IP phone sends a SIP 100 Trying response to Gateway 1. The 100 Trying response indicates that the INVITE request has been received by the Cisco SIP IP phone. |
Call Flow Scenarios for Failed Calls

Client, Server, or Global Error

Figure B-20 illustrates an unsuccessful call in which User A initiates a call to User B and receives a class 4xx, 5xx, or 6xx response.

### Figure B-20  Client, Server, or Global Error

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>180 Ringing—Cisco SIP IP phone to Gateway 1</td>
<td>The Cisco SIP IP phone sends a SIP 180 Ringing response to Gateway 1. The 180 Ringing response indicates that the user is being alerted.</td>
</tr>
<tr>
<td>6.</td>
<td>Alerting—Gateway 1 to PBX A</td>
<td>Gateway 1 sends an Alert message to PBX A.</td>
</tr>
<tr>
<td>7.</td>
<td>CANCEL (Ring Timeout)—Gateway 1 to Cisco SIP IP phone</td>
<td>Because Gateway 1 did not return an appropriate response within the time allocated in the INVITE request, Gateway 1 sends a SIP CANCEL request to Gateway 2. A CANCEL request cancels a pending request with the same Call-ID, To, From, and CSeq header field values.</td>
</tr>
<tr>
<td>8.</td>
<td>Disconnect—Gateway 1 to PBX A</td>
<td>Gateway 1 sends a Disconnect message to PBX A.</td>
</tr>
<tr>
<td>9.</td>
<td>Release Complete—Gateway 1 to PBX A</td>
<td>Gateway 1 sends a Release Complete message to PBX A and the call session attempt is terminated.</td>
</tr>
<tr>
<td>10.</td>
<td>200 OK—Cisco SIP IP phone to Gateway 1</td>
<td>The Cisco SIP IP phone sends a SIP 200 OK response to Gateway 1. The 200 OK response confirms that User A has received the 486 Busy Here response. The call session attempt is now being terminated.</td>
</tr>
<tr>
<td>11.</td>
<td>Release Complete—Gateway 1 to PBX A</td>
<td>Gateway 1 sends a Release Complete message to PBX A and the call session is terminated.</td>
</tr>
</tbody>
</table>
### Call Flow Scenarios for Failed Calls

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Setup—PBX A to Gateway 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Call Setup is initiated between PBX A and Gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>INVITE—Gateway 1 to Cisco SIP IP phone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gateway 1 maps the SIP URL phone number to a dial peer. The dial peer includes the IP address and the port number of the SIP enabled entity to contact. Gateway 1 sends a SIP INVITE request to the address it receives as the dial peer which, in this scenario, is the Cisco SIP IP phone.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the INVITE request:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The IP address of the Cisco SIP IP phone is inserted in the Request-URI field.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PBX A is identified as the call session initiator in the From field.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The transaction number within a single call leg is identified in the CSeq field.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The media capability User A is ready to receive is specified.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The port on which the gateway is prepared to receive the RTP data is specified.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Call Proceeding—Gateway 1 to PBX A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>100 Trying—Cisco SIP IP phone to Gateway 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Cisco SIP IP phone sends a SIP 100 Trying response to Gateway 1. The 100 Trying response indicates that the INVITE request has been received by the Cisco SIP IP phone.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>4xx/5xx/6xx Failure—Cisco SIP IP phone to Gateway 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Cisco SIP IP phone sends a class 4xx, 5xx, or class 6xx failure response to Gateway 1. Depending on which class the failure response is, the call actions differ.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the Cisco SIP IP phone sends a class 4xx failure response (a definite failure response that is a client error), the request will not be retried without modification.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the Cisco SIP IP phone sends a class 5xx failure response (an indefinite failure that is a server error), the request is not terminated but rather other possible locations are tried.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the Cisco SIP IP phone sends a class 6xx failure response (a global error), the search for User B is terminated because the 6xx response indicates that a server has definite information about User B, but not for the particular instance indicated in the Request-URI field. Therefore, all further searches for this user will fail.</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Disconnect—Gateway 1 to PBX A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gateway 1 sends a Release message to PBX A.</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Release—PBX A to Gateway 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PBX A sends a Release message to Gateway 1.</td>
<td></td>
</tr>
</tbody>
</table>
Cisco SIP IP Phone to Cisco SIP IP Phone

The following scenarios are Cisco SIP IP phone to Cisco SIP IP phone:

- Called User Is Busy, page B-57
- Called User Does Not Answer, page B-58
- Authentication Error, page B-59

Called User Is Busy

Figure B-21 illustrates an unsuccessful call in which User A initiates a call to User B but User B is on the phone and is unable or unwilling to take another call.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>ACK—Gateway 1 to Cisco SIP IP phone</td>
<td>Gateway 1 sends a SIP ACK to the Cisco SIP IP phone. The ACK confirms that User A has received the 486 Busy Here response. The call session attempt is now being terminated.</td>
</tr>
<tr>
<td>9.</td>
<td>Release Complete—Gateway 1 to PBX A</td>
<td>Gateway 1 sends a Release Complete message to PBX A and the call session attempt is terminated.</td>
</tr>
</tbody>
</table>
### Call Flow Scenarios for Failed Calls

#### Called User Does Not Answer

Figure B-22 illustrates an unsuccessful call in which User A initiates a call to User B but User B does not answer.

![Figure B-22 Called User Does Not Answer](image)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.  
  In the INVITE request:  
  - The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an e-mail address (user@host, where user is the telephone number and host is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as “INVITE sip:555-0002@companyb.com; user=phone.” The “user=phone” parameter distinguishes that the Request-URI address is a telephone number rather than a username.  
  - Cisco SIP IP phone A is identified as the call session initiator in the From field.  
  - A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.  
  - The transaction number within a single call leg is identified in the CSeq field.  
  - The media capability User A is ready to receive is specified. |
<p>| 2.   | 486 Busy Here—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a 486 Busy here message to the Cisco SIP IP phone A. The message indicates that Cisco SIP IP phone B is in use and the user is not willing or able to take additional calls. |
| 3.   | ACK—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP ACK to the Cisco SIP IP phone B. The ACK confirms that Cisco SIP IP phone A has received the 486 Busy Here response from Cisco SIP IP phone B. |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request:  
- The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an e-mail address (user@host, where user is the telephone number and host is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as “INVITE sip:555-0002@companyb.com; user=phone.” The “user=phone” parameter distinguishes that the Request-URI address is a telephone number rather than a username.  
- Cisco SIP IP phone A is identified as the call session initiator in the From field.  
- A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.  
- The transaction number within a single call leg is identified in the CSeq field.  
- The media capability User A is ready to receive is specified. |
| 2.   | 180 Ringing—Cisco SIP IP phone B to Cisco SIP IP phone A | Cisco SIP IP phone B sends a SIP 180 Ringing response to Cisco SIP IP phone A. |
| 3.   | CANCEL (Ring Timeout)—Cisco SIP IP phone A to Cisco SIP IP phone B | Cisco SIP IP phone A sends a CANCEL request to Cisco SIP IP phone B to cancel the invitation. |

**Authentication Error**

*Figure B-23* illustrates an unsuccessful call in which User A initiates a call to User B but is prompted for authentication credentials by the proxy server. User A’s SIP IP phone then reinitiates the call with an SIP INVITE request that includes its authentication credentials.
### Call Flow Scenarios for Failed Calls

#### Authentication Error

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | INVITE—Cisco SIP IP phone A to SIP proxy server | Cisco SIP IP phone A sends a SIP INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request:  
  - The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an e-mail address `(user@host, where user is the telephone number and host is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as “INVITE sip:555-0002@companyb.com; user=phone.” The “user=phone” parameter distinguishes that the Request-URI address is a telephone number rather than a username.
  - Cisco SIP IP phone A is identified as the call session initiator in the From field.
  - A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
  - The transaction number within a single call leg is identified in the CSeq field.
  - The media capability User A is ready to receive is specified. |
| 2.   | 407 Authentication Error—SIP proxy server to Cisco SIP IP phone A | SIP proxy server sends a SIP 407 Authentication Error response to Cisco SIP IP phone A. |
| 3.   | ACK—Cisco SIP IP phone A to SIP proxy server | Cisco SIP IP phone A sends a SIP ACK to the SIP proxy server acknowledging the 407 error message. |
| 4.   | Resend INVITE—Cisco SIP IP phone A to SIP proxy server | Cisco SIP IP phone A resends a SIP INVITE to the SIP proxy server with authentication credentials. |
Technical Specifications

The following sections describe the technical specifications for the Cisco SIP IP phone:

- Physical and Operating Environment Specifications, page C-1
- Cable Specifications, page C-2
- Regulatory Safety Compliance, page C-2
- Connections Specifications, page C-3

Physical and Operating Environment Specifications

The following table lists the physical and operating specifications of the Cisco SIP IP phone.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating temperature</td>
<td>32 to 104°F (0 to 40°C).</td>
</tr>
<tr>
<td>Operating relative humidity</td>
<td>10 to 95% (noncondensing).</td>
</tr>
<tr>
<td>Storage temperature</td>
<td>14 to 140°F (−10 to 60°C).</td>
</tr>
<tr>
<td>Height</td>
<td>8 in. (20.32 cm).</td>
</tr>
<tr>
<td>Width</td>
<td>10.5 in. (26.67 cm).</td>
</tr>
<tr>
<td>Depth</td>
<td>6 in. (15.24 cm).</td>
</tr>
<tr>
<td>Weight</td>
<td>3.5 lb (1.6 kg).</td>
</tr>
<tr>
<td>Power</td>
<td>100 to 240 VAC, 50 to 60 Hz, 0.5 A—when using the AC adapter.</td>
</tr>
<tr>
<td></td>
<td>48 VDC, 0.2 A—when using the in-line power over the network cable.</td>
</tr>
<tr>
<td>Cables</td>
<td>Two (2) pair of Category 3 for 10-Mbps cables.</td>
</tr>
<tr>
<td></td>
<td>Two (2) pair of Category 5 for 100-Mbps cables.</td>
</tr>
<tr>
<td>Distance Requirements</td>
<td>As supported by the Ethernet Specification, it is assumed that most phones</td>
</tr>
<tr>
<td></td>
<td>that are deployed in the field will be within 330 ft (100 m) of a phone closet.</td>
</tr>
</tbody>
</table>
Cable Specifications

The following cables are required to connect the Cisco SIP IP phone:

- RJ-11 for the handset connection.
- RJ-45 jack for the LAN connection (labeled “10/100 SW”).
- RJ-45 jack for a second 10BASE-T compliant connection (labeled “10/100 PC”).
- 48-volt power connector. The diameter of the center pin in the phone power jack (Switchcraft 712A) is 0.1 in (2.5 mm). The center pin is positive (+) voltage. The miniature power plug required to mate with the power jack on the phone is a Switchcraft 760 or equivalent.

Regulatory Safety Compliance

The Cisco IP Phone 7960, 7940, and 7910 meet the following regulatory safety and compliance approvals:

- CE Marking
- Safety
  - UL1950
  - CSA C22.2 No. 950
  - EN 60950
  - IEC 60950
  - AS/NZS 3260
  - TS001
- EMC
  - AS/NZS 3548 Class B
  - VCCI Class B
  - FCC (47 CFR) Part 15 Class B
  - EN 55022, Class B
- Telecom
  - IC CS-03
  - FCC (47 CFR) Part 68

Figure C-1 contains the FCC Class B Declaration for the Cisco IP Phone 7960, 7940, 7910, and 7910+SW.
Connections Specifications

The Cisco SIP IP phone has two RJ-45 ports that each support 10/100 Mbps half- or full-duplex connections to external devices—the network port and access port. You can use either Category 3 or 5 cabling for 10 Mbps connections, but use Category 5 for 100 Mbps connections. On both the LAN-to-phone port (left RJ-45 port facing the back of the phone) and PC-to-phone port (right port), use full-duplex to avoid collisions. Use the LAN-to-phone port to connect the phone to the network a LAN-to-phone jack. Use the PC-to-phone port to connect a network device, such as a computer, to the phone.

For a diagram identifying the different ports on the back of the Cisco SIP IP phone, see the “Installing the Cisco SIP IP Phone” section on page 2-2.
Translated Safety Warnings

This appendix contains in multiple languages the warnings that should be used with the “Getting Started with Your Cisco SIP IP Phone” chapter of this guide.

Installation Warning

⚠️ Warning

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

Waarschuwing Raadpleeg de installatie-aanwijzingen voordat u het systeem met de voeding verbindt.

Varoitus Lue asennusohjeet ennen järjestelmän yhdistämistä virtalähteesseen.

Attention Avant de brancher le système sur la source d'alimentation, consulter les directives d'installation.

Warnung Lesen Sie die Installationsanweisungen, bevor Sie das System an die Stromquelle anschließen.

Avvertenza Consultare le istruzioni di installazione prima di collegare il sistema all'alimentatore.

Advarsel Les installasjonsinstruksjonene før systemet kobles til strømkilden.

Aviso Leia as instruções de instalação antes de ligar o sistema à sua fonte de energia.

¡Advertencia! Ver las instrucciones de instalación antes de conectar el sistema a la red de alimentación.

Warning Läs installationsanvisningarna innan du kopplar systemet till dess strömförsörjningsenhet.

Product Disposal Warning

⚠️ Warning

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

Waarschuwing Dit produkt dient volgens alle landelijke wetten en voorschriften te worden afgedankt.

Varoitus Tämän tuotteen lopullisesta hävittämisestä tulee huolehtia kaikkia valtakunnallisia lakeja ja säännöksiä noudattaen.

Attention La mise au rebut définitive de ce produit doit être effectuée conformément à toutes les lois et réglementations en vigueur.

Warnung Dieses Produkt muß den geltenden Gesetzen und Vorschriften entsprechend entsorgt werden.
Lightning Activity Warning

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

**Waarschuwing** Tijdens onweer dat gepaard gaat met bliksem, dient u niet aan het systeem te werken of kabels aan te sluiten of teontkoppelen.

**Varoitus** Älä työskentele järjestelmän parissa äläkää yhdistää tai irrota kaapeleita ukkosilmalla.

**Attention** Ne pas travailler sur le système ni brancher ou débrancher les câbles pendant un orage du foudre.

**Warnung** Arbeiten Sie nicht am System und schließen Sie keine Kabel an bzw. trennen Sie keine ab, wenn es gewittert.

**Avvertenza** Non lavorare sul sistema o collegare oppure scollegare i cavi durante un temporale con fulmini.

**Advarsel** Utfør aldri arbeid på systemet, eller koble kabler til eller fra systemet når det tordner eller lyner.

**Aviso** Não trabalhe no sistema ou ligue e desligue cabos durante períodos de mau tempo (trovoada).

**¡Advertencia!** No operar el sistema ni conectar o desconectar cables durante el transcurso de descargas eléctricas en la atmósfera.

**Warning!** Vid åska skall du aldrig utföra arbete på systemet eller ansluta eller koppla loss kablar.

SELV Circuit Warning

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

**Waarschuwing** Om elektrische schokken te vermijden, mogen veiligheidscircuits met extra lage spanning (genaamd SELV = Safety Extra-Low Voltage) niet met telefoonnetwerkspanning (TNV) circuits verbonden worden. LAN (Lokaal netwerk) poorten bevatten SELV circuits en WAN (Regionaal netwerk) poorten bevatten TNV circuits. Sommige LAN en WAN poorten gebruiken allebei RJ-45 connectors. Ga voorzichtig te werk wanneer u kabels verbindt.
Circuit Breaker (15A) Warning

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

Varoitus  Tämä tuote on riippuvainen rakennukseen asennetusta oikosulkusuojauksesta (ylivirtasuojauksesta). Varmista, että vaihevirtajohtimissa (kaikissa virroitetuissa johtimissa) käytetään Yhdysvalloissa alle 120 voltin, 15 ampeerin ja monissa muissa maissa 240 voltin, 10 ampeerin sulaketta tai suojakytkintä.

Attention  Pour ce qui est de la protection contre les courts-circuits (surtension), ce produit dépend de l'installation électrique du local. Vérifier qu'un fusible ou qu'un disjoncteur de 120 V alt., 15 A U.S. maximum (240 V alt., 10 A international) est utilisé sur les conducteurs de phase (conducteurs de charge).


Avvertenza  Questo prodotto dipende dall’installazione dell’edificio per quanto riguarda la protezione contro cortocircuiti (sovracorrente). Verificare che un fusibile o interruttore automatico, non superiore a 120 VCA, 15 A U.S. (240 VCA, 10 A internazionale) sia stato usato nei fili di fase (tutti i conduttori portatori di corrente).

Advarsel  Dette produktet er avhengig av bygningens installasjoner av kortslutningsbeskyttelse (overstrøm). Kontroller at det brukes en sikring eller strømbyter som ikke er større enn 120 VAC, 15 A (USA) (240 VAC, 10 A internasjonalt) på faselederne (alle strømførende ledere).

Aviso  Este producto depende de las instalaciones existentes para protección contra cortocircuitos (sobrecarga). Asegúrese de que un fusible o disjuntor no superior a 240 VAC, 10A es utilizado nos condutores de fase (todos os condutores de transporte de corrente).

¡Advertencia!  Este equipo utiliza el sistema de protección contra cortocircuitos (o sobrecorrientes) deló propio edificio. Asegurarse de que se utiliza un fusible o interruptor automático de no más de 240 voltios en corriente alterna (VAC), 10 amperios del estándar internacional (120 VAC, 15 amperios del estándar USA) en los hilos de fase (todos aquéllos portadores de corriente).

Warning!  Denna produkt är beroende av i byggnaden installerat kortslutningsskydd (överströmsskydd). Kontrollera att säkring eller överspänningsskydd används på fasledarna (samtliga strömförande ledare) för internationellt bruk max. 240 V växelström, 10 A (i USA max. 120 V växelström, 15 A).
A

AAA Authentication, authorization, and accounting. AAA is a suite of network security services that provides the primary framework through which access control can be set up on your Cisco router or access server.

ANI Automatic number identification.

B

BTXML Basic telephony extensible markup language

C

CAS Channel-associated signaling.

CCAPI Call control applications programming interface.

CLI Command-line interface.

CO Central office.

CPE Customer premises equipment. Terminating equipment, such as terminals, telephones, and modems, supplied by the telephone company, installed at the customer sites, and connected to the telephone company network.

CSM Call switching module.

d

D

dial peer An addressable call endpoint. In Voice over IP (VoIP), there are two types of dial peers: POTS and VoIP.

DNS Domain Name System. Used to address translation to convert H.323 IDs, URLs, or e-mail IDs to IP addresses. DNS is also used to assist in the locating remote gatekeepers and to reverse-map raw IP addresses to host names of administrative domains.

DNIS Dialed number identification service (the called number)
### Glossary

**DSP**  
Digital signal processor.

**DTMF**  
Dual tone multifrequency.

---

**E**  
**E.164**  
The international public telecommunications numbering plan. A standard set by ITU-T which addresses telephone numbers.

**E&M**  
Ear and mouth RBS signaling.

**endpoint**  
A SIP terminal or gateway. An endpoint can call and be called. It generates and/or terminates the information stream.

---

**G**  
**gateway**  
A gateway allows SIP or H.323 terminals to communicate with terminals configured to other protocols by converting protocols. A gateway is the point where a circuit-switched call is encoded and repackaged into IP packets.

**H**  
**H.323**  
An International Telecommunication Union (ITU-T) standard that describes packet-based video, audio, and data conferencing. H.323 is an umbrella standard that describes the architecture of the conferencing system and refers to a set of other standards (H.245, H.225.0, and Q.931) to describe its actual protocol.

**H.323 RAS**  
Registration, admission, and status. The RAS signaling function performs registration, admissions, bandwidth changes, status and disengage procedures between the VoIP gateway and the gatekeeper.

---

**I**  
**IVR**  
Interactive voice response. When someone dials in, IVR responds with a prompt to get a personal identification number (PIN), and so on.

---

**L**  
**LEC**  
Local exchange carrier.

**location server**  
A SIP redirect or proxy server uses a location service to get information about a caller’s locations. Location services are offered by location servers.
M

MF  Multifrequency tones are made of six frequencies that provide 15 two frequency combinations for indication digits 0-9 and KP/ST signals.

multicast  A process of transmitting protocol data units (PDUs) from one source to many destinations. The actual mechanism (that is, IP multicast, multiunicast, and so forth) for this process might be different for LAN technologies.

multipoint-unicast  A process of transferring PDUs where an endpoint sends more than one copy of a media stream to different endpoints. This can be necessary in networks that do not support multicast.

N

node  A H.323 entity that uses RAS to communicate with the gatekeeper; for example, an endpoint such as a terminal, proxy, or gateway.

P

PDU  Protocol data units used by bridges to transfer connectivity information.

POTS  Plain old telephone service. Basic telephone service supplying standard single line telephones, telephone lines, and access to the PSTN.

proxy server  An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, possibly after translation, to other servers. A proxy interprets, and, if necessary, rewrites a request message before forwarding it.

PSTN  Public switched telephone network. PSTN refers to the local telephone company.

R

redirect server  A redirect server is a server that accepts a SIP request, maps the address into zero or more new addresses and returns these addresses to the client. It does not initiate its own SIP request nor accept calls.

registrar  A registrar is a server that accepts REGISTER requests. A registrar is typically colocated with a proxy or redirect server and may offer location services.

RAS  Registration, admission, and status protocol. This is the protocol that is used between endpoints and the gatekeeper to perform management functions.

RBS  Robbed-bit signaling.
**S**

**SIP**

Session Initiation Protocol. This is a protocol developed by the IETF MMUSIC Working Group as an alternative to H.323. SIP features are compliant with IETF RFC 2543, published in March 1999.

SIP equips platforms to signal the setup of voice and multimedia calls over IP networks.

**SPI**

Service provider interface.

---

**T**

**TDM**

Time-division multiplexing. Technique in which information from multiple channels can be allocated bandwidth on a single wire, based on preassigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit.

---

**U**

user agent

See **UAS**.

**UAC**

User agent client. A user agent client is a client application that initiates the SIP request.

**UAS**

User agent server (or user agent). A user agent server is a server application that contacts the user when a SIP request is received, then returns a response on behalf of the user. The response accepts, rejects, or redirects the request.

---

**V**

**VoIP**

Voice over IP. The ability to carry normal telephone-style voice over an IP-based Internet with POTs-like functionality, reliability, and voice quality. VoIP is a blanket term, that generally refers to the Cisco standards-based (for example H.323) approach to IP voice traffic.
Numerics

10/100 PC port 1-13
10/100 SW port 1-13
1xx responses A-2
2xx responses A-3
3xx responses A-3
4xx responses A-4
5xx responses A-6
6xx responses A-7

A

abbreviations, time zone 3-32
Accept-Encoding header field A-7
Accept header field A-7
Accept-Language header field A-7
accessing
  firmware version 3-36
  network statistics 4-8, 4-10
  status messages 4-8, 4-9
access port 1-13
address
  proxy server 3-27
  TFTP server 3-6
adjusting, phone placement 2-12
administrative VLAN ID parameter 3-4
Allow header field A-7
Also header field A-7
alternate TFTP server, enabling 3-4
authentication
  name, configuring 3-25
  services 1-3

Authorization header field A-7

B

basic telephony extensible markup language (BTXML) 1-5
billing services 1-3
book
  objectives x
  organization x
BTXML 1-5
buttons
  information 1-5
  line 1-4
  volume 1-5

C

cables
  connecting 2-11
  specifications C-2
Caller ID blocking 1-8
call flows B-1
  successful B-1
  unsuccessful B-52
call forward 1-8
call hold 1-8
Call-ID header field A-7
call preferences menu 3-6
call transfer 1-9
call waiting disabled 1-8
call waiting enabled 1-8
character support 1-10
circuit breaker (15A) warning  D-3
CiscoCallManager XML  1-5
clients  gateways  1-3
phones  1-3
SIP  1-3
codec, specifying  3-18, 3-29
common parameters  3-9
compliance information  A-1
configuration, erasing  3-5
configuration files
default  creating  2-5
example  3-22
modifying  3-9
guidelines  2-5
phone-specific  2-4, 2-7
creating  2-6
example  3-25
modifying  3-24
naming convention  2-5
SIPDefault.cnf  2-5
storing  2-5
configuration mode
entering into  3-2
locking  3-3
unlocking  3-2
configuring
lines
authentication name  3-25
name  3-25
password  3-25
short name  3-25
network parameters  2-9
manually  2-10
via DHCP  2-10
SIP parameters
manually  2-7
via TFTP  2-4
connections  1-12, 2-11
Contact header field  A-7
Content-Encoding header field  A-7
Content-Length header field  A-7
Content-Type header field  A-7
conventions, document  x
Cseq header field  A-7

collection
Date header field  A-7
daylight savings time  3-30
default configuration file
example  2-6, 3-22
guidelines  2-5
modifying  3-9
SIPDefault.cnf  2-3
default router parameters  3-4
DHCP
description  1-11
enabling  3-4
options
default IP gateway  2-10
DNS server  2-10
domain name  2-10
IP address  2-10
IP subnet mask  2-10
TFTP server  2-10
releasing address  3-4
server parameter  3-4
dialing pad  1-5
dial plans
example using # character  2-21
specifying secondary dial tone  2-21
directory services  1-3
DNS
description  1-11
server parameters  3-4
documentation
<table>
<thead>
<tr>
<th><strong>Index</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>conventions</td>
<td>x</td>
</tr>
<tr>
<td>related</td>
<td>xi</td>
</tr>
<tr>
<td>domain name parameter</td>
<td>3-4</td>
</tr>
<tr>
<td>Domain Name System (DNS)</td>
<td>1-11</td>
</tr>
<tr>
<td>do not disturb</td>
<td>1-8</td>
</tr>
<tr>
<td>downloading required files</td>
<td>2-3</td>
</tr>
<tr>
<td>DST</td>
<td>3-30</td>
</tr>
<tr>
<td>DTMF</td>
<td></td>
</tr>
<tr>
<td>DB level</td>
<td>3-13</td>
</tr>
<tr>
<td>inband</td>
<td>3-13</td>
</tr>
<tr>
<td>outofbound</td>
<td>3-14, 3-28</td>
</tr>
<tr>
<td>payload</td>
<td>3-13</td>
</tr>
<tr>
<td>dual booting</td>
<td>3-39</td>
</tr>
<tr>
<td>Dynamic Host Control Protocol (DHCP)</td>
<td>1-11</td>
</tr>
<tr>
<td>E</td>
<td></td>
</tr>
<tr>
<td>enabling</td>
<td></td>
</tr>
<tr>
<td>alternate TFTP server</td>
<td>3-4</td>
</tr>
<tr>
<td>DHCP</td>
<td>3-4</td>
</tr>
<tr>
<td>registration</td>
<td>3-19, 3-29</td>
</tr>
<tr>
<td>Encryption header field</td>
<td>A-7</td>
</tr>
<tr>
<td>endpoint, SIP</td>
<td>1-2</td>
</tr>
<tr>
<td>erasing</td>
<td></td>
</tr>
<tr>
<td>configuration</td>
<td>3-5</td>
</tr>
<tr>
<td>parameters</td>
<td>3-35</td>
</tr>
<tr>
<td>settings</td>
<td>3-35</td>
</tr>
<tr>
<td>example</td>
<td></td>
</tr>
<tr>
<td>default configuration file</td>
<td>3-22</td>
</tr>
<tr>
<td>phone-specific configuration file</td>
<td>3-25</td>
</tr>
<tr>
<td>Expires header field</td>
<td>A-7</td>
</tr>
<tr>
<td>F</td>
<td></td>
</tr>
<tr>
<td>features</td>
<td></td>
</tr>
<tr>
<td>call forward</td>
<td>1-8</td>
</tr>
<tr>
<td>call hold</td>
<td>1-8</td>
</tr>
<tr>
<td>call transfer</td>
<td>1-9</td>
</tr>
<tr>
<td>call waiting disabled</td>
<td>1-8</td>
</tr>
<tr>
<td>call waiting enabled</td>
<td>1-8</td>
</tr>
<tr>
<td>do not disturb</td>
<td>1-8</td>
</tr>
<tr>
<td>secondary directory number</td>
<td>1-8</td>
</tr>
<tr>
<td>URL dialing</td>
<td>1-8</td>
</tr>
<tr>
<td>file</td>
<td></td>
</tr>
<tr>
<td>default</td>
<td>3-22</td>
</tr>
<tr>
<td>phone-specific</td>
<td>3-25</td>
</tr>
<tr>
<td>files</td>
<td></td>
</tr>
<tr>
<td>audio</td>
<td>2-3</td>
</tr>
<tr>
<td>dual boot</td>
<td>2-3</td>
</tr>
<tr>
<td>firmware image</td>
<td>2-3</td>
</tr>
<tr>
<td>OS79XX.txt</td>
<td>2-3</td>
</tr>
<tr>
<td>RINGLIST.DAT</td>
<td>2-3</td>
</tr>
<tr>
<td>SIPDefault.cnf</td>
<td>2-3</td>
</tr>
<tr>
<td>firmware image</td>
<td>2-3</td>
</tr>
<tr>
<td>updating</td>
<td>3-37</td>
</tr>
<tr>
<td>version, viewing</td>
<td>3-36</td>
</tr>
<tr>
<td>footstand adjustment</td>
<td>1-4</td>
</tr>
<tr>
<td>From header field</td>
<td>A-7</td>
</tr>
<tr>
<td>functions</td>
<td></td>
</tr>
<tr>
<td>proxy server</td>
<td>A-1</td>
</tr>
<tr>
<td>redirect server</td>
<td>A-1</td>
</tr>
<tr>
<td>UAC</td>
<td>A-1</td>
</tr>
<tr>
<td>UAS</td>
<td>A-1</td>
</tr>
<tr>
<td>G</td>
<td></td>
</tr>
<tr>
<td>gateways</td>
<td>1-3</td>
</tr>
<tr>
<td>glossary</td>
<td>GL-1</td>
</tr>
<tr>
<td>guidelines</td>
<td>2-10</td>
</tr>
<tr>
<td>H</td>
<td></td>
</tr>
<tr>
<td>handset</td>
<td>1-5</td>
</tr>
<tr>
<td>header fields</td>
<td>A-7</td>
</tr>
<tr>
<td>headset</td>
<td></td>
</tr>
</tbody>
</table>
supported types 1-14
headset and speaker toggle 1-5
Hide header field A-7
host name parameter 3-5
HTTP proxy address parameter 3-5

K
keys
on-screen mode 1-5
scroll 1-5
soft 1-5

L
language support 1-10
LCD screen 1-4
line buttons 1-4
lines, configuring
  authentication name 3-25
  name 3-25
  password 3-25
  short name 3-25
linex_authname parameter 3-25
linex_name parameter 3-25
linex_password parameter 3-25
linex_shortname parameter 3-25
locking, configuration mode 3-3

M
MAC address parameter 3-5
Max-Forwards header field A-7
menu
  call preferences 3-6
messages, status 4-8, 4-9
messages URI parameter 3-28
Message Waiting Indication 1-8
methods
  ACK A-2
  BYE A-2
  CANCEL A-2
  INVITE A-2
  OPTIONS A-2
  REGISTER A-2
modifying
  network parameters 3-2, 3-3
  SIP parameters 3-9, 3-24
mute toggle 1-5

N
name, configuring 3-25
naming convention, phone-specific configuration file 2-5
NAT  3-16
  network  1-13
  parameters
    administrative VLAN ID  3-4
    alternate TFTP  3-4
    configuring via DHCP  2-10
    default router  3-4
    DHCP address release  3-4
    DHCP enable  3-4
    DHCP server  3-4
    domain name  3-4
    dynamic DNS server  3-5
    dynamic TFTP server  3-5
    erase configuration  3-5
    guidelines  2-10
    host name  3-5
    HTTP proxy address  3-5
    HTTP proxy port  3-5
    IP address  3-5
    MAC address  3-5
    operational VLAN ID  3-6
    subnet mask  3-6
    TFTP server  3-6
    port  1-13
  statistics  4-8, 4-10
  network address translation (NAT)  3-16, 3-28
  network connections  1-13

O
  on-screen mode keys  1-5
  operating environment specifications  C-1
  operational VLAN ID parameter  3-6
  Organization header field  A-7
  OS79XX.txt  2-3
  Out of Band DTMF parameter  3-28
  overview

Cisco SIP IP phone  1-4
  initialization process  2-1
  product  1-1
  SIP  1-2

P
  parameters
    common  2-5, 3-9
    configuring
      network  2-9
      SIP  2-4
    directory_url  1-5
    erasing  3-35
    logo_url  1-5
    nat_enable  3-16
    network  2-9
      administrative VLAN ID  3-4
      alternate TFTP  3-4
      default routers  3-4
      DHCP address release  3-4
      DHCP enable  3-4
      DHCP server  3-4
      DNS server  3-4
      domain name  3-4
      dynamic DNS server  3-5
      dynamic TFTP server  3-5
      erase configuration  3-5
      guidelines  2-10
      host name  3-5
      HTTP proxy address  3-5
      HTTP proxy port  3-5
      IP address  3-5
      MAC address  3-5
      modifying  3-2, 3-3
      operational VLAN ID  3-6
      subnet mask address  3-6
      TFTP server  3-6
      required  2-7
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>services_url</td>
<td>1-5</td>
</tr>
<tr>
<td>SIP</td>
<td></td>
</tr>
<tr>
<td>Authentication Name</td>
<td>3-27</td>
</tr>
<tr>
<td>Authentication Password</td>
<td>3-27</td>
</tr>
<tr>
<td>dtmf_avt_payload</td>
<td>3-13</td>
</tr>
<tr>
<td>dtmf_db_level</td>
<td>3-13</td>
</tr>
<tr>
<td>dtmf_outofbound</td>
<td>3-14</td>
</tr>
<tr>
<td>image_version</td>
<td>3-15</td>
</tr>
<tr>
<td>linex_authname</td>
<td>3-25</td>
</tr>
<tr>
<td>linex_name</td>
<td>3-25</td>
</tr>
<tr>
<td>linex_password</td>
<td>3-25</td>
</tr>
<tr>
<td>linex_shortname</td>
<td>3-25</td>
</tr>
<tr>
<td>Messages URI</td>
<td>3-28</td>
</tr>
<tr>
<td>Name</td>
<td>3-27</td>
</tr>
<tr>
<td>Out of Band DTMF</td>
<td>3-28</td>
</tr>
<tr>
<td>Prefered Codec</td>
<td>3-29</td>
</tr>
<tr>
<td>preferred_codec</td>
<td>3-18</td>
</tr>
<tr>
<td>proxy_register</td>
<td>3-19</td>
</tr>
<tr>
<td>proxy1_address</td>
<td>3-19</td>
</tr>
<tr>
<td>proxy1_port</td>
<td>3-19</td>
</tr>
<tr>
<td>Proxy Address</td>
<td>3-27</td>
</tr>
<tr>
<td>Proxy Port</td>
<td>3-28</td>
</tr>
<tr>
<td>Register Expires</td>
<td>3-29</td>
</tr>
<tr>
<td>Register with Proxy</td>
<td>3-29</td>
</tr>
<tr>
<td>required</td>
<td>2-6</td>
</tr>
<tr>
<td>Short Name</td>
<td>3-28</td>
</tr>
<tr>
<td>sip_invite_retx</td>
<td>3-20</td>
</tr>
<tr>
<td>sip_retx</td>
<td>3-20</td>
</tr>
<tr>
<td>telnet_enable</td>
<td>3-21</td>
</tr>
<tr>
<td>timer_invite_expires</td>
<td>3-21</td>
</tr>
<tr>
<td>timer_register_expires</td>
<td>3-21</td>
</tr>
<tr>
<td>timer_t1</td>
<td>3-21</td>
</tr>
<tr>
<td>timer_t2</td>
<td>3-21</td>
</tr>
<tr>
<td>tos_media</td>
<td>3-22</td>
</tr>
<tr>
<td>password</td>
<td></td>
</tr>
<tr>
<td>configuring</td>
<td>3-25</td>
</tr>
<tr>
<td>line</td>
<td>3-25</td>
</tr>
<tr>
<td>phone</td>
<td>3-9</td>
</tr>
<tr>
<td>adjusting placement</td>
<td>2-12</td>
</tr>
<tr>
<td>connecting</td>
<td>2-11</td>
</tr>
<tr>
<td>connections</td>
<td>1-12</td>
</tr>
<tr>
<td>access port</td>
<td>1-13</td>
</tr>
<tr>
<td>network</td>
<td>1-13</td>
</tr>
<tr>
<td>network port</td>
<td>1-13</td>
</tr>
<tr>
<td>features</td>
<td></td>
</tr>
<tr>
<td>dialing pad</td>
<td>1-5</td>
</tr>
<tr>
<td>footstand adjustment</td>
<td>1-4</td>
</tr>
<tr>
<td>handset</td>
<td>1-5</td>
</tr>
<tr>
<td>headset</td>
<td>1-14</td>
</tr>
<tr>
<td>headset and speaker toggle</td>
<td>1-5</td>
</tr>
<tr>
<td>information button</td>
<td>1-5</td>
</tr>
<tr>
<td>LCD screen</td>
<td>1-4</td>
</tr>
<tr>
<td>line buttons</td>
<td>1-4</td>
</tr>
<tr>
<td>mute toggle</td>
<td>1-5</td>
</tr>
<tr>
<td>on-screen mode keys</td>
<td>1-5</td>
</tr>
<tr>
<td>physical</td>
<td>1-4</td>
</tr>
<tr>
<td>scroll key</td>
<td>1-5</td>
</tr>
<tr>
<td>soft keys</td>
<td>1-5</td>
</tr>
<tr>
<td>volume buttons</td>
<td>1-5</td>
</tr>
<tr>
<td>installing</td>
<td>2-2</td>
</tr>
<tr>
<td>interfaces</td>
<td>1-4</td>
</tr>
<tr>
<td>mounting to wall</td>
<td>2-13</td>
</tr>
<tr>
<td>overview</td>
<td>1-4</td>
</tr>
<tr>
<td>prerequisites</td>
<td>1-12</td>
</tr>
<tr>
<td>secondary directory number</td>
<td>1-8</td>
</tr>
<tr>
<td>supported features</td>
<td>1-6</td>
</tr>
<tr>
<td>supported protocols</td>
<td>1-11</td>
</tr>
<tr>
<td>DHCP</td>
<td>1-11</td>
</tr>
<tr>
<td>DNS</td>
<td>1-11</td>
</tr>
<tr>
<td>ICMP</td>
<td>1-11</td>
</tr>
<tr>
<td>IP</td>
<td>1-11</td>
</tr>
<tr>
<td>RTP</td>
<td>1-11</td>
</tr>
<tr>
<td>SDP</td>
<td>1-11</td>
</tr>
<tr>
<td>SNTP</td>
<td>1-11</td>
</tr>
<tr>
<td>TCP</td>
<td>1-11</td>
</tr>
<tr>
<td>TFTP</td>
<td>1-12</td>
</tr>
<tr>
<td>UDP</td>
<td>1-12</td>
</tr>
<tr>
<td>URL dialing</td>
<td>1-8</td>
</tr>
</tbody>
</table>
verifying startup 2-14

phone-specific configuration file
creating 2-7
example 2-6, 3-25
modifying 3-24

physical specifications C-1

port
access 1-13
network 1-13
proxy server 3-28

power source
Cisco Catalyst switches 1-14
external 1-13
prerequisites 1-12

Priority header field A-7

product
overview 1-1
product disposal warning D-1

protocols 1-11
DHCP 1-11
DNS 1-11
ICMP 1-11
IP 1-11
RTP 1-11
SDP 1-11
SNTP 1-11
TCP 1-11
TFTP 1-12
UDP 1-12

Proxy-Authenticate header field A-7
Proxy-Authorization header field A-8

proxy port
specifying 3-19

Proxy-Required header field A-8
proxy server 1-3
address 3-27
port 3-28
registration, enabling 3-19, 3-29
specifying 3-19

R
Real-Time Transport Protocol (RTP) 1-11
Record-Route header field A-8
redirect server 1-4
registrar server 1-4
registration
enabling 3-19
timer 3-21, 3-29
related documentation xi
release, DHCP address 3-4
remote reboot 3-40
request methods B-1
Require header field A-8
resetting
network statistics 4-9, 4-10
Response-Key header field A-8
responses A-2
global (6xx) A-7
information (1xx) A-2
redirection (3xx) A-3
request failure (4xx) A-4
server failure (5xx) A-6
successful (2xx) A-3
retransmission timers 3-21

Retry-After header field A-8

RFC
2131 1-11
2543 1-4
3261 1-2
768 1-12
791 1-11
792 1-11
RINGLIST.DAT 2-3
Route header field A-8
RTP, description 1-11
safety warnings, translated 

circuit breaker (15A) warning 

installation warning 

lightning activity warning 

product disposal warning 

SELV circuit warning 

scroll key 

SDP, description 

SDP, usage 

secondary directory number 

SELV circuit warning 

server 

alternate TFTP 

proxy 

redirect 

registrar 

Server header field 

Session Description Protocol (SDP) 

settings, erasing 

short name, configuring 

Simple Network Time Protocol (SNTP) 

SIP 

architecture 

call flows 

successful 

unsuccessful 

clients 

gateways 

phones 

compliance information 

components 

UAC 

user agent server 

default configuration file, example 

dtmf_inband 

direct point 

functions 


gateways 

header fields 

IP phone, overview 

methods 

overview 

parameters 

Authentication Name 

Authentication Password 

configuring on your phone 

Message URI 

Name 

Out of Band DTMF 

phone-specific configuration file 

Preferred Codec 

Proxy Address 

Proxy Port 

Register Expires 

Register with proxy 

Short Name 

request methods 

responses 

servers 

proxy 

redirect 

registrar 

services 

authentication 

billing 

directory 

SIPDefault.cnf 

SIP parameters 

configuring on your phone
configuring via TFTP server 2-4
SNTP, description 1-11
soft keys 1-5
specifications C-1
cable C-2
connections C-3
operating environment C-1
physical C-1
specifying 3-15
codec 3-18, 3-29
DTMF level 3-13
DTMF payload 3-13
DTMF signaling 3-13, 3-14
image version 3-15
proxy port 3-19
proxy server 3-19
retransmission timers 3-21
TOS media 3-22
specifying out of bound 3-28
startup, verifying 2-14
statistics, network 4-8, 4-10
status information
accessing 3-36, 4-7, 4-8, 4-9, 4-10
Subject header field A-8
subnet mask parameter 3-6

TCP, description 1-11
technical specifications C-1
cable C-2
operating environment C-1
physical C-1
telnet_enable parameter 3-21
TFTP, description 1-12
TFTP server parameter 3-6
timer
registration 3-21, 3-29
retransmission 3-21
timer_t2 3-21
timers, retransmission 3-21
Timestamp header field A-8
time zone abbreviations 3-32
time zone setting
setting
time zone 3-30
toggle	headset and speaker 1-5
mute 1-5
To header field A-8
TOS media
specifying 3-22
traceroute command 4-7
translated safety warnings D-1
circuit breaker (15A) warning D-3
installation warning D-1
lightning activity warning D-2
product disposal warning D-1
SELV circuit warning D-2
Transmission Control Protocol (TCP) 1-11
Trivial File Transfer Protocol (TFTP) 1-12

U
UAC 1-2
UDP, description 1-12
unlocking, configuration mode 3-2
Unsupported header field A-8
updating
firmware 3-37
upgrade scenarios
release 5.0 and 5.1 3-38
release 5.0 and release 5.1 3-37
upgrading
from release 2.1 or earlier 3-39
from release 2.2 or later 3-38
URL dialing 1-8
user
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>agent server</td>
<td>1-2</td>
</tr>
<tr>
<td>User-Agent header field</td>
<td>A-8</td>
</tr>
<tr>
<td>User Datagram Protocol (UDP)</td>
<td>1-12</td>
</tr>
<tr>
<td>Verifying startup</td>
<td>2-14</td>
</tr>
<tr>
<td>Via header field</td>
<td>A-8</td>
</tr>
<tr>
<td>viewing firmware version</td>
<td>3-36</td>
</tr>
<tr>
<td>VLAN administrative</td>
<td>3-4</td>
</tr>
<tr>
<td>operational</td>
<td>3-6</td>
</tr>
<tr>
<td>volume</td>
<td></td>
</tr>
<tr>
<td>buttons</td>
<td>1-5</td>
</tr>
<tr>
<td>Wall mounting phone</td>
<td></td>
</tr>
<tr>
<td>Warning header field</td>
<td>A-8</td>
</tr>
<tr>
<td>what’s new in this release</td>
<td></td>
</tr>
<tr>
<td>release 5.0</td>
<td>1-1</td>
</tr>
<tr>
<td>release 5.1</td>
<td>1-1</td>
</tr>
<tr>
<td>what’s new in this release?</td>
<td>1-1</td>
</tr>
<tr>
<td>WWW-Authenticate header field</td>
<td>A-8</td>
</tr>
<tr>
<td>XML</td>
<td>1-5</td>
</tr>
</tbody>
</table>