



# **Cisco SIP IP Phone 7960 Administrator Guide**

Version 2.0

## **Corporate Headquarters**

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

Customer Order Number: DOC-7810497=  
Text Part Number: 78-10497-02

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

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

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

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

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

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

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

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

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

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

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

Access Registrar, AccessPath, Are You Ready, ATM Director, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, CiscoLink, the Cisco NetWorks logo, Cisco Powered Network logo, Cisco Systems Networking Academy, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, iQ Logo, iQ Readiness Scorecard, Kernel Proxy, MGX, Natural Network Viewer, Network Registrar, the Networkers logo, Packet, PIX, Point and Click Internetworking, Policy Builder, RateMUX, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, WebViewer, Workgroup Director, and Workgroup Stack are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Collision Free, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratum, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0010R)

*Cisco SIP IP Phone 7960 Administrator Guide*

Copyright © 2000, Cisco Systems, Inc.

All rights reserved.



## **About This Guide ix**

- Overview ix
- Who Should Use This Guide ix
- Objectives x
- Organization x
- Related Documentation xi
- Document Conventions xi
- Obtaining Documentation xv
  - World Wide Web xv
  - Documentation CD-ROM xv
  - Ordering Documentation xv
- Obtaining Technical Assistance xv
  - Cisco Connection Online xvi
  - Technical Assistance Center xvi
  - Documentation Feedback xvii

---

## **CHAPTER 1**

## **Product Overview 1-1**

- What is Session Initiation Protocol? 1-1
  - Components of SIP 1-3
    - SIP Clients 1-4
    - SIP Servers 1-5

- What is the Cisco SIP IP Phone 7960? 1-5
  - Supported Features 1-7
  - Supported Protocols 1-10
- Prerequisites 1-12
- Cisco SIP IP Phone Connections 1-13
  - Connecting to the Network 1-13
  - Connecting to Power 1-14
  - Using a Headset 1-15
- The Cisco SIP IP Phone with a Catalyst Switch 1-16

---

**CHAPTER 2**

**Getting Started with Your Cisco SIP IP Phone 2-1**

- Initialization Process Overview 2-1
- Installing the Cisco SIP IP Phone 2-3
  - Installation Task Summary 2-3
  - Downloading Files to Your TFTP Server 2-4
- Configuring SIP Parameters 2-5
  - Configuring SIP Parameters via a TFTP Server 2-6
  - Manually Configuring the SIP Parameters 2-11
- Configuring Network Parameters 2-13
  - Configuring Network Parameters via a DHCP Server 2-14
  - Manually Configuring the Network Parameters 2-14
- Connecting the Phone 2-16
  - Adjusting the Placement of the Cisco SIP Phone 2-18
- Verifying Startup 2-20

Using the Cisco SIP IP Phone Menu Interface	2-21
Reading the Cisco SIP IP Phone Icons	2-22
Customizing the Cisco SIP IP Phone Ring Types	2-24
Creating Dial Plans	2-24

---

**CHAPTER 3****Managing Cisco SIP IP Phones 3-1**

Entering Configuration Mode	3-1
Unlocking Configuration Mode	3-2
Locking Configuration Mode	3-2
Modifying the Phone's Network Settings	3-2
Modifying the Phone's SIP Settings	3-5
Modifying SIP Parameters via a TFTP Server	3-8
Modifying the Default SIP Configuration File	3-8
Modifying the Phone-Specific SIP Configuration File	3-15
Modifying the SIP Parameters Manually	3-18
Setting the Date, Time, and Daylight Savings Time	3-22
Erasing the Locally-Defined Settings	3-28
Erasing the Locally-Defined Network Settings	3-28
Erasing the Locally-Defined SIP Settings	3-29
Accessing Status Information	3-30
Viewing Status Messages	3-31
Viewing Network Statistics	3-31
Viewing the Firmware Version	3-33
Upgrading the Cisco SIP IP Phone Firmware	3-33
Performing an Image Upgrade and Remote Reboot	3-35

---

**APPENDIX A**

**SIP Compliance with RFC-2543 Information A-1**

SIP Functions A-2

SIP Methods A-2

SIP Responses A-3

1xx Response— Information Responses A-4

2xx Response— Successful Responses A-4

3xx Response— Redirection Responses A-5

4xx Response— Request Failure Responses A-5

5xx Response— Server Failure Responses A-10

6xx Response— Global Responses A-10

SIP Header Fields A-10

SIP Session Description Protocol (SDP) Usage A-12

---

**APPENDIX B**

**SIP Call Flows B-1**

Call Flow Scenarios for Successful Calls B-2

Gateway-to-Cisco SIP IP Phone— Successful Call Setup and Disconnect B-3

Gateway-to-Cisco SIP IP Phone— Successful Call Setup and Call Hold B-7

Gateway-to-Cisco SIP IP Phone— Successful Call Setup and Call  
Transfer B-11

Cisco SIP IP Phone-to-Cisco SIP IP Phone Simple Call Hold B-16

Cisco SIP IP Phone-to-Cisco SIP IP Phone Call Hold with Consultation B-20

Cisco SIP IP Phone-to-Cisco SIP IP Phone Call Waiting B-25

Cisco SIP IP Phone-to-Cisco SIP IP Phone Call Transfer without  
Consultation B-31

Cisco SIP IP Phone-to-Cisco SIP IP Phone Call Transfer with  
Consultation B-35

Cisco SIP IP Phone-to-Cisco SIP IP Phone Network Call Forwarding  
(Unconditional) B-41

Cisco SIP IP Phone-to-Cisco SIP IP Phone Network Call Forwarding (Busy) **B-44**

Cisco SIP IP Phone-to-Cisco SIP IP Phone Network Call Forwarding (No Answer) **B-48**

Cisco SIP IP Phone-to-Cisco SIP IP Phone 3-Way Calling **B-52**

Call Flow Scenarios for Failed Calls **B-58**

Gateway-to-Cisco SIP IP Phone— Called User is Busy **B-58**

Gateway-to-Cisco SIP IP Phone— Called User Does Not Answer **B-60**

Gateway-to-Cisco SIP IP Phone— Client, Server, or Global Error **B-63**

Cisco SIP IP Phone-to-Cisco SIP IP Phone— Called User is Busy **B-66**

Cisco SIP IP Phone-to-Cisco SIP IP Phone— Called User Does Not Answer **B-68**

Cisco SIP IP Phone-to-Cisco SIP IP Phone— Authentication Error **B-70**

---

**APPENDIX C****Technical Specifications C-1**

Physical and Operating Environment Specifications **C-1**

Cable Specifications **C-3**

Connections Specifications **C-3**

---

**APPENDIX D****Translated Safety Warnings D-1**

Installation Warning **D-1**

Product Disposal Warning **D-2**

Lightning Activity Warning **D-3**

SELV Circuit Warning (other versions available) **D-4**

Circuit Breaker (15A) Warning **D-6**







## About This Guide

---

### Overview

The *Cisco Session Initiation Protocol (SIP) IP Phone 7960 Administrator Guide* provides information about how to setup, connect cables to, and configure a Cisco SIP IP phone 7960 (hereafter referred to as a Cisco SIP IP phone). The administrator guide 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 telecommunication engineers should use this guide to learn the steps required to properly set up the Cisco SIP IP phone on the network.

The tasks described are considered to be administration-level tasks and are not intended for end-users of the phones. Many of the tasks involve configuring network settings which could affect the phone's ability to function in the network and require an understanding of IP networking and telephony concepts.

# Objectives

The *Cisco SIP IP Phone 7960 Administrator Guide* 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.

# Organization

This administrator guide is divided into the following chapters and appendixes:

- 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’s network and SIP settings, how to access network and call status information, and how to upgrade the firmware.
- Appendix A, “SIP Compliance with RFC-2543 Information” provides reference information about the SIP IP phone compliance to RFC 2543.
- Appendix B, “SIP Call Flows” provides reference information about the 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 SIP IP phone.

## 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*
- *Session Initiation for VoIP on Cisco Access Platforms*
- *Getting Started with the Cisco IP Phone 7960*
- *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:

- *Service Provider Features for Voice over IP* (introduced in Cisco IOS Release 12.0(3)T)
- *Cisco IOS IP and IP Routing Configuration Guide*
- *Cisco IOS Release 12.1 Multiservice Applications Configuration Guide*
- *Voice over IP for the Cisco 2600 and Cisco 3600 Series Routers*
- *Voice over IP for the Cisco AS5300 Documents*

## 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.
- 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 the system displays are in `screen` font.
- Information you must enter is in **boldface screen** font.

Notes use the following conventions:

**Note**

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

Cautions use the following conventions:

**Caution**

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

Warnings use the following conventions:

**Warning**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix, “Translated Safety Warnings.”)

**Waarschuwing**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel “Translated Safety Warnings” (Vertalingen van veiligheidsvoorschriften) raadplegen.)

Varoitus	Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)
Attention	Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).
Warnung	Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)
Avvertenza	Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).

<b>Advarsel</b>	Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)
<b>Aviso</b>	Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").
<b>Advertencia</b>	Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")
<b>Varning!</b>	Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)

# Obtaining Documentation

## World Wide Web

You can access the most current Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

## Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

## Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at <http://www.cisco.com/cgi-bin/subcat/kaojump.cgi>.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

# Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

## Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: [www.cisco.com](http://www.cisco.com)
- Telnet: [cco.cisco.com](http://cco.cisco.com)
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to [cco-team@cisco.com](mailto:cco-team@cisco.com).

## Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.



To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use [www.cisco.com/techsupport](http://www.cisco.com/techsupport).

To contact by e-mail, use one of the following:

Language	E-mail Address
English	<a href="mailto:tac@cisco.com">tac@cisco.com</a>
Hanzi (Chinese)	<a href="mailto:chinese-tac@cisco.com">chinese-tac@cisco.com</a>
Kanji (Japanese)	<a href="mailto:japan-tac@cisco.com">japan-tac@cisco.com</a>
Hangul (Korean)	<a href="mailto:korea-tac@cisco.com">korea-tac@cisco.com</a>
Spanish	<a href="mailto:tac@cisco.com">tac@cisco.com</a>
Thai	<a href="mailto:thai-tac@cisco.com">thai-tac@cisco.com</a>

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

## Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.  
Document Resource Connection  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate and value your comments.





## Product Overview

---

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

- What is Session Initiation Protocol?, page 1-1
- What is the Cisco SIP IP Phone 7960?, page 1-5
- Prerequisites, page 1-12
- Cisco SIP IP Phone Connections, page 1-13
- The Cisco SIP IP Phone with a Catalyst Switch, page 1-16

## What is Session Initiation Protocol?

Session Initiation Protocol (SIP) is the Internet Engineering Task Force's (IETF's) standard for multimedia conferencing over IP. SIP is an ASCII-based, application-layer control protocol (defined in RFC 2543) that can be used to establish, maintain, and terminate calls between two or more end points.

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:

- Determine the location of the target end point—SIP supports address resolution, name mapping, and call redirection.
- Determine the media capabilities of the target end point—Via Session Description Protocol (SDP), SIP determines the “lowest level” of common services between the end points. Conferences are established using only the media capabilities that can be supported by all end points.
- Determine the availability of the target end point—If a call cannot be completed because the target end point 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 indicating why the target end point was unavailable.
- Establish a session between the originating and target end point—If the call can be completed, SIP establishes a session between the end points. SIP also supports mid-call changes, such as the addition of another end point 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 end point to another. During a call transfer, SIP simply establishes a session between the transferee and a new end point (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 end points. 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 end point 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.

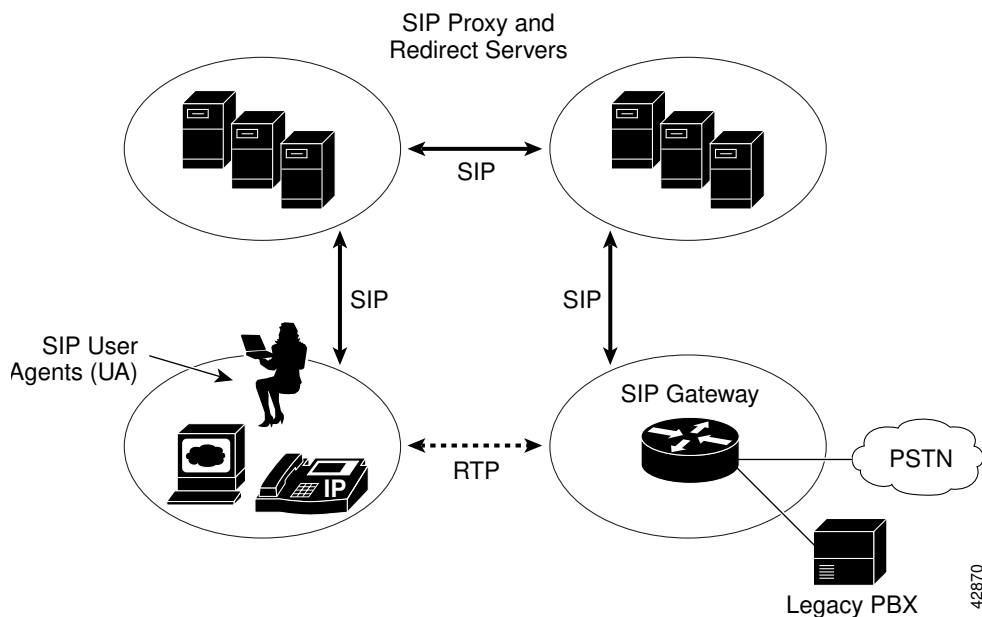
**Note**

---

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

SIP clients include:

- **Phones**—Can act 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**—Provide 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

SIP servers include:

- **Proxy server**—The proxy server is an intermediate device that receives SIP requests from a client and then forwards the requests on the client's behalf. 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.
- **Redirect server**—Receives SIP requests, strips out the address in the request, checks its address tables for any other addresses that may be mapped to the one in the request, and then returns the results of the address mapping to the client. Basically, redirect servers provide the client with information about the next hop or hops that a message should take and then the client contacts the next hop server or UAS directly.
- **Registrar server**—Processes requests from UACs for registration of their current location. Registrar servers are often co-located with a redirect or proxy server.

## What is the Cisco SIP IP Phone 7960?

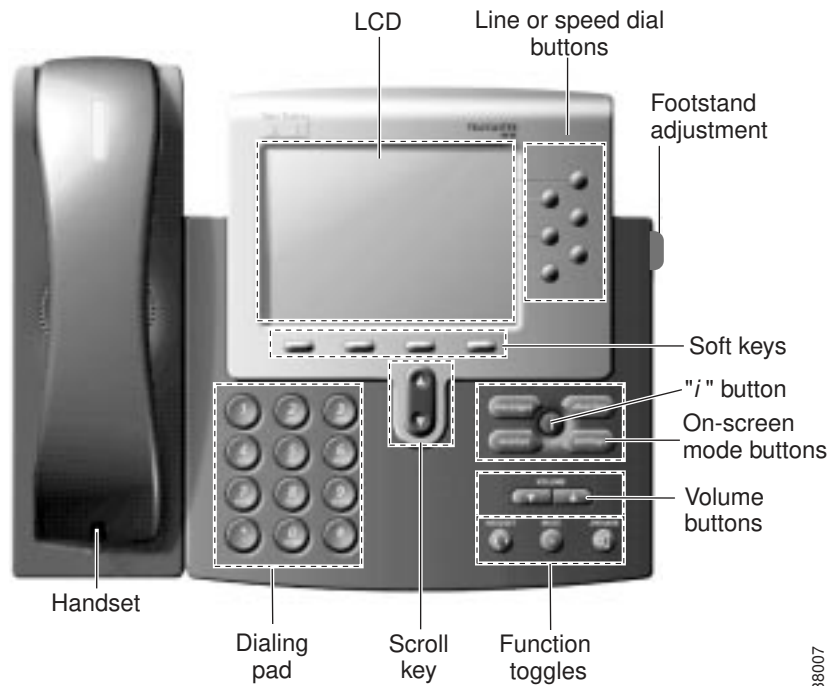
Cisco SIP IP phones 7960s (hereafter referred to as Cisco SIP IP phones) are full-featured telephones that can be plugged directly into an IP network and used very much like a standard private branch exchange (PBX) telephone. The Cisco SIP IP phone is an IP telephony instrument that can be used in VoIP networks.

The Cisco SIP IP phone model terminals can attach to the existing in place data network infrastructure, via 10BaseT/100BaseT 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/PBX.

The Cisco SIP IP phone complies with RFC 2543.

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

**Figure 1-2 Cisco SIP IP Phone Physical Features**



- LCD screen—Desktop which displays information about your Cisco SIP IP phone, such as the time, date, your phone number, caller ID, line/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.
- 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. This feature will be available in a future release.



- 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, ringer and adjusts the brightness contrast settings on the LCD screen.
- Function toggles—Includes these 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 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, answer a call, and so on.

## Supported Features

In addition to the physical features illustrated in Figure 1-2, the Cisco SIP IP phone also provides the following:

- An adjustable ring tone
- A hearing-aid compatible handset
- Headset compatibility
- An integrated two-port Ethernet switch that allows the telephone and a computer to share a single Ethernet jack
- A direct connection to a 10BaseT or 100BaseT Ethernet (RJ-45) network (half- or full-duplex connections are supported)
- A large (4.25 x 3 in.) display with adjustable contrast
- G.711 (u-law and a-law) and G.729a audio compression
- IP address assignment—Dynamic Host Configuration Protocol (DHCP) client or manually configured via a local setup menu

- Ability to:
  - Configure Ethernet port mode and speed
  - Register with or unregister from a 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
- 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 or remote (using the SIP 183 Ringing message) call progress tone
- AVT payload type negotiation
- Network startup via DHCP and Trivial File Transfer Protocol (TFTP)
- Dial plan support that enables automatic dialing and automatic generation of a secondary dial tone
- Current date and time support via Simple Network Time Protocol (SNTP) and time zone and daylight savings time support
- Call redirection information support via the CC-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
- 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 based on their usage and age. The oldest entry 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 voicemail server.
- Speed dial to voicemail via the messages button
- Remote reset support (via the Event header in NOTIFY messages)
- The following 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 2-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 2-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” 3-way call. When a 3-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.
  - 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—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.

- 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 email address instead of a phone number.
- Caller ID blocking—Allows the user to instruct the system to block their phone number or email 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.

**Note**

For information on how to use the standard telephony features and URL dialing, refer to the *Getting Started Cisco IP Phone 7960* and *Quick Reference Cisco IP Phone 7960* documents that shipped with the phone.

## Supported Protocols

The Cisco SIP IP phone supports the following standard protocols:

- Domain Name System (DNS)

DNS is used in the Internet for translating names of network nodes into addresses. SIP uses DNS to resolve the host names of end points to IP addresses.

- Dynamic Host Control Protocol (DHCP)

DHCP is 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)

ICMP is 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 supports ICMP as it is documented in RFC 792.

- Internet Protocol (IP)

IP is 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)

RTP transports real-time data (such as voice data) over data networks. RTP also the ability to obtain Quality of Service (QoS) information.

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

- Session Description Protocol (SDP)

SDP is 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)

SNTP synchronizes computer clocks on an IP network. The Cisco SIP IP phones use SNTP for their date and time support.

- Trivial File Transfer Protocol (TFTP)

TFTP allows files to be transferred from one computer to another over a network.

The Cisco SIP IP phone uses TFTP to download configuration files and software updates.

- User Datagram Protocol (UDP)

UDP is a simple protocol that exchanges data packets without acknowledgments or guaranteed delivery. SIP can use UDP as the underlying transport protocol. If UDP is used, retransmissions are used to ensure reliability.

The Cisco SIP IP phone supports UDP as it is defined in RFC 768 for SIP signaling.

## 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 *Cisco IOS IP and IP Routing Configuration Guide*.

- VoIP is configured on your Cisco routers.

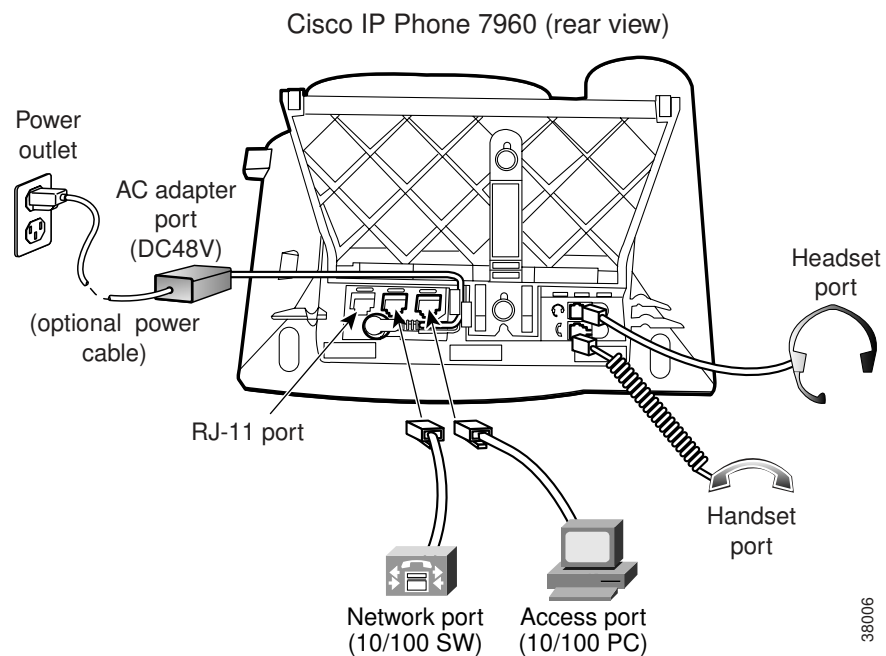
For more information about configuring VoIP, refer to the *Cisco IOS Release 12.1 Multiservice Applications Configuration Guide* for the appropriate access platform. For more information about configuring SIP VoIP, refer to the *Enhancements to SIP for VoIP on Cisco Access Platforms*.

- 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.

**Figure 1-3 Cisco SIP IP Phone Cable Connections**



## 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—network port (labeled 10/100 SW) and access port (labeled 10/100 PC). You can use either Category 3 or 5 cabling for 10 Mbps connections, but use Category 5 for 100 Mbps connections. On both the network port and 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 Cisco Catalyst switch over this connection. See the “Connecting to Power” section on page 1-14 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 adaptor 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 10/100BaseTX switching module.

This module sends power on pins 1 & 2 and 3 & 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 10/100BaseTX 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 -48V DC power shelf common equipment for the Catalyst 4006 with two AC-to-DC PSUs and one empty bay for redundant option and the 110V 15A AC-to-48V DC 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 Cisco Catalyst switches.

---

For redundancy, you can use the Cisco AC adapter even if you are using inline power from the Cisco 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 un-powered Cisco SIP IP phone to the network. After the phone powers up, connect the external power supply to the phone.

## 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 will 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. For information on ordering compatible headsets and coil cords for the Cisco IP phone 7960, see <http://cisco.getheadsets.com>.

---

## 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 the 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 these 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:

- 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 more information, refer to the documentation included with the Cisco Catalyst switch.



## 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.

This chapter provides the following major sections:

- Initialization Process Overview, page 2-1
- Installing the Cisco SIP IP Phone, page 2-3
- Verifying Startup, page 2-20
- Using the Cisco SIP IP Phone Menu Interface, page 2-21
- Reading the Cisco SIP IP Phone Icons, page 2-22
- Customizing the Cisco SIP IP Phone Ring Types, page 2-24
- Creating Dial Plans, page 2-24

### Initialization Process Overview

The initialization process of the Cisco SIP IP phone is responsible for establishing network connectivity and for making 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 non-volatile 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 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, then the phone will use IP settings that are stored in Flash memory.

4. The TFTP server is contacted.

On the TFTP server is the latest Cisco SIP IP phone firmware image and the dual boot file (OS79XX.TXT) that enables the phone to automatically determine and initialize for 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 will use 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, you must complete the following tasks:

1. Download the required files from CCO to the TFTP server as described in the the “Downloading Files to Your TFTP Server” section on page 2-4.
2. If you are configuring SIP parameters via a TFTP server, create and store the configuration files as described in the “Configuring SIP Parameters via a TFTP Server” section on page 2-6.
3. If you are using DHCP to configure the phones’ network settings, configure the required network parameters on your DHCP server as described in the “Configuring Network Parameters via a DHCP Server” section on page 2-14.
4. Connect the phone to the network and to a power supply as described in the “Connecting the Phone” section on page 2-16.
5. If you are not using DHCP to configure network parameters, manually configure the required network parameters as described in the “Manually Configuring the Network Parameters” section on page 2-14.
6. If you are not configuring the SIP parameters via a TFTP server, manually configure the required parameters as described in the “Manually Configuring the SIP Parameters” section on page 2-11.

## Downloading Files to Your TFTP Server

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

File	Description
OS79XX.TXT	(Required) Enables the phone to automatically determine and initialize for the VoIP environment in which it is being installed.  After downloading this file, you will need to use an ASCII editor to open it and specify the file name (without the file extension) of the image version that you plan to run on your phones.
SIPDefaultGeneric.cnf	(Optional) 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 2-7.
SIPConfigGeneric.cnf	(Required) File which 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.
RINGLIST.DAT	(Optional) 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 2-24.
POS3xxyy.bin (where xx is the version number and yy is the subversion number)	(Required) The Cisco SIP IP phone firmware image.
dialplan.xml	(Optional) North American example dial plan.
syncinfo.xml	(Optional) Controls the image version and associated sync value to be used for remote reboots.

## 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 Phone’s SIP Settings” section on page 3-5.

The SIP parameters are those parameters that a Cisco SIP IP phone needs 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 will override the values stored in Flash memory.
- Parameters defined in the phone-specific configuration file will override the values specified in the default configuration file.
- Parameters entered locally will be 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 via a TFTP Server

If you are configuring SIP parameters via 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 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, 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 manually configured. 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) will override those parameters stored in Flash memory. Parameters specified in a phone-specific configuration file will override those stored in Flash memory and parameters specified in the default configuration file.
- The name of each phones' phone-specific configuration file is unique and is based on the MAC address of the phone.

The format of the file name must be "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 lower case (for example, SIP00503EFFF842.cnf).

**Note**

The MAC address of a phone is identified on the middle sticker adhered to the base of the phone and can also be viewed on the Network Configuration menu.



- 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 have as much 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 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).

### Creating the Default SIP Configuration File

In the default configuration file (SIPDefault.cnf), we recommend 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, will the phones be required to register with a proxy server and which codec will the phones 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 CCO to the root directory of your TFTP server.
- Review the guidelines and restrictions documented in the “Configuration File Guidelines” section on page 2-6.
- For a complete list of the SIP parameters that you can configure, see the “Modifying the Phone’s SIP Settings” section on page 3-5.

**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 file name because the version is also built into the file header. Trying to change the image version by changing the file name will cause the firmware to fail when it compares the version in the header against the file name.
  - **proxy1\_address**—(Required) IP address of the primary SIP proxy server that will be used by the phones. Enter this address in IP dotted-decimal notation.
  - **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 file name, SIPDefault.cnf, to the root directory of your TFTP server.
-

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

```
; sip default configuration file

#Image Version
image_version:POS3xxyy ;

#Proxy server address
proxyl_address: 192.168.1.1 ;

#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 and restrictions documented in the “Configuration File Guidelines” section on page 2-6.
- Line parameters (those identified as `linex`) define a line on the phone. If you configure a line to use an e-mail address, that line can be called only using an e-mail address. Similarly, if you configure a line to use a number, that line can only be called 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 Phone’s SIP Settings” section on page 3-5.

### 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):
- **linex\_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.
  - **linex\_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 **linex\_authname** parameter when registration is enabled, the default name is used. The default name is UNPROVISIONED.
  - **linex\_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 **linex\_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 a subdirectory containing all the phone-specific configuration files). Name the file “SIPXXXXXXXXXXXX.cnf” where XXXXXXXXXXXXXXX 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, SIP00503EFFF842.cnf).
- 

The following is an example of a configuration file:

```
; phone-specific configuration file sample
; 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
```

## Manually Configuring the SIP Parameters

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 2-16.

### Before You Begin

- Connect your phone as described in the “Connecting the Phone” section on page 2-16.
- 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 2-21.
- When configuring the Preferred Codec and Out of Band DTMF parameters, press the **Change** soft key until the option 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 3-2.
- For a complete list of the SIP parameters that you can configure, see the “Modifying the Phone’s SIP Settings” section on page 3-5.

### Procedure

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Press the <b>settings</b> key. The Settings menu is displayed.                |
| <b>Step 2</b> | Highlight <b>SIP Configuration</b> . The SIP Configuration menu is displayed. |
| <b>Step 3</b> | Highlight <b>Line 1 Settings</b> .  |
| <b>Step 4</b> | Press the <b>Select</b> soft key. The Line 1 Configuration menu is displayed. |

- Step 5** Highlight and press the **Select** soft key to configure the following parameters:
- **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.
  - **Authentication Name**—(Required when registration is enabled) 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 *SIPmacaddress* where *macaddress* is the MAC address of the phone.
  - **Authentication Password**—(Required when registration is enabled) 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 *SIPmacaddress* where *macaddress* is the MAC address of the phone.
  - **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.
- 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.
- 

**Caution**

When you have completed your changes, ensure that you lock the phone as described in the “Locking Configuration Mode” section on page 3-2.

## Configuring Network Parameters

**Note**

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 Phone’s Network Settings” section on page 3-2.

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

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

- Phone's 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

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 non-zero 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 via 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)

## Manually Configuring the Network Parameters

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 2-16.
- 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 2-21.



- When configuring a domain name:
  - Press the **Number** soft key if entering 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 lower case “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.
- After making your changes, relock configuration mode as described in the “Locking Configuration Mode” section on page 3-2.
- For a complete list of the SIP parameters that you can configure, see the “Modifying the Phone’s Network Settings” section on page 3-2.

#### Procedure

- 
- Step 1** Press the **settings** key. The Settings menu is displayed.
- Step 2** Highlight **Network Configuration**.
- Step 3** Press the **Select** soft key. The Network Configuration menu is displayed.
- Step 4** Highlight **DHCP Enabled**.
- Step 5** Press the **No** soft key. DHCP is now disabled.
- Step 6** Highlight and configured 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 will attempt 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 result names to IP addresses. The phone will attempt to use DNS Servers 2 through 5 if DNS Server 1 is unavailable.

**Step 7** When done, press the **Save** soft key. The phone programs the new information into Flash memory and resets.

---

**Caution**

---

When you have completed your changes, ensure that you lock the phone as described in the “Locking Configuration Mode” section on page 3-2.

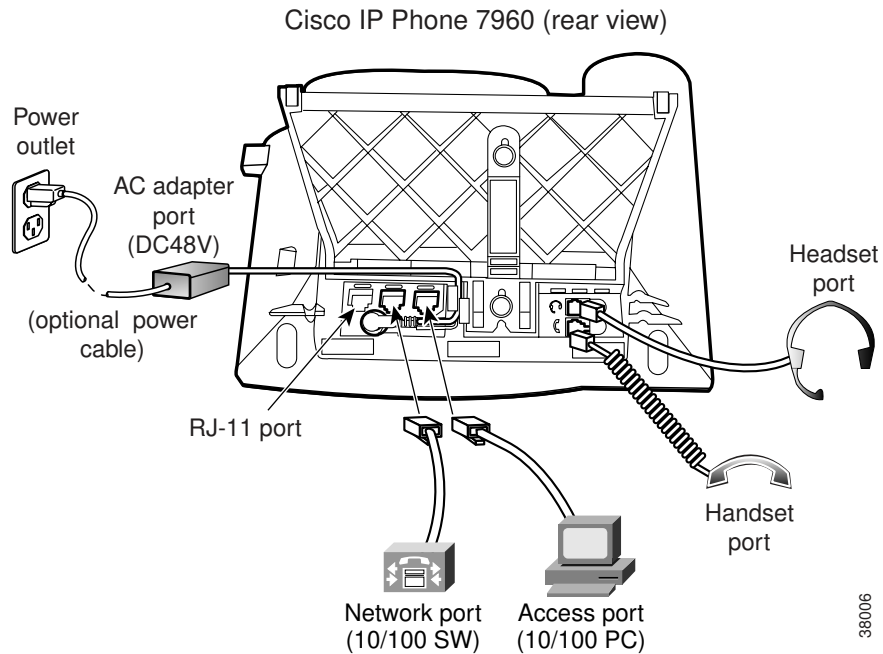
---

## 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****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 “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 “Using a Headset” section on page 1-15 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 “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 “Connecting to Power” section on page 1-14 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 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.

To adjust the phone placement on the desktop:

- 
- Step 1** Push in the footstand adjustment knob.
- Step 2** Adjust the footstand to its desired height and release the knob.
- 

### 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:

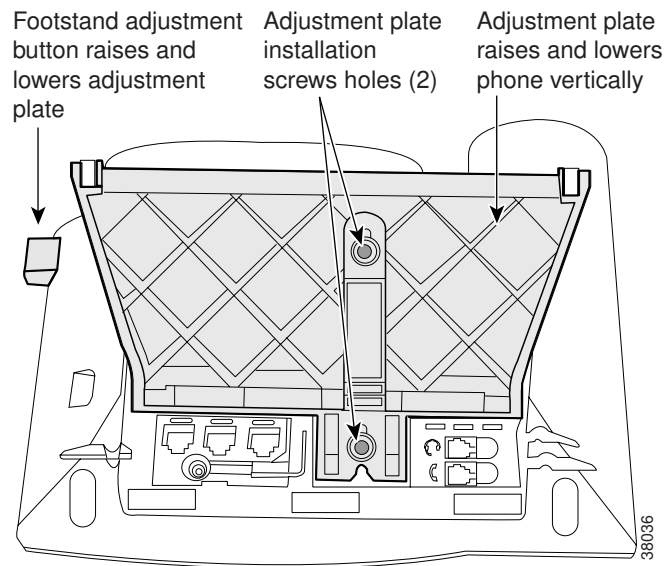
- Screwdriver
- Screws to secure the Cisco SIP IP phone to the wall
- Refer to Figure 2-1 for a graphical overview of these procedures.

**Procedure**

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

**Figure 2-2 Adjusting the Footstand**

Cisco IP Phone 7960 (rear view)



## Verifying Startup

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

1. These buttons flash on and off in sequence:
  - Headset
  - Mute
  - Speaker
2. The Cisco Systems, Inc. copyright displays on the LCD.

3. These messages display as 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 will automatically reboot to run the new image.
4. The main LCD screen appears displaying:
  - 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 an SIP IP address or ID parameter:
  - Press the **Number** soft key if entering 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 lower case “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 an 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 1 lists and describes each icon that you might see while using the Cisco SIP IP phone.

**Table 1** Cisco SIP IP Phone User Interface Icon Meanings

Icon	Meaning
	The Cisco IP phone 7960 that you are using is running SIP.
	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.



**Table 1** Cisco SIP IP Phone User Interface Icon Meanings (continued)

Icon	Meaning
	<p>The line is configured for E.164 number dialing and 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.</p> <p>You can change to URL dialing at any time while dialing on a line by pressing the <b>more</b> soft key and then the <b>URL</b> soft key.</p> <p>The character “x” displayed to the right of the icon indicates that registration has failed.</p>
	<p>The line is configured for URL dialing and you can enter both numbers and letters when placing the call.</p> <p>The character “x” displayed to the right of the icon indicates that registration has failed.</p>
	<p>The line is configured for URL dialing and ready for you to place the call. When a line is configured for URL dialing, you can enter both numbers and letters when placing the call.</p> <p>You can change to E.164 number dialing at any time while dialing on a line by pressing the <b>more</b> soft key and then the <b>Number</b> soft key.</p> <p>The character “x” displayed to the right of the icon indicates that registration has failed.</p>
	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 configure mode is unlocked. When the phone is unlocked, the phone’s network or SIP settings can be modified.

## 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 the 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 comply with the following format guidelines:
- 8000 Hz sampling rate
  - 8 bits per sample
  - ulaw compression
- Step 2** Using a ASCII editor, open the RINGLIST.DAT file and for each of the ring types you are adding, specify the name as you want it to display 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 1    ringer1.pcm
```
- Step 3** After defining pointers for each of the ring types 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 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.

**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 each on a separate line:

```
<TEMPLATE MATCH="pattern" Timeout="sec" User="type" Rewrite="altstrng"
```

Where:

- `MATCH="pattern"` is the dial pattern to match. When entering the *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 will occur and the number will be dialed as entered by the user. To have the number dial immediately, specify 0.

## ■ Creating Dial Plans

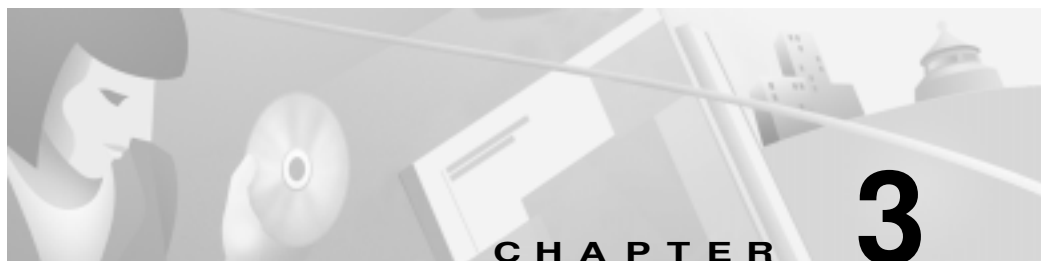
- User=*type* is the either IP or Phone. Enter User=phone or User=IP to have the tag automatically added to the dialed number.
- Rewrite=*altstrng* is the alternate string to be dialed instead of what the user enters.

- 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, specify `</DIALTEMPLATE>` to indicate the end 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 you 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) via 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 via the dial\_template parameter in the default configuration file. For more information on defining the dial\_template parameter, see the “Modifying the Phone’s SIP Settings” section on page 3-5.

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

### **Example 2-1 Example of a PBX North American Dial Plan**

```
<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="1" User="Phone"/> <!-- PSTN Operator-->
  <TEMPLATE MATCH="9,11" Timeout="0" User="Phone" Rewrite="9911"/> <!-- Emergency-->
  <TEMPLATE MATCH="w!" 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,....." Timeout="0" User="Phone"/> <!-- Local numbers -->
  <TEMPLATE MATCH="*" Timeout="15"/> <!-- Anything else -->
</DIALTEMPLATE>
```



## Managing Cisco SIP IP Phones

---

This chapter provides information on the following:

- Entering Configuration Mode, page 3-1
- Modifying the Phone's Network Settings, page 3-2
- Modifying the Phone's SIP Settings, page 3-5
- Setting the Date, Time, and Daylight Savings Time, page 3-22
- Erasing the Locally-Defined Settings, page 3-28
- Accessing Status Information, page 3-30
- Upgrading the Cisco SIP IP Phone Firmware, page 3-33

### 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

To unlock the Cisco SIP IP phone, press **\*\*#**.



**Note**

You have activated the configuration mode for your phone. There is no indication 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 will change 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 panels, the lock icon will be displayed in an unlocked state.

The unlocked symbol indicates that you can modify the network and SIP configuration settings.

## Locking Configuration Mode

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 will change 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 unlocked symbol indicates that you can modify the network and SIP configuration settings.

## Modifying the Phone's 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 DHCP server, MAC address, IP address, and domain name.

**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 2-21.
- After making your changes, relock configuration mode as described in the “Locking Configuration Mode” section on page 3-2.

**Procedure**

---

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

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

**Step 3** Press the **Select** soft key. The Network Configuration menu is displayed.

The following network parameters are available on the Network Configuration menu:

- **DHCP Server**—IP address of the DHCP server from which the phone received its IP address and additional network settings. You cannot change the information in this field.
- **MAC Address**—Factory-assigned unique 48-bit hexadecimal MAC address of the phone. You cannot change the information in this field.
- **Host Name**—Unique host name assigned to the phone. The value in this field is always *SIPmac* where *mac* is the MAC address of the phone. You cannot change the information in this field.
- **Domain Name**—Name of the DNS domain in which the phone resides.
- **IP Address**—IP address of the phone that was assigned by DHCP or locally configured. To edit this field, DHCP must be disabled.
- **Subnet Mask**—IP subnet mask used by the phone. A subnet mask partitions the IP address into a network and a host identifier. To edit this field, DHCP must be disabled.

- TFTP Server—IP address of the TFTP server from which the phone downloads its configuration files and firmware images. To edit this field, DHCP must be disabled.
- 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 will attempt to use as an alternate gateway if the primary gateway is NA. To edit this field, DHCP must be disabled.
- DNS Servers 1 through 5—IP address of the DNS server used by the phone to result names to IP addresses. The phone will attempt to use DNS Servers 2 through 5 if DNS Server 1 is unavailable. To edit this field, DHCP must be disabled.
- Operational VLAN Id—Unique identifier of the VLAN of which the phone is a member. This identifier is obtained through Cisco Discovery Protocol (CDP). You cannot change the information in this field.
- Admin. VLAN Id—Unique identifier of the VLAN to which the phone is attached. The value in this field is only used in non-Cisco switched networks. You can change the administrative VLAN used by the phone, however, if you have an administrative VLAN assigned on the Catalyst switch, that setting overrides any changes made on the phone.
- Network Media Type—Ethernet port negotiation mode. Possible values are
  - Auto—Port is auto-negotiated.
  - Full-100—Port is configured to be a full-duplex, 100MB connection.
  - Half-100—Port is configured to be a half-duplex, 100MB connection.
  - Full-10—Port is configured to be a full-duplex, 10MB connection.
  - Half-10—Port is configured to be a half-duplex, 10MB connection.

The default is Auto.

- DHCP Enabled—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). Possible 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.
- DHCP Address Released—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.

- **Alternate TFTP**—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.
- **Erase Configuration**—Whether to erase all of the locally-defined settings on the phone and reset the values to the defaults. Selecting Yes will re-enable DHCP. For more information on erasing the local configuration, see the “Erasing the Locally-Defined Settings” section on page 3-28.

**Step 4** When done, press the **Save** soft key. The phone programs the new information into Flash memory and resets.

---

**Caution**

When you have completed your changes, ensure that you lock the phone as described in the “Locking Configuration Mode” section on page 3-2.

---

## Modifying the Phone's SIP Settings

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 will override the values stored in Flash memory.
- Parameters defined in the phone-specific configuration file will override the values specified in the default configuration file.
- Parameters entered locally will be 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 3-1 lists each of the SIP parameters that you can configure. In the Configuration column, the name of a parameter as you would specify it in a configuration file is listed. In the menu column (SIP Configuration, Network Configuration, and Services), the name of the same parameter as it would appear on the user interface is listed. If NA appears for a parameter name in a menu column, it can cannot be defined via that menu.

**Table 3-1 SIP Parameters Summary**

Configuration File	SIP Configuration Menu	Network Configuration Menu	Services Menu
anonymous_call_block	NA	NA	Anonymous Call Block
autocomplete	NA	NA	Auto-Complete Numbers
callerid_blocking	NA	NA	Caller ID Block
dial_template	NA	NA	NA
dnd_control	NA	NA	NA
dst_auto_adjust	NA	NA	NA
dst_offset	NA	NA	NA
dst_start_day	NA	NA	NA
dst_start_day_of_week	NA	NA	NA
dst_start_month	NA	NA	NA
dst_start_time	NA	NA	NA
dst_start_week_of_month	NA	NA	NA
dst_stop_day	NA	NA	NA
dst_stop_day_of_week	NA	NA	NA
dst_stop_month	NA	NA	NA
dst_stop_time	NA	NA	NA
dst_stop_week_of_month	NA	NA	NA
dtmf_avt_payload	NA	NA	NA
dtmf_db_level	NA	NA	NA
dtmf_inband	NA	NA	Do Not Disturb

**Table 3-1 SIP Parameters Summary (continued)**

Configuration File	SIP Configuration Menu	Network Configuration Menu	Services Menu
dtmf_outofband	Out of Band DTMF	NA	NA
image_version	NA	NA	NA
linex_authname (line1 to line6)	Authentication Name	NA	NA
linex_displayname (line1 to line6)	Display Name	NA	NA
linex_name (line1 to line6)	Name	NA	NA
linex_password (line1 to line6)	Authentication Password	NA	NA
linex_shortname (line1 to line6)	Shortname	NA	NA
messages_uri	Messages URI	NA	NA
network_media_type	NA	Network Media Type	NA
phone_label	Phone Label	NA	NA
preferred_codec	Preferred Codec	NA	NA
proxy_register	Register with Proxy	NA	NA
proxy1_address	Proxy Address	NA	NA
proxy1_port	Proxy Port	NA	NA
sip_invite_retx	NA	NA	NA
sip_retx	NA	NA	NA
sntp_mode	NA	NA	NA
sntp_server	NA	NA	NA
sync	NA	NA	NA
tftp_cfg_dir	TFTP Directory	NA	NA
time_format_24hr	NA	NA	NA
time_zone	NA	NA	NA
timer_invite_expires	NA	NA	NA

**Table 3-1 SIP Parameters Summary (continued)**

Configuration File	SIP Configuration Menu	Network Configuration Menu	Services Menu
timer_register_expires	Register Expires	NA	NA
timer_t1	NA	NA	NA
timer_t2	NA	NA	NA
tos_media	NA	NA	NA

## 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 “Configuring SIP Parameters via a TFTP Server” section on page 2-6, you can also modify your SIP parameters using the configuration files.

As explained in the “Configuring SIP Parameters” section on page 2-5, 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 a subdirectory in which phone-specific configuration files are stored.

While not required, we recommend 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 an easier task. You can then define only those parameters that are specific to a phone in the phone-specific configuration file. Phone-specific parameters should only be defined in a phone-specific configuration file or 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), we recommend that you maintain the SIP parameters that are common to all of 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 CCO to the root directory of your TFTP server.
- Review the guidelines and restrictions documented in the “Configuration File Guidelines” section on page 2-6.

**Procedure**

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

- **image\_version**—(Required) Firmware version that the Cisco SIP IP phone should run.  
  
Enter the name of the image version (as it is release by Cisco). Do not enter the extension. You cannot change the image version by changing the file name because the version is also built into the file header. Trying to change the image version by changing the file name will cause the firmware to fail when it compares the version in the header against the file name.
- **proxy1\_address**—(Required) IP address of the primary SIP proxy server that will be used by the phones. Enter this address in IP dotted-decimal notation.
- **proxy1\_port**—(Optional) Port number of the primary SIP proxy server. This is the port on which the SIP client will listen for messages. The default is 5060.
- **tos\_media**—(Optional) Type of Service (ToS) level for the media stream being used. Valid values are:
  - 0 (IP\_ROUTINE)
  - 1 (IP\_PRIORITY)
  - 2 (IP\_IMMEDIATE)
  - 3 (IP\_FLASH)
  - 4 (IP\_OVERRIDE)
  - 5 (IP\_CRITIC)

The default is 5.

- **preferred\_codec**—(Optional) CODEC to use when initiating a call. Valid values are g711alaw, g711ulaw, and g729a. The default is g711ulaw.

- **dtmf\_inband**—(Optional) Whether to detect and generate 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.
- **dtmf\_db\_level**—(Optional) In-band DTMF digit tone level. Valid values are:
  - 1 (6 db below nominal)
  - 2 (3 db below nominal)
  - 3 (nominal)
  - 4 (3 db above nominal)
  - 5 (6 db above nominal)

The default is 3.

- **dtmf\_outofband**—(Optional) Whether to 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-band signaling via the AVT tone method. Valid values are:
  - **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.

- **dtmf\_avt\_payload**—(Optional) Payload type for AVT packets. Possible range is 96 to 127. If the value specified exceeds 127, the phone will default to 101.
- **timer\_t1**—(Optional) Lowest value (in milliseconds) of the retransmission timer for SIP messages. The valid value is any positive integer. The default is 500.
- **timer\_t2**—(Optional) Highest value (in milliseconds) of the retransmission timer for SIP messages. The valid value is any positive integer greater than timer\_t1. The default is 4000.
- **timer\_invite\_expires**—(Optional) The amount of time, in seconds, after which a SIP INVITE will expire. This value is used in the Expire header field. The valid value is any positive number, however, we recommend 180 seconds. The default is 180.

- `sip_retx`—(Optional) Maximum number of times a SIP message other than an INVITE request will be retransmitted. The valid value is any positive integer. The default is 10.
- `sip_invite_retx`—(Optional) Maximum number of times an INVITE request will be retransmitted. The valid value is any positive integer. The default is 6.
- `proxy_register`—(Optional) Whether 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 to 0 will unregister the phone from the proxy server. To reinitiate a registration, change the value of this parameter back to 1.

**Note**

If you enable registration, and authentication is required, you must specify values for the `linex_authname` and `linex_password` parameters (where *x* is a number 1 through 6) in the phone-specific configuration file. For information on configuring the phone-specific configuration file, see the “Modifying the Phone-Specific SIP Configuration File” section on page 3-15.

- `timer_register_expires`—(Optional) The amount of time, in seconds, after which a REGISTRATION request will expire. This value is inserted into the Expire header field. The valid value is any positive number, however, we recommend 3600 seconds. The default is 3600.
- `messages_uri`—(Optional) Number to call to check voicemail. This number will be called when the **Messages** key is pressed.
- Date, Time, and Daylight Savings Time parameters. See the “Setting the Date, Time, and Daylight Savings Time” section on page 3-22 section for more information on setting the following parameters:
  - `sntp_mode`—(Optional) Mode in which the phone will listen for the SNTP server.
  - `sntp_server`—(Optional) IP address of the SNTP server from which the phone will obtain time data.
  - `time_zone`—(Optional) Time zone in which the phone is located.

- dst\_offset—(Optional) Offset from the phone's time when DST is in effect.
- dst\_start\_month—(Optional) Month in which DST starts.
- dst\_start\_day—(Optional) Day of the month on which DST begins.
- dst\_start\_day\_of\_week—(Optional) Day of the week on which DST begins.
- dst\_start\_week\_of\_month—(Optional) Week of month in which DST begins.
- dst\_start\_time—(Optional) Time of day on which DST begins.
- dst\_stop\_month—(Optional) Month in which DST ends.
- dst\_stop\_day—(Optional) Day of the month on which DST ends.
- dst\_stop\_day\_of\_week—(Optional) Day of the week on which DST ends.
- dst\_stop\_week\_of\_month—(Optional) Week of month in which DST ends.
- dst\_stop\_time—(Optional) Time of day on which DST ends.
- dst\_auto\_adjust—(Optional) Whether or not DST is automatically adjusted on the phones.
- dnd\_control—(Optional) Whether the Do Not Disturb feature is enabled or disabled by default on the phone or whether the feature is permanently enabled. When the feature is permanently enabled, a phone is a “call out” phone only. When the Do Not Disturb feature is turned on, the phone will block all calls placed to the phone and log those calls in the Missed Calls directory. Valid values are:
  - 0—The Do Not Disturb feature is off by default, but can be turn on and off locally via the phone's user interface.
  - 1—The Do Not Disturb feature is on by default, but can be turned on and off locally via the phone's user interface.



- 2—The Do Not Disturb feature is off permanently and cannot be turned on and off locally via the phone's user interface. If specifying this value, specify this parameter in the phone-specific configuration file.
  - 3—The Do Not Disturb feature is on permanently and cannot be turned on and off locally via the phone's user interface. This setting sets the phone to be a “call out” phone only. If specifying this value, specify this parameter in the phone-specific configuration file.
- callerid\_blocking—(Optional) Whether the Caller ID Blocking feature is enabled or disabled by default on the phone. When enabled, the phone will block its number or email address from phones that have caller identification capabilities. Valid values are:
  - 0—The Caller ID Blocking feature is disabled by default, but can be turned on and off via the phone's user interface. When disabled, the caller identification is included in the Request-URI header field.
  - 1—The Caller ID Blocking feature is enabled by default, but can be turned on and off via the phone's user interface. When enabled, “Anonymous” is included in place of the user identification in the Request-URI header field.
  - 2—The Caller ID Blocking feature is disabled permanently and cannot be turned on and off locally via the phone's user interface. If specifying this value, specify this parameter in the phone-specific configuration file.
  - 3—The Caller ID Blocking feature is enabled permanently and cannot be turned on and off locally via the phone's user interface. If specifying this value, specify this parameter in the phone-specific configuration file.
- anonymous\_call\_block—(Optional) Whether the Anonymous Call Block feature is enabled or disabled by default on the phone. Valid values are:
  - 0—The Anonymous Call Blocking feature is disabled by default, but can be turned on and off via the phone's user interface. When disabled, anonymous calls will be received.
  - 1—The Anonymous Call Blocking features is enabled by default, but can be turned on and off via the phone's user interface. When enabled, anonymous calls will be rejected

- 2—The Anonymous Call Blocking feature is disabled permanently and cannot be turned on and off locally via the phone's user interface. If specifying this value, specify this parameter in the phone-specific configuration file.
- 3—The Anonymous Call Blocking feature is enabled permanently and cannot be turned on and off locally via the phone's user interface. If specifying this value, specify this parameter in the phone-specific configuration file.
- `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.
- `network_media_type`—(Optional) Ethernet port negotiation mode. Valid values are:
  - Auto—Port is auto-negotiated.
  - Full100—Port is configured to be a full-duplex, 100MB connection.
  - Half100—Port is configured to be a half-duplex, 100MB connection.
  - Full10—Port is configured to be a full-duplex, 10MB connection.
  - Half10—Port is configured to be a half-duplex, 10MB connection.

The default is Auto.

- `autocomplete`—(Optional) Whether to have numbers automatically completed when dialing. Valid values are 0 (disable auto completion) or 1 (enable auto completion). The default is 1.
- `sync`—Value against which to compare the value in the `syncinfo.xml` before performing a remote reboot. Valid value is a character string up to 32 characters long.
- `time_format_24hr`—Whether a 12 or 24-hour time format is displayed by default on the phones' user interface. Valid values are:
  - 0—The 12-hour format is displayed by default but can be changed to a 24-hour format via the phone's user interface.
  - 1—The 24-hour format is displayed by default but can be changed to a 12-hour format via the phone's user interface.
  - 3—The 12-hour format is displayed and cannot be changed to a 24-hour format via the phone's user interface.

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

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

```
; sip default configuration file

#Image Version
image_version:POS3xxyy ;

#Default Codec
preferred_codec :g711ulaw

#Enable Registration
proxy_register :1 ;

#Registration expiration
timer_register_expires :3600 ;

#Proxy address
proxy1_address: 192.168.1.1 ;
```

## Modifying the Phone-Specific SIP Configuration File

In the phone-specific SIP configuration file, maintain those 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 and restrictions documented in the “Configuration File Guidelines” section on page 2-6.
- Line parameters (those identified as linex) define a line on the phone. If you configure a line to use an e-mail address, that line can be called only using an e-mail address. Similarly, if you configure a line to use a number, that line can only be called using the number. Each line can have a different proxy configured.

### 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* a number 1 through 6):

- **linex\_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.
- **linex\_shortcode**—(Optional) Name or number associated with the **linex\_name** as you want it to display on the phone's LCD if the **linex\_name** length exceeds the allowable space in 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 3444 display on the LCD instead. Alternately, if the value for the **linex\_name** parameter is the email address "username@company.com", you can specify the "username" to have just the user name appear on the LCD instead.

This parameter is used for display-only purposes. If a value is not specified for this parameter, the value in the **linex\_name** variable is displayed.

- **linex\_authname**—(Required for line 1 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 **linex\_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.
- **linex\_password**—(Required for line 1 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 **linex\_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.

- `linex_displayname`—(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 callee end instead. If a value is not specified for this parameter, nothing is used.
- `dnd_control`—(Optional) Whether the Do Not Disturb feature is enabled or disabled by default on the phone or whether the feature is permanently enabled, making the phone a “call out” phone only. When the Do Not Disturb feature is turned on, the phone will block all calls placed to the phone and log those calls in the Missed Calls directory. Valid values are:
  - 0—The Do Not Disturb feature is off by default, but can be turned on and off locally via the phone's user interface.
  - 1—The Do Not Disturb feature is on by default, but can be turned on and off locally via the phone's user interface.
  - 2—The Do Not Disturb feature is off permanently and cannot be turned on and off locally via the phone's user interface. If specifying this value, specify this parameter in the phone-specific configuration file.
  - 3—The Do Not Disturb feature is on permanently and cannot be turned on and off locally via the phone's user interface. This setting sets the phone to be a “call out” phone only. If specifying this value, specify this parameter in the phone-specific configuration file.

**Note**

This parameter is best configured in the `SIPDefault.dnf` file unless configuring a phone to be a “call-out” phone only. When configuring a phone to be a “call-out” phone, define this parameter in the phone-specific configuration file.

- `phone_label`—Label to display on the top status line of the LCD. This field is for end-user display only purposes. For example, a phone's label can display “John Doe's phone.” Approximately up to 11 characters can be used when specifying the phone label.

- Step 2** Save the file to your TFTP server (in the root directory or a subdirectory containing all the phone-specific configuration files). Name the file “SIPXXXXXXXXXXXX.cnf” where XXXXXXXXXX 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, SIP00503EFFF842.cnf).
- 

The following is an example of a configuration file:

```
; phone-specific configuration file sample
; 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
```

## Modifying the SIP Parameters Manually

If you did not configure the SIP parameters via a TFTP server, you can configure them manually 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 2-21.
- Line parameters (those identified as lineX) define a line on the phone. If you configure a line to use an e-mail address, that line can be called only using an e-mail address. Similarly, if you configure a line to use a number, that line can only be called using the number.

- When configuring the Preferred Codec and Out of Band DTMF parameters, press the **Change** soft key until the option 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 3-2.

#### 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 following parameters as necessary:
- **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.
  - **Short Name**—(Optional) 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 3444 display on the LCD instead. Alternately, if the value for the `linex_name` parameter is the email address “username@company.com”, you can specify the “username” to have just the user name appear on the LCD instead. This parameter is used for display-only purposes.  
  
If a value is not specified for this parameter, the value in the Name variable is displayed.
  - **Authentication Name**—(Required when registration is enabled) Name used by the phone for authentication if a registration is challenged by the proxy server during initialization.
  - **Authentication Password**—(Required when registration is enabled) 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 *SIPmacaddress* where *macaddress* is the MAC address of the phone.

- **Display Name**—(Optional) Identification as it should appear for caller-identification purposes. For example, instead of *jdoo@company.com* displaying on phones that have caller ID, you can specify John Doe in this parameter to have John Doe display on the callee end instead. If a value is not specified for this parameter, the Name value is used.
- **Proxy Address**—(Required) IP address of the primary SIP proxy server that will be used by the phone. Enter this address in IP dotted-decimal notation.
- **Proxy Port**—(Optional) Port number of the primary SIP proxy server. This is the port on which the SIP client will listen for messages. The default is 5060.

**Step 6** Press the **Back** soft key 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 following parameters on the SIP Configuration menu:

- **Message URI**—Number to call to check voicemail. This number will be called when the **Messages** key is pressed.
- **Preferred Codec**—(Optional) CODEC to use when initiating a call. Valid values are *g711alaw*, *g711ulaw*, and *g729a*. The default is *g711ulaw*.
- **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:
  - *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*.



- **Register with Proxy**—(Optional) Whether the phone must register with a proxy server during initialization. Valid values are Yes and No. Select the **No** soft key to disable registration during initialization. Select the **Yes** 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 will unregister the phone from the proxy server. To reinitiate a registration, change the value of this parameter back to Yes.



**Note** If you enable registration, and authentication is required, you must specify values for the Authentication Name and Authentication Password parameters.

- **Register Expires**—(Optional) The amount of time, in seconds, after which a REGISTRATION request will expire. This value is used the Expire header field. The valid value is any positive number, however, we recommend 3600 seconds. The default is 3600.
- **TFTP Directory**—(Required if phone-specific configuration files are located in a subdirectory) Path to the TFTP subdirectory in which phone-specific configuration files are stored.
- **Phone Label**—(Optional) Label to display on the top status line of the LCD. This field is for end-user display only purposes. For example, a phone's label can display "John Doe's phone."

**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 3-2.

---

## Setting the Date, Time, and Daylight Savings 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 savings 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 the first Sunday in April and ends on the last day of October) configuration.

We recommend that date and time-related parameters be defined in the SIPDefault.cnf 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 “Configuration File Guidelines” section on page 2-6.
- 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 3-2 and Table 3-3 before configuring the SNTP parameters:

Table 3-2 lists the actions that take place when a null value (0.0.0.0) is specified in the sntp\_server parameter.

**Table 3-2** *Actions Based on sntp\_mode When the sntp\_server Parameter is Set to a Null Value*

<b>sntp_server =0.0.0.0</b>	<b>sntp_mode= unicast</b>	<b>sntp_mode= multicast</b>	<b>sntp_mode= anycast</b>	<b>sntp mode= directedbroadcast</b>
<b>Sends</b>	Nothing.  No known server with which to communicate.	Nothing.  When in multicast mode, SNTP requests are not sent.	SNTP packet to the local network address.  After the first SNTP response is received, the phone switches to unicast mode with the server being set as the one who first responded.	SNTP packet to the local network address.  After the first SNTP response is received, the phone switches to multicast mode.
<b>Receives</b>	Nothing.  No known server with which to communicate.	SNTP data via the SNTP/NTP multicast address from the local network broadcast address from any server on the network.	Unicast SNTP data from the SNTP server that first responded to the network broadcast request.	SNTP data from the SNTP/NTP multicast address and the local network broadcast address from any server on the network.

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

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

<b>sntp_server = 0.0.0.0</b>	<b>sntp_mode=unicast</b>	<b>sntp_mode=multicast</b>	<b>sntp_mode=anycast</b>	<b>sntp_mode=directedbroadcast</b>
<b>Sends</b>	SNTP request to the SNTP server.	Nothing.  When in multicast mode, SNTP requests are not sent.	SNTP request to the SNTP server.	SNTP packet to the SNTP server.  After the first SNTP response is received, the phone switches to multicast mode.
<b>Receives</b>	SNTP response from the SNTP server and ignores responses from other SNTP servers.	SNTP data via the SNTP/NTP multicast address from the local network broadcast address.	SNTP response from the SNTP server and ignores responses from other SNTP servers.	SNTP data from the SNTP/NTP multicast address and the local network broadcast address and ignores responses from other SNTP servers.

### Procedure

- 
- 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 will listen for the SNTP server. Valid values are unicast, multicast, anycast, or directedbroadcast.  
See Table 3-2 and Table 3-3 for an explanation on how these values work depending on the sntp\_server parameter value.
  - **sntp\_server**—(Required) IP address of the SNTP server from which the phone will obtain time data.  
See Table 3-2 and Table 3-3 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 hour/minute, -hour/minute, +hour/minute, hour, -hour, +hour, PST, MST, CST, or EST.
- 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 the same as for the time\_zone parameter.
  - **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 case-sensitive and should be typed as cited in this description.
  - **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 case-sensitive and should be typed as cited in this description.

- `dst_start_time`—Time of day on which DST begins. Valid values are hour/minute (02/00) or hour (14:30).
- `dst_stop_time`—Time of day on which DST ends. Valid values are hour/minute (02/00) or hour (14:30).

**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 specify 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 specify 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 case-sensitive and should be typed as cited in this description.
- `dst_start_week_of_month`—Week of month in 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.

- `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 case-sensitive and should be typed as cited in this description.
- `dst_stop_week_of_month`—Week of month in 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.

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

---

The following is an example of the configuration for an absolute DST configuration:

```
; sip default configuration file
(additional configuration text omitted)

time_zone : 03/00
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

(additional configuration text omitted)
```

The following is an example of the configuration for a relative DST configuration:

```
; sip default configuration file
(additional configuration text omitted)

time_zone : PST
dst_offset : 01/00
dst_start_month : April
dst_start_day : 0
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 : 1

(additional configuration text omitted)
```

## Erasing the Locally-Defined Settings

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

### Erasing the Locally-Defined Network Settings

When you erase the locally-defined 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 will reenable 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).



---

**Procedure**

- 
- Step 1** Press the **settings** key. The Settings menu is displayed.
  - Step 2** Highlight **Network Configuration**.
  - Step 3** Press the **Select** soft key. The Network Configuration settings are displayed.
  - Step 4** Highlight **Erase Configuration**.
  - Step 5** Press the **Yes** soft key.
  - Step 6** Press the **Save** soft key. The phone programs the new information into Flash memory and resets.
- 

## Erasing the Locally-Defined SIP Settings

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

**Note**

---

If your system has been set up to have the phones retrieve their SIP parameters via a TFTP server, you will need to edit the configuration file in which a parameter is defined to delete the parameter. When deleting a parameter, leave the variable in the file, but change its value to a null value "" or "UNPROVISIONED". If both the variable and its value are removed, the phone will use the setting for that variable that it has stored in Flash memory.

---

**Before You Begin**

Unlock configuration mode as described in the "Unlocking Configuration Mode" section on page 3-2.

---

**Procedure**

- 
- Step 1** Press the **settings** key. The Settings menu is displayed.
  - Step 2** Highlight **SIP Configuration**.
  - Step 3** Press the **Select** soft key. The SIP Configuration settings are displayed.

- Step 4** Highlight the parameter for which you wish to erase the setting.
  - Step 5** Press the **Edit** soft key.
  - Step 6** Press the << soft key to delete the current value.
  - Step 7** Press the **Validate** soft key to save your change and exit the Edit panel.
  - Step 8** If modifying a line parameter, press the **Back** soft key to exit the Line Configuration panel.
  - Step 9** Press the **Save** soft key. The phone programs the new information into Flash memory and resets.
- 

## 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 which 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, complete the following steps:

- 
- |               |                                                                           |
|---------------|---------------------------------------------------------------------------|
| <b>Step 1</b> | Press the <b>Settings</b> key. The Settings menu is displayed.            |
| <b>Step 2</b> | Highlight <b>Status</b> .                                                 |
| <b>Step 3</b> | Press the <b>Select</b> soft key. The Setting Status menu is displayed.   |
| <b>Step 4</b> | Highlight <b>Status Messages</b> .                                        |
| <b>Step 5</b> | Press the <b>Select</b> soft key. The Status Messages panel is displayed. |
| <b>Step 6</b> | To exit the Status Messages panel, press the <b>Exit</b> soft key.        |
- 

## Viewing Network Statistics

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

- 
- |               |                                                                              |
|---------------|------------------------------------------------------------------------------|
| <b>Step 1</b> | Press the <b>settings</b> key. The Settings menu is displayed.               |
| <b>Step 2</b> | Highlight <b>Status</b> .                                                    |
| <b>Step 3</b> | Press the <b>Select</b> soft key. The Setting Status menu is displayed.      |
| <b>Step 4</b> | Highlight <b>Network Statistics</b> .                                        |
| <b>Step 5</b> | Press the <b>Select</b> soft key. The Network Statistics panel is displayed. |

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 auto-negotiated a full-duplex 100Mbps connection.
- Port 0 Half, 100—Indicates that the network is in a linked state and has auto-negotiated a half-duplex 100Mbps connection.
- Port 0 Full, 10—Indicates that the network is in a linked state and has auto-negotiated a full-duplex 10Mbps connection.
- Port 0 Half, 10—Indicates that the network is in a linked state and has auto-negotiated a half-duplex 10Mbps connection.
- Port 1 Full, 100—Indicates that the network is in a linked state and has auto-negotiated a full-duplex 100Mbps connection.
- Port 1 Half, 100—Indicates that the network is in a linked state and has auto-negotiated a half-duplex 100Mbps connection.
- Port 1 Full, 10—Indicates that the network is in a linked state and has auto-negotiated a full-duplex 10Mbps connection.
- Port 1 Half, 10—Indicates that the network is in a linked state and has auto-negotiated a half-duplex 10Mbps connection.

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

---



**Note**

To reset the values displayed on Network Statistics panel, power off and power on the phone.

---

## Viewing the Firmware Version

To view network statistics, complete the following steps:

- 
- Step 1** Press the **settings** key. The Settings menu is displayed.
  - Step 2** Highlight **Status**.
  - Step 3** Press the **Select** soft key. The Setting Status menu is displayed.
  - Step 4** Highlight **Firmware Versions**.
  - Step 5** Press the **Select** soft key. The Firmware Versions panel is displayed.

The following information is displayed on this panel:

- Application Load ID—Current software image on the phone.
- Boot Load ID—Bootstrap loader image version that is manufactured on the phone. This image name does not change.

- Step 6** To exit the Firmware Versions panel, press the **Exit** soft key.
- 

## Upgrading the Cisco SIP IP Phone Firmware

There are two methods that you can use to upgrade the firmware on your Cisco SIP IP phones. You can upgrade the firmware on one phone at a time via the phone-specific configuration or you can upgrade the firmware on a system of phones using the default configuration file.

### Before You Begin

- To upgrade the firmware on just one phone at a time, you upgrade 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.
- Ensure that the latest version of the Cisco SIP IP phone firmware has been copied from CCO to the root directory of your TFTP server.

### Procedure

- 
- Step 1** Copy the binary file POS3xxyy.bin (where *xx* is the version number and *yy* is the subversion number) from CCO 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 `image_version` variable should match the version name (without the .bin extension) of the latest firmware that you downloaded.
- 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 for which you have updated their phone-specific configuration file with the new image version and restarted will use the latest firmware image. All other phones will use the older version until their configuration files have been updated with the new image version.

---

## Performing an Image Upgrade and Remote Reboot

With Version 2.0 of the Cisco SIP IP Phone 7960, you can perform an image upgrade and remote reboot using Notify messages and the syncinfo.xml file.

**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, complete the following tasks:

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.
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:

```
<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 sync level for the phone is 1. Valid values is a character-string up to 32 characters.
3. Send a NOTIFY message to the phone. In the Notify message, ensure that the an Event header equal to “check-sync” is included.

The following is an example of a Notify message:

```
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
```

Once 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 will wait 20 seconds and then contact the TFTP server for the syncinfo.xml file. If the phone is not in an idle state, the phone will wait until it is in an idle state for 20 seconds and then contact 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 c. If not, the phone proceeds to b.
  - b. Determines whether there is a wildcard entry (\*) in the image version parameter. If so, the phone proceeds to c. If not, the phone proceeds to d.
  - c. Determines if the sync value is different than what is stored on the phone. If so, the phone proceeds to e. If not, the phone proceeds to d.
  - d. The phone does nothing.
  - e. The phone reboots.

The phone then performs a normal reboot process as described in “Initialization Process Overview” section on page 2-1, sees the new image, and upgrades to the new image with a sync value of 2.





## SIP Compliance with RFC-2543 Information

---

This section describes how the Cisco SIP IP phone complies with the IETF definition of SIP as described in RFC 2543.

This section contains compliance information on the following:

- SIP Functions, page A-2
- SIP Methods, page A-2
- SIP Responses, page A-3
- SIP Header Fields, page A-10
- SIP Session Description Protocol (SDP) Usage, page A-12

## SIP Functions

Function	Supported?
User Agent Client (UAC)	Yes
User Agent Server (UAS)	Yes
Proxy Server	Third-party only
Redirect Server	Third-party only

## SIP Methods

Five of the six methods used by the SIP gateway are supported:

Method	Supported?	Comments
INVITE	Yes	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.
ACK	Yes	None.
OPTIONS	No	
BYE	Yes	
CANCEL	Yes	
REGISTER	Yes	The Cisco SIP IP phone supports both user and device registration.

# SIP Responses

Release 1.0 of the Cisco SIP IP phone supports the following SIP responses:

- 1xx Response—Information Responses, page A-4
- 2xx Response—Successful Responses, page A-4
- 3xx Response—Redirection Responses, page A-5
- 4xx Response—Request Failure Responses, page A-5
- 5xx Response—Server Failure Responses, page A-10
- 6xx Response—Global Responses, page A-10

## 1xx Response— Information Responses

1xx Response	Supported?	Comments
100 Trying	Yes	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.
180 Ringing	Yes	None
181 Call is being forwarded	See comments	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.
182 Queued		
183 Session Progress		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.

## 2xx Response— Successful Responses

2xx Response	Supported?	Comments
200 OK	Yes	None

## 3xx Response—Redirection Responses

3xx Response	Supported	Comments
300 Multiple Choices	Yes	None
301 Moved Permanently	Yes	
302 Moved Temporarily	Yes	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.
305 Use Proxy	Yes	The phone does not generate these responses. The gateway contacts the new address in the Contact header field.
380 Alternate Service	Yes	

## 4xx Response—Request Failure Responses

4xx Response	Supported?	Comments
400 Bad Request	Yes	The phone generates a 400 Bad Request response for a 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.

4xx Response	Supported?	Comments
401 Unauthorized	Yes	<p>This response is only received in this release.</p> <p>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 2543.</p>
402 Payment Required	Yes	The phone does not generate the 402 Payment Required response.
403 Forbidden	Yes	<p>This response is only received in this release.</p> <p>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.</p>
404 Not Found	Yes	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.
405 Method Not Allowed	See comments	<p>This response is only received in this release.</p> <p>If the phone receives a 405 Method Not Allowed response, it notifies the user of the response.</p>
406 Not Acceptable	See comments	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.

4xx Response	Supported?	Comments
407 Proxy Authentication Required	See comments	<p>This response is only received in this release.</p> <p>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.</p>
408 Request Timeout	See comments	<p>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.</p>
409 Conflict	See comments	<p>This response is only received the phone in this release.</p> <p>The 409 Conflict response indicates that the INVITE request could not be process because of a conflict with the current state of the resource. If this response is received, the user is notified.</p>
410 Gone	See comments	<p>This response is only received by the phone in this release.</p> <p>The 410 Gone response indicates that a resource is no longer available at the server and no forwarding address is known.</p>

4xx Response	Supported?	Comments
411 Length Required	See comments	<p>This response is only received by the phone in this release.</p> <p>This response indicates that the user refuses to accept the request without a defined content length. If received the phone resends the INVITE request if it can add a valid Content-Length header field.</p>
413 Request Entity Too Large	See comments	<p>This response is only received by the phone in this release.</p> <p>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.</p>
414 Request—URL Too Long	See comments	<p>This response is only received by the phone in this release. The user is notified if this response is received.</p>
415 Unsupported Media	See comments	<p>This response is only received by the phone in this release. The user is notified if this response is received.</p>
420 Bad Extension	See comments	<p>This response is only received by the phone in this release. The user is notified if this response is received.</p> <p>If the phone does not understand the protocol extension specified in the Require field, the 420 Bad Extension response is generated.</p>



4xx Response	Supported?	Comments
480 Temporarily Unavailable	See comments	<p>This response is only received by the phone in this release. The user is notified if this response is received.</p> <p>If this response is received, the user is notified that the callee is temporarily unavailable (perhaps not logged on) and any retry information is displayed.</p>
481 Call Leg/Transaction Does Not Exist	See comments	<p>This response is only received by the phone in this release. The user is notified if this response is received.</p>
482 Loop Detected		
483 Too Many Hops		
484 Address Incomplete		
485 Ambiguous	See comments	<p>This response is only received by the phone in this release.</p> <p>If a new contact is received, the phone might re-initiate the call.</p>
486 Busy Here	Yes	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.
487 Request Canceled	See comments	<p>This response is only received by the phone in this release.</p> <p>This response indicates that the initial request is terminated with a BYE or CANCEL request.</p>
488 Not Acceptable	Yes	The Cisco SIP IP phone receives and generates this response.

## 5xx Response— Server Failure Responses

5xx Response	Comments
500 Internal Server Error	For an incoming response, the Cisco SIP IP phone sends a new request if an additional contact address is present. If an additional contact address is not present, the gateway initiates a graceful call disconnect.
501 Not Implemented	
502 Bad Gateway	
503 Service Unavailable	
504 Gateway Timeout	
505 Version Not Supported	

## 6xx Response— Global Responses

6xx Response	Comments
600 Busy Everywhere	The Cisco SIP IP phone does not generate these 6xx responses. For an incoming response, the gateway initiates a graceful call disconnect.
603 Decline	
604 Does Not Exist Anywhere	
606 Not Acceptable	

## SIP Header Fields

Header Field	Supported?
Accept	Yes
Accept-Encoding	Yes
Accept-Language	Yes
Allow	Yes
Also	Yes

Header Field	Supported?
Authorization	Yes
Call-ID	Yes
Contact	Yes
Content-Encoding	Yes
Content-Length	Yes
Content-Type	Yes
Cseq	Yes
Date	Yes
Encryption	No
Expires	Yes
From	Yes
Hide	No
Max-Forwards	Yes
Organization	No
Priority	No
Proxy-Authenticate	Yes
Proxy-Authorization	Yes
Proxy-Require	Yes
ReBy	Yes
Record-Route	Yes
Require	Yes
Response-Key	No
Retry-After	Yes
Route	Yes

## ■ SIP Session Description Protocol (SDP) Usage

Header Field	Supported?
Server	No
Subject	No
Timestamp	Yes
To	Yes
Unsupported	Yes
User-Agent	Yes
Via	Yes
Warning	Yes
WWW-Authenticate	Yes

# SIP Session Description Protocol (SDP) Usage

SDP Headers	Supported?
v—Protocol version	Yes
o—Owner/creator and session identifier	Yes
a—Session name	Yes
c—Connection information	Yes
m—Media name and transport address	Yes



## SIP Call Flow s

---

SIP uses six request methods:

- INVITE—Indicates 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.

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 call flows for the following scenarios, which illustrate successful calls:

- Gateway-to Cisco SIP IP Phone—Successful Call Setup and Disconnect, page B-3
- Gateway-to-Cisco SIP IP Phone—Successful Call Setup and Call Hold, page B-7
- Gateway to-Cisco SIP IP Phone—Successful Call Setup and Call Transfer, page B-11
- Cisco SIP IP Phone-to-Cisco SIP IP Phone Simple Call Hold, page B-16
- Cisco SIP IP Phone-to-Cisco SIP IP Phone Call Hold with Consultation, page B-20
- Cisco SIP IP Phone-to-Cisco SIP IP Phone Call Waiting, page B-25
- Cisco SIP IP Phone-to-Cisco SIP IP Phone Call Transfer without Consultation, page B-31
- Cisco SIP IP Phone-to-Cisco SIP IP Phone Call Transfer with Consultation, page B-35
- Cisco SIP IP Phone-to-Cisco SIP IP Phone Network Call Forwarding (Unconditional), page B-41
- Cisco SIP IP Phone-to-Cisco SIP IP Phone Network Call Forwarding (Busy), page B-44
- Cisco SIP IP Phone-to-Cisco SIP IP Phone Network Call Forwarding (No Answer), page B-48
- Cisco SIP IP Phone-to Cisco SIP IP Phone 3-Way Calling, page B-52

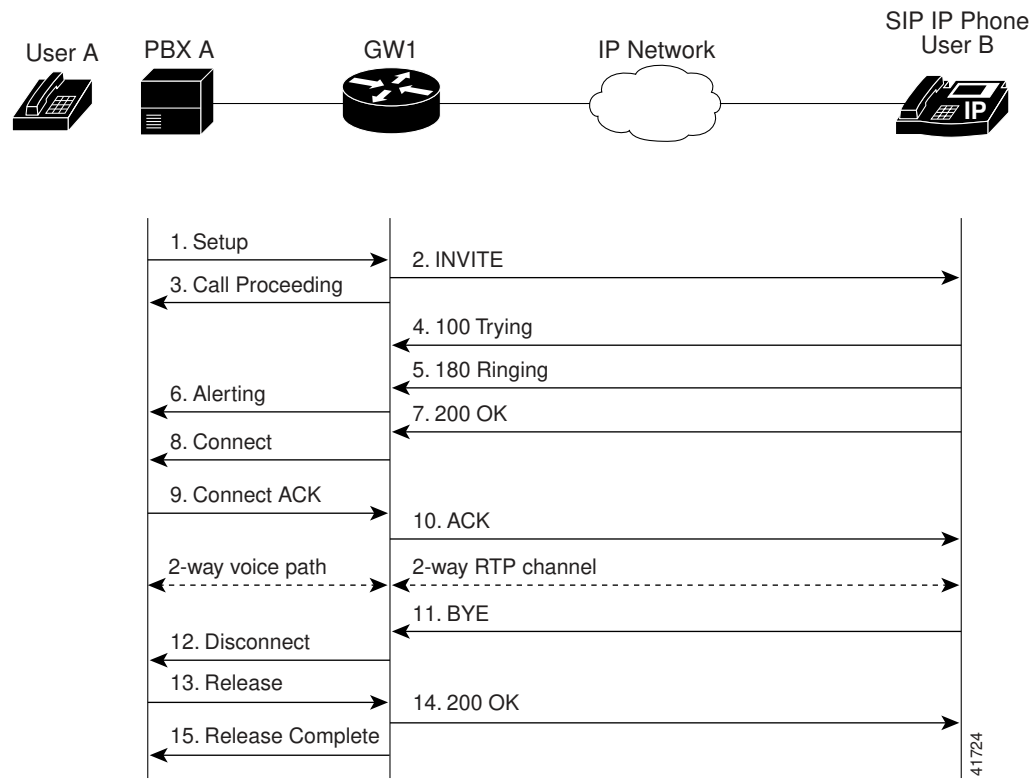
## Gateway-to Cisco SIP IP Phone— Successful Call Setup and Disconnect

Figure B-1 illustrates a successful gateway-to-Cisco SIP IP 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 Gateway-to-Cisco SIP IP Phone—Successful Setup and Disconnect





Step	Action	Description
1	Setup—PBX A to Gateway 1	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.
2	INVITE—Gateway 1 to Cisco SIP IP phone	<p>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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> <li>• The IP address of the Cisco SIP IP phone is inserted in the Request-URI field.</li> <li>• PBX A is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> <li>• The port on which the Gateway is prepared to receive the RTP data is specified.</li> </ul>
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.

## Call Flow Scenarios for Successful Calls

Step	Action	Description
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.
14	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 phone that Gateway 1 has received the BYE request.
15	Release Complete—Gateway 1 to PBX A	Gateway 1 sends a Release Complete message to PBX A and the call session is terminated.

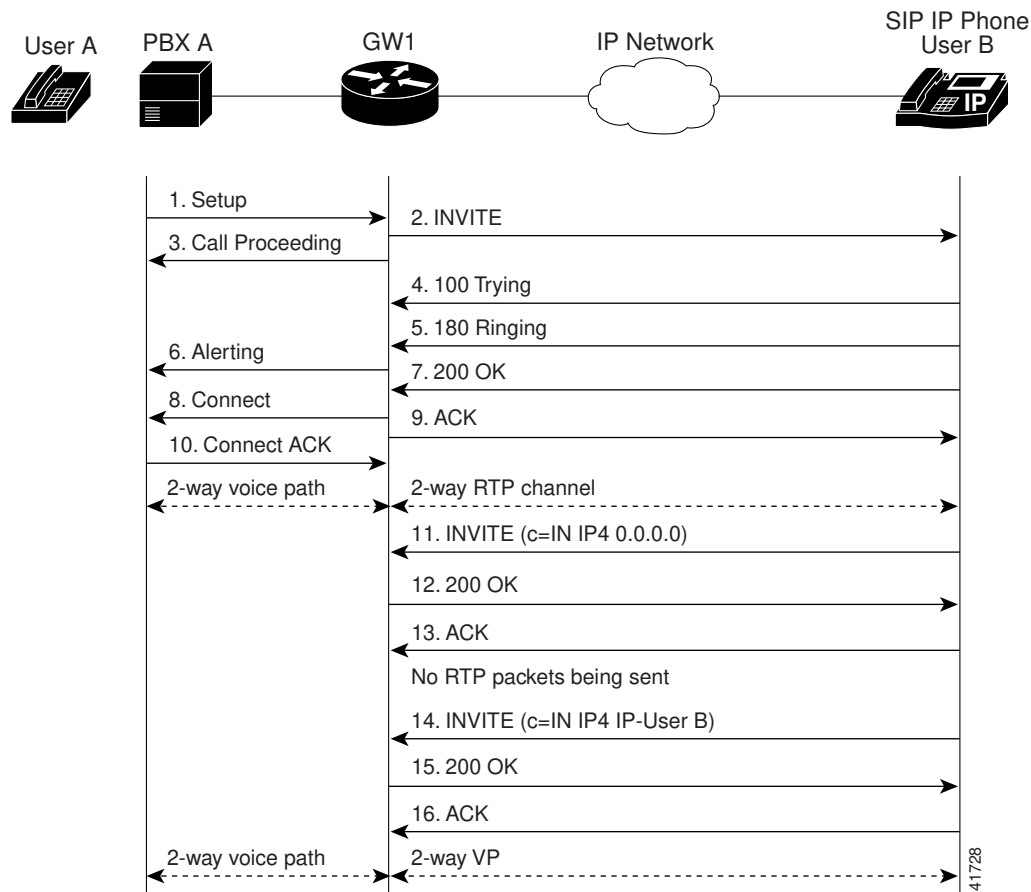
## Gateway-to-Cisco SIP IP Phone— Successful Call Setup and Call Hold

Figure B-2 illustrates a successful gateway-to-Cisco SIP IP 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 Gateway-to-Cisco SIP IP Phone Call—Successful Call Setup and Call Hold



Step	Action	Description
1	Setup—PBX A to Gateway 1	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.
2	INVITE—Gateway 1 to Cisco SIP IP phone	<p>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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> <li>• The IP address of the Cisco SIP IP phone is inserted in the Request-URI field.</li> <li>• PBX A is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> <li>• The port on which the Gateway is prepared to receive the RTP data is specified.</li> </ul>
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.

## Call Flow Scenarios for Successful Calls

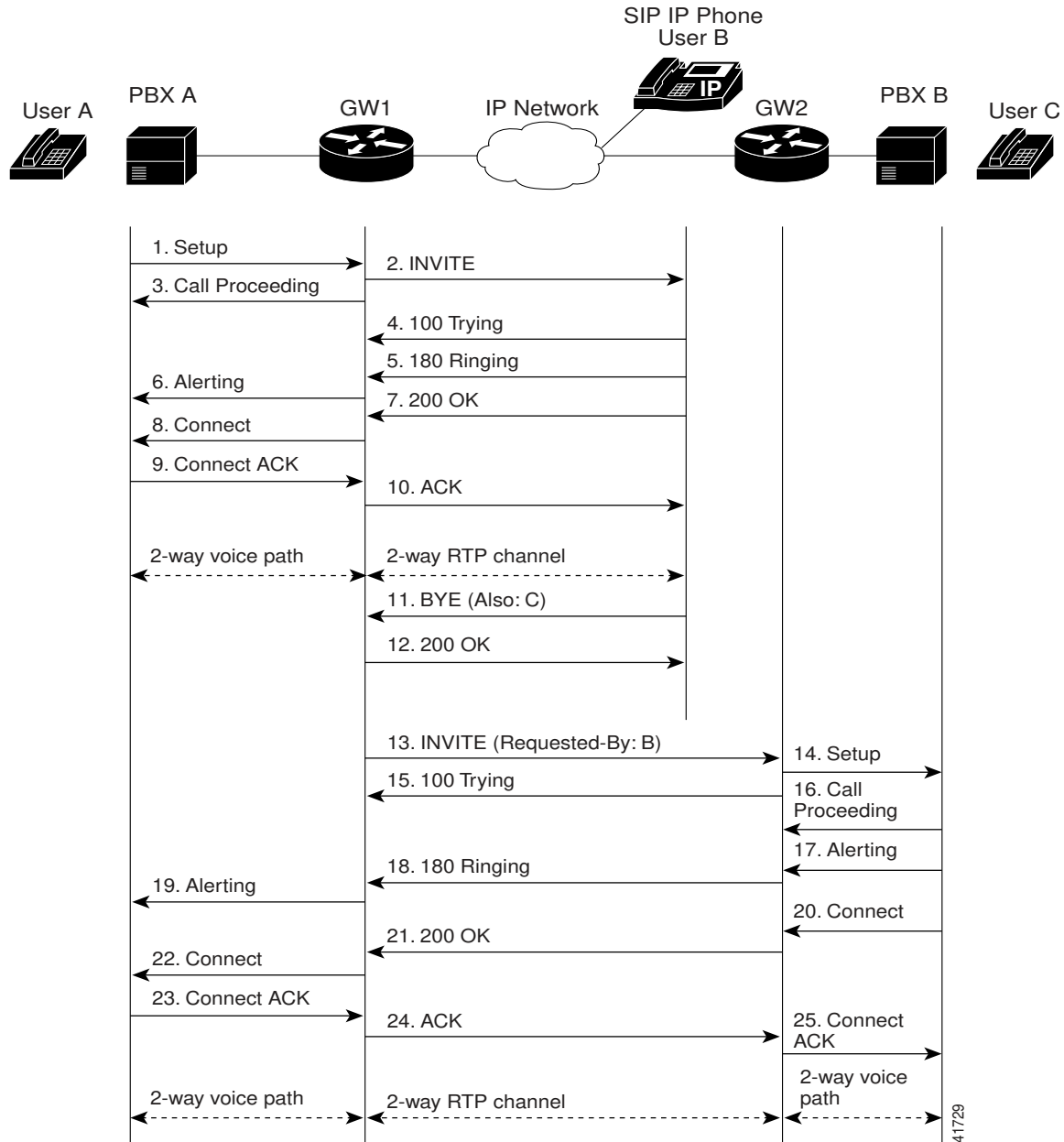
Step	Action	Description
6	Alerting—Gateway 1 to PBX A	Gateway 1 sends an Alert message to User A. The Alert message indicates that Gateway 1 has received a 180 Ringing response from the Cisco SIP IP phone. User A hears the ringback tone that indicates that User B is being alerted.
7	200 OK—Cisco SIP 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.
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.

## Gateway-to-Cisco SIP IP Phone—Successful Call Setup and Call Transfer

Figure B-3 illustrates a successful gateway-to-Cisco SIP IP phone PC call setup and call transfer without consultation. In this scenario, there are three end users: User A, User B, and User C. 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 and is directly connected to the IP network. User C is located at PBX B. PBX B is connected to Gateway 2 (SIP Gateway) via a T1/E1. Gateway 1, Gateway 2, and the Cisco SIP IP phone are connected to one another 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 transfers User A's call to User C and then hangs up.
4. User C answers the call.

**Figure B-3 Gateway-to-Cisco SIP IP Phone Call—Successful Call Setup and Call Transfer**



Step	Action	Description
1	Setup—PBX A to Gateway 1	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.
2	INVITE—Gateway 1 to Cisco SIP IP phone	<p>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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> <li>• The IP address of the Cisco SIP IP phone is inserted in the Request-URI field.</li> <li>• PBX A is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> <li>• The port on which the Gateway is prepared to receive the RTP data is specified.</li> </ul>
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.

## Call Flow Scenarios for Successful Calls

Step	Action	Description
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 Gateway 1 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	BYE—Cisco SIP IP phone to Gateway 1	<p>User B transfers User A's call to User C and then hangs up. The Cisco SIP IP phone sends a SIP BYE request to Gateway 1. The SIP BYE request includes the Also header. In this scenario, the Also header indicates that User C needs to be brought into the call while User B hangs up. This header distinguishes the call transfer BYE request from a normal disconnect BYE request.</p> <p>The Request-By header could be included in the BYE request, however, Cisco's implementation does not require the header to complete the transfer. If the Requested-By header is included, the INVITE sent to the transferred-to party will include the Requested-By header. If the Requested-By header is not included, the INVITE sent to the transferred-to party will not include the Requested-By header.</p>
12	200 OK—Gateway 1 to Cisco SIP IP phone	Gateway 1 sends a SIP 200 OK message to the Cisco SIP IP phone. The 200 OK response notifies the Cisco SIP IP phone that the BYE request has been received. The call session between User A and User B is now terminated.

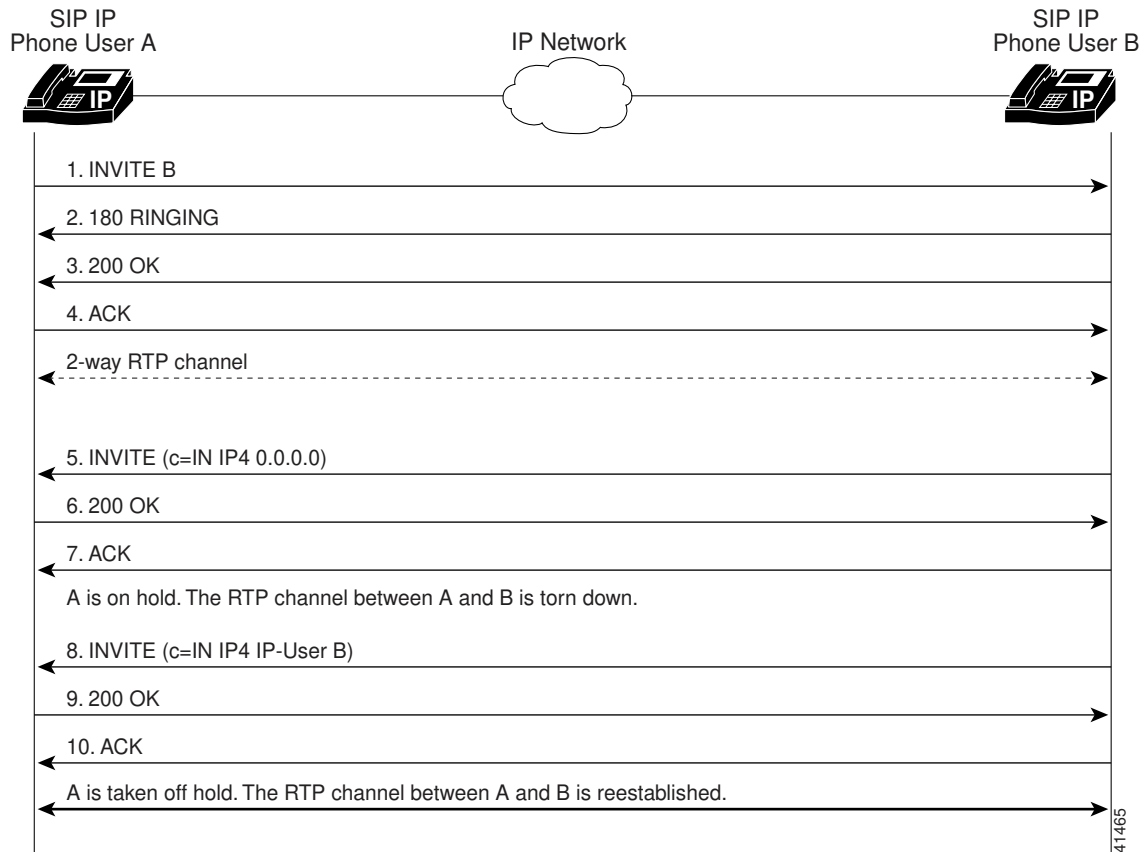
Step	Action	Description
13	INVITE—Gateway 1 to Gateway 2	Gateway 1 sends a SIP INVITE request to Gateway 2. In the INVITE request, a unique Call-ID is generated and the Requested-By field indicates that User B requested the call.
14	Setup—Gateway 2 to PBX B	Gateway 2 receives the INVITE request from Gateway 1 and initiates a Call Setup with User C via PBX B.
15	100 Trying—Gateway 2 to Gateway 1	Gateway 2 sends a SIP 100 Trying response to the INVITE request sent by Gateway 1. The 100 Trying response indicates that Gateway 2 has received the INVITE request but that User C has not yet been located.
16	Call Proceeding—PBX B to Gateway 2	PBX B sends a Call Proceeding message to Gateway 2. User C's phone begins to ring.
17	Alerting—PBX B to Gateway 2	PBX B sends an Alert message to Gateway 2.
18	180 Ringing—Gateway 2 to Gateway 1	Gateway 2 sends a SIP 180 Ringing response to Gateway 1. The 180 Ringing response indicates that Gateway 2 has located, and is trying to alert, User C.
19	Connect—PBX B to Gateway 2	User C answers the phone. PBX B sends a Connect message to Gateway 2. The Connect message notifies Gateway 2 that the connection has been made.
20	200 OK—Gateway 2 to Gateway 1	Gateway 2 sends a SIP 200 OK response to Gateway 1. The 200 OK response notifies Gateway 1 that the connection has been made.  If User C supports the media capability advertised in the INVITE message sent by User A, it advertises the intersection of its own and User A's media capability in the 200 OK response. If User C does not support the media capability advertised by User A, it sends back a 400 Bad Request response with a 304 Warning header field.
21	Connect ACK—Gateway 2 to PBX B	Gateway 2 acknowledges PBX B's Connect message.
22	ACK—Gateway 1 to Gateway 2	Gateway 1 sends a SIP ACK to Gateway 2. The ACK confirms that Gateway 1 has received the 200 OK message from Gateway 2.

## Cisco SIP IP Phone-to-Cisco SIP IP Phone 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 Cisco SIP IP Phone-to-Cisco SIP IP Phone Simple Call Hold**

Step	Action	Description
1	INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B	<p>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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> <li>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 email address (<i>user@host</i> where <i>user</i> is the telephone number and <i>host</i> 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 user name.</li> <li>Cisco SIP IP phone A is identified as the call session initiator in the From field.</li> <li>A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>The transaction number within a single call leg is identified in the CSeq field.</li> <li>The media capability User A is ready to receive is specified.</li> </ul>
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	Action	Description
3	200 OK—Cisco SIP IP phone B to Cisco SIP IP phone A	<p>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.</p> <p>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.</p>
4	ACK—Cisco SIP IP phone A to Cisco SIP IP phone B	<p>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.</p> <p>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.</p>
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 B to Cisco SIP IP phone A	<p>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.</p> <p>Call_ID=1 SDP: c=IN IP4 0.0.0.0</p> <p>The c= SDP field of the SIP INVITE contains an 0.0.0.0. This places the call in limbo.</p>
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.
7	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.		

Step	Action	Description
8	INVITE—Cisco SIP IP phone B to Cisco SIP IP phone A	<p>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.</p> <p>Call_ID=1 SDP: c=IN IP4 181.23.250.2</p> <p>To reestablish the call between phone A and phone B, the IP address of phone B is inserted into the c= SDP field.</p>
9	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.
10	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.

A two-way RTP channel is reestablished between IP phone A and IP phone B.

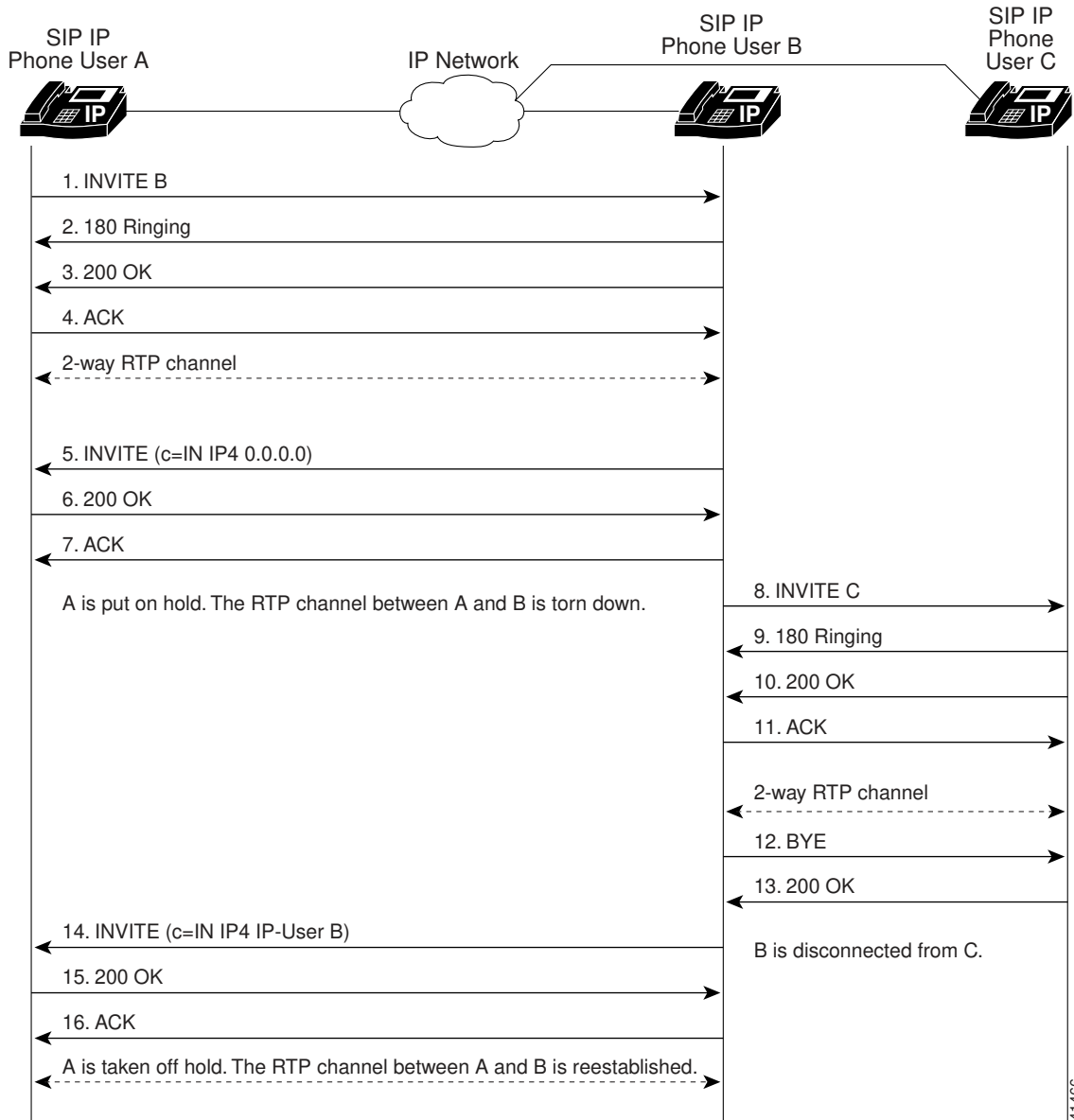
## Cisco SIP IP Phone-to-Cisco SIP IP Phone Call Hold with Consultation

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 Cisco SIP IP Phone-to-Cisco SIP IP Phone Call Hold with Consultation**

Step	Action	Description
1	INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B	<p>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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> <li>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 email address (<i>user@host</i> where <i>user</i> is the telephone number and <i>host</i> 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 user name.</li> <li>Cisco SIP IP phone A is identified as the call session initiator in the From field.</li> <li>A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>The transaction number within a single call leg is identified in the CSeq field.</li> <li>The media capability User A is ready to receive is specified.</li> </ul>
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	Action	Description
3	200 OK—Cisco SIP IP phone B to Cisco SIP IP phone A	<p>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.</p> <p>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.</p>
4	ACK—Cisco SIP IP phone A to Cisco SIP IP phone B	<p>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.</p> <p>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.</p>
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 B to Cisco SIP IP phone A	<p>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.</p> <p>Call_ID=1 SDP: c=IN IP4 0.0.0.0</p> <p>The c= SDP field of the SIP INVITE contains 0.0.0.0. This places the call in limbo.</p>
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.
7	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.		

## Call Flow Scenarios for Successful Calls

Step	Action	Description
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 C to participate in a call session.
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 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.
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 Cisco SIP IP phone B and Cisco SIP IP phone C.		
12	BYE—Cisco SIP IP phone B to Cisco SIP IP phone C	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.
13	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. The call session between User A and User B is now terminated.

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

Step	Action	Description
14	INVITE—Cisco SIP IP phone B to Cisco SIP IP phone A	<p>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.</p> <p>Call_ID=1 SDP: c=IN IP4 181.23.250.2</p> <p>To reestablish the call between phone A and phone B, the IP address of phone B is inserted into the c= SDP field.</p>
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 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.

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

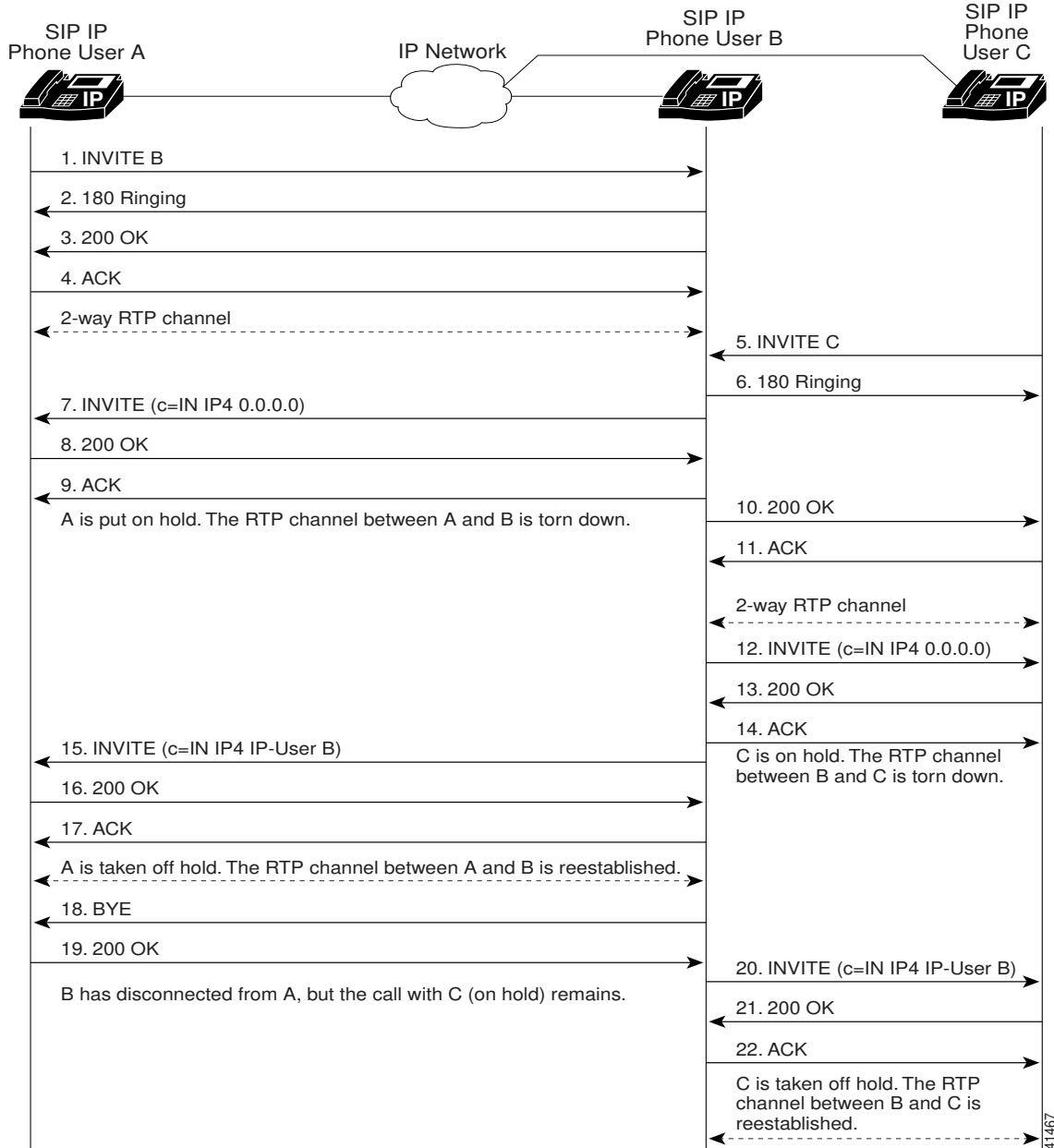
## Cisco SIP IP Phone-to-Cisco SIP IP Phone Call Waiting

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.

Figure B-6 Cisco SIP IP Phone-to-Cisco SIP IP Phone Call Waiting



Step	Action	Description
1	INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B	<p>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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"><li>• 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 email address (<i>user@host</i> where <i>user</i> is the telephone number and <i>host</i> 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 user name.</li><li>• Cisco SIP IP phone A is identified as the call session initiator in the From field.</li><li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li><li>• The transaction number within a single call leg is identified in the CSeq field.</li><li>• The media capability User A is ready to receive is specified.</li></ul>
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.

## Call Flow Scenarios for Successful Calls

Step	Action	Description
3	200 OK—Cisco SIP IP phone B to Cisco SIP IP phone A	<p>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.</p> <p>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.</p>
4	ACK—Cisco SIP IP phone A to Cisco SIP IP phone B	<p>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.</p> <p>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.</p>
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.
7	INVITE—Cisco SIP IP phone B to Cisco SIP IP phone A	<p>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.</p> <pre>Call_ID=1 SDP: c=IN IP4 0.0.0.0</pre> <p>The c= SDP field of the SIP INVITE contains 0.0.0.0. This places the call in limbo.</p>
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.



Step	Action	Description
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.
A 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.  <code>Call_ID=2</code> <code>SDP: c=IN IP4 0.0.0.0</code>  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.		

## Call Flow Scenarios for Successful Calls

Step	Action	Description
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 181.23.250.2
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.
17	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.
A two-way RTP channel is reestablished between Cisco SIP IP phone A and Cisco SIP IP phone B.		
18	BYE—Cisco SIP IP phone B to Cisco SIP IP phone A	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.
19	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. The call session between User A and User B is now terminated.
The RTP channel between Cisco SIP IP phone A and Cisco SIP IP phone B is torn down.		
14	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 181.23.250.2
15	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.

Step	Action	Description
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 A.

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

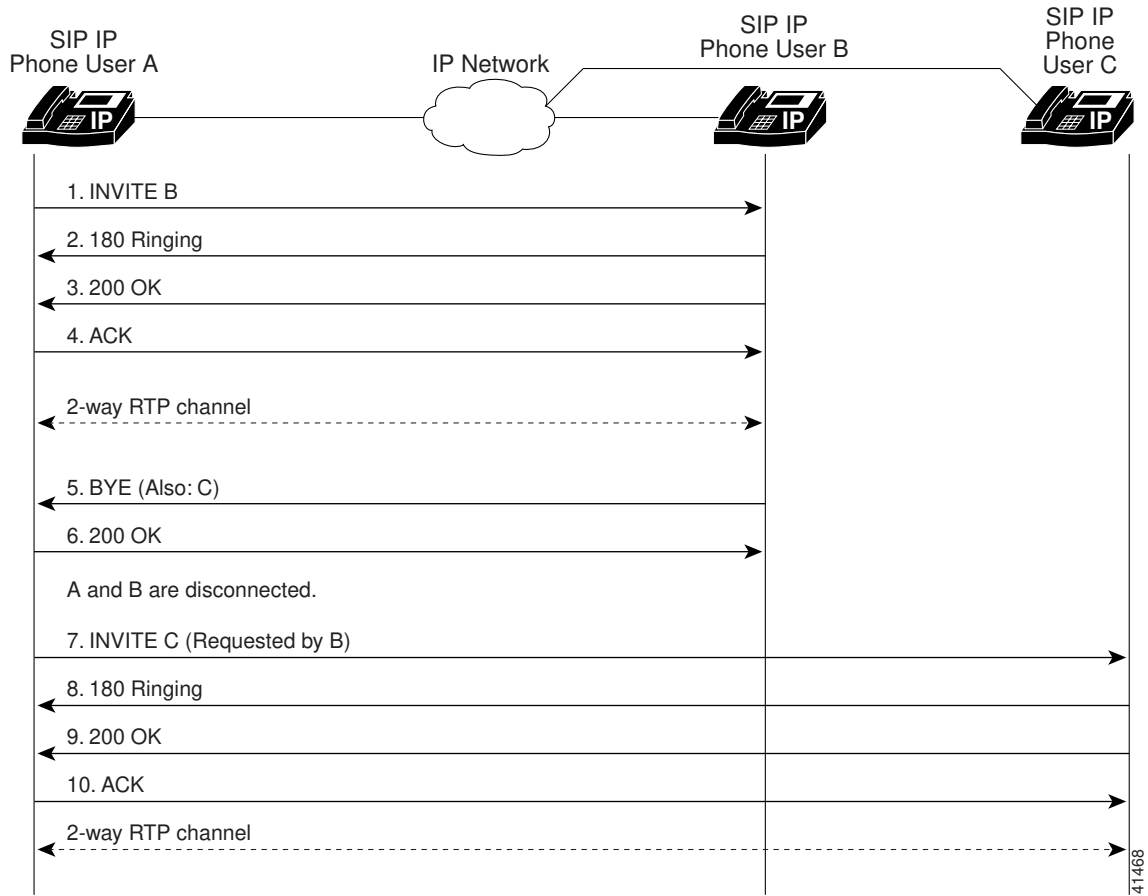
## Cisco SIP IP Phone-to-Cisco SIP IP Phone Call Transfer without Consultation

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 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.

Figure B-7 Cisco SIP IP Phone-to-Cisco SIP IP Phone Call Transfer without Consultation



Step	Action	Description
1	INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B	<p>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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"><li>• 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 email address (<i>user@host</i> where <i>user</i> is the telephone number and <i>host</i> 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 user name.</li><li>• Cisco SIP IP phone A is identified as the call session initiator in the From field.</li><li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li><li>• The transaction number within a single call leg is identified in the CSeq field.</li><li>• The media capability User A is ready to receive is specified.</li></ul>
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.

## Call Flow Scenarios for Successful Calls

Step	Action	Description
3	200 OK—Cisco SIP IP phone B to Cisco SIP IP phone A	<p>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.</p> <p>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.</p>
4	ACK—Cisco SIP IP phone A to Cisco SIP IP phone B	<p>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.</p> <p>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.</p>
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.		
5	BYE—Cisco SIP IP phone B to Cisco SIP IP phone A	<p>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.</p> <p>The SIP BYE request includes the Also header. The Also header indicates that User C needs to be brought into the call while User B hangs up. The header distinguishes the call transfer BYE request from a normal disconnect BYE request.</p>
6	200 OK—Cisco SIP IP phone A to Cisco SIP IP phone B	<p>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.</p>

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

Step	Action	Description
7	INVITE—Cisco SIP IP phone A to Cisco SIP IP phone C (Requested by Cisco SIP IP phone B)	At the request of 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.
8	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.
9	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.
10	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.

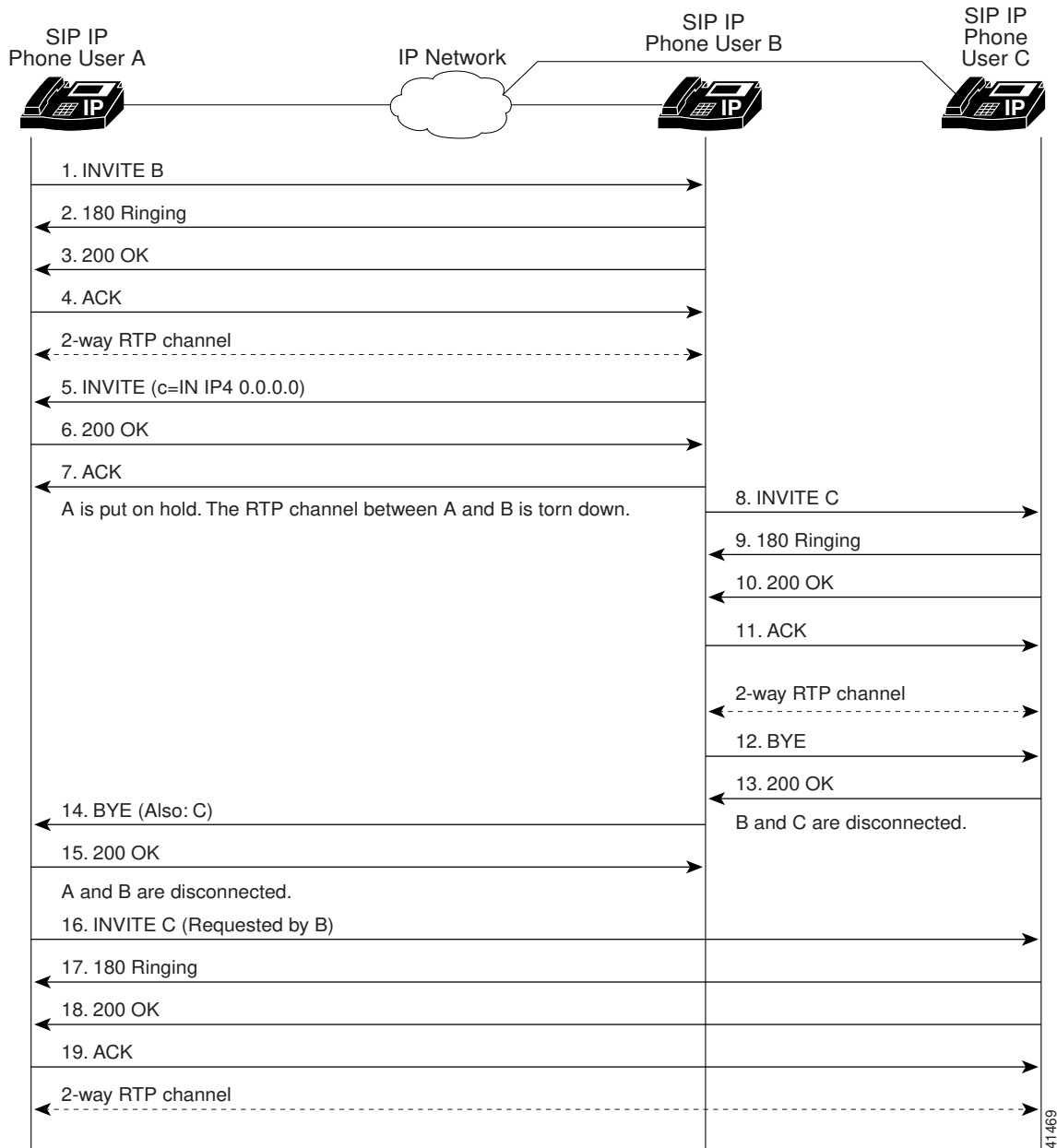
A two-way RTP channel is established between Cisco SIP IP phone A and Cisco SIP IP phone C.

## Cisco SIP IP Phone-to-Cisco SIP IP Phone Call Transfer with Consultation

Figure B-8 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.

**Figure B-8 Cisco SIP IP Phone-to-Cisco SIP IP Phone Call Transfer with Consultation**

41469



Step	Action	Description
1	INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B	<p>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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"><li>• 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 email address (<i>user@host</i> where <i>user</i> is the telephone number and <i>host</i> 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 user name.</li><li>• Cisco SIP IP phone A is identified as the call session initiator in the From field.</li><li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li><li>• The transaction number within a single call leg is identified in the CSeq field.</li><li>• The media capability User A is ready to receive is specified.</li></ul>
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.

## Call Flow Scenarios for Successful Calls

Step	Action	Description
3	200 OK—Cisco SIP IP phone B to Cisco SIP IP phone A	<p>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.</p> <p>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.</p>
4	ACK—Cisco SIP IP phone A to Cisco SIP IP phone B	<p>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.</p> <p>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.</p>
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.		
5	INVITE—Cisco SIP IP phone B to Cisco SIP IP phone A	<p>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.</p> <p>Call_ID=1 SDP: c=IN IP4 0.0.0.0</p>
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.
7	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.		
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 C to participate in a call session.

Step	Action	Description
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	<p>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.</p> <p>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.</p>
11	ACK—Cisco SIP IP phone B to Cisco SIP IP phone C	<p>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.</p> <p>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.</p>
A two-way RTP channel is established between Cisco SIP IP phone B and Cisco SIP IP phone C.		
12	BYE—Cisco SIP IP phone B to Cisco SIP IP phone C	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.
13	200 OK—Cisco SIP IP phone C to Cisco SIP IP phone B	<p>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.</p> <p>The call session between User A and User B is now terminated.</p>
The RTP channel between Cisco SIP IP phone B and Cisco SIP IP phone C is torn down.		

# Call Flow Scenarios for Successful Calls

Step	Action	Description
14	BYE—Cisco SIP IP phone B to Cisco SIP IP phone A	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 SIP BYE request includes the Also header. The Also header indicates that User C needs to be brought into the call while User B hangs up. The header distinguishes the call transfer BYE request from a normal disconnect BYE request.
15	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. The call session between User A and User B is now terminated.

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

16	INVITE—Cisco SIP IP phone A to Cisco SIP IP phone C (Requested by Cisco SIP IP phone B)	At the request of 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.
17	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.
18	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.
19	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.

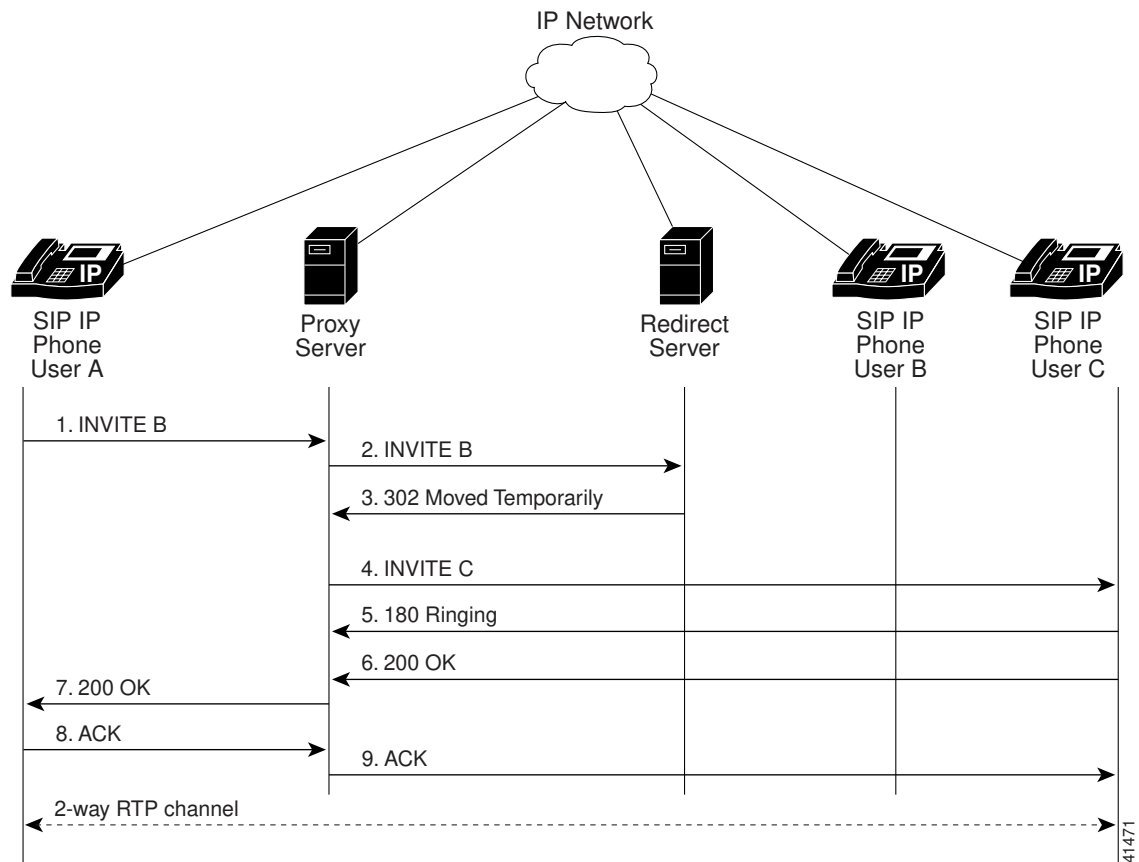
A two-way RTP channel is established between Cisco SIP IP phone A and Cisco SIP IP phone C.

## Cisco SIP IP Phone-to-Cisco SIP IP Phone Network Call Forwarding (Unconditional)

Figure B-9 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-9 Cisco SIP IP Phone-to-Cisco SIP IP Phone Network Call Forwarding (Unconditional)**

Step	Action	Description
1	INVITE—Cisco SIP IP phone A to SIP proxy server	<p>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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> <li>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 email address (<i>user@host</i> where <i>user</i> is the telephone number and <i>host</i> 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 user name.</li> <li>Cisco SIP IP phone A is identified as the call session initiator in the From field.</li> <li>A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>The transaction number within a single call leg is identified in the CSeq field.</li> <li>The media capability User A is ready to receive is specified.</li> </ul>
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.

Step	Action	Description
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.

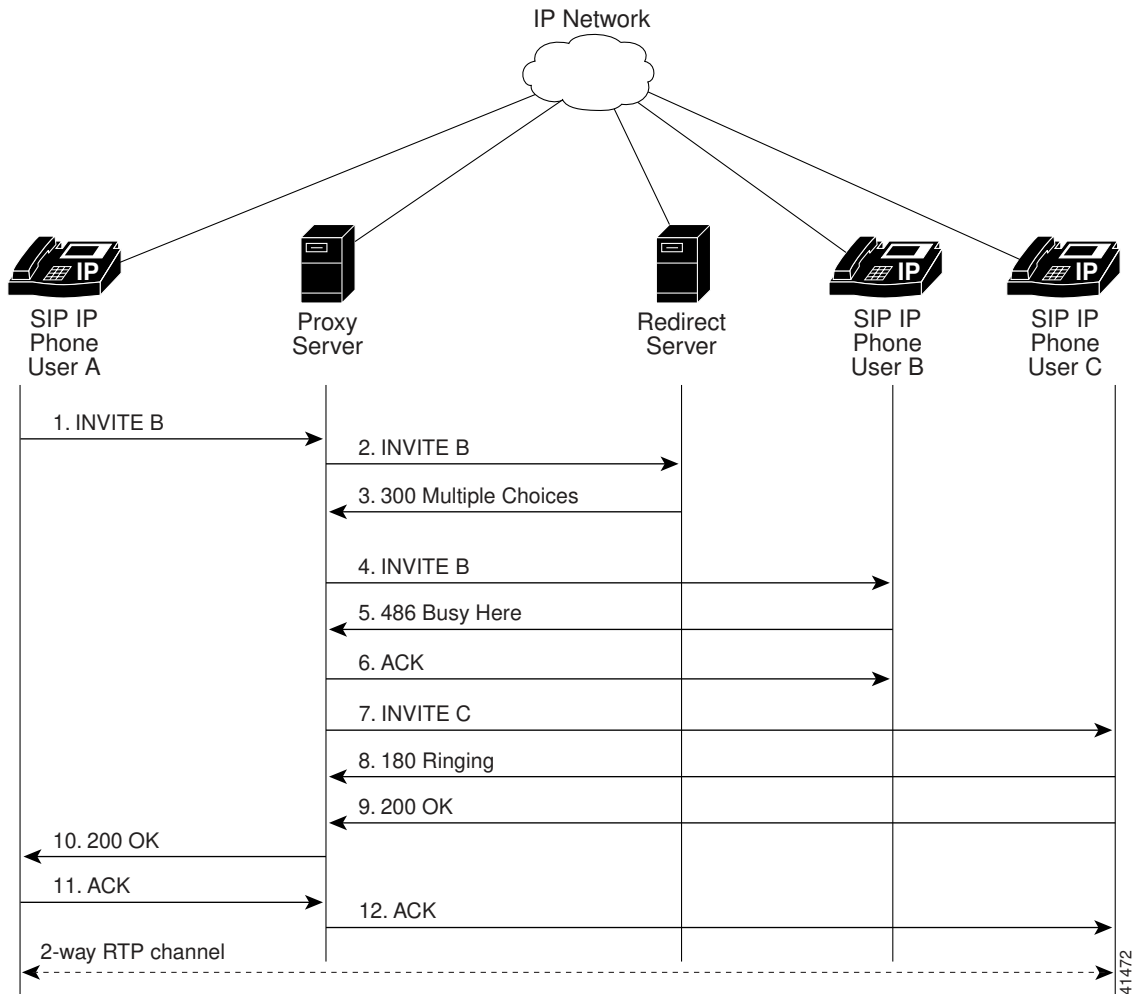
## Cisco SIP IP Phone-to-Cisco SIP IP Phone Network Call Forwarding (Busy)

Figure B-10 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.



**Figure B-10 Cisco SIP IP Phone-to-Cisco SIP IP Phone Network Call Forwarding (Busy)**

Step	Action	Description
1	INVITE—Cisco SIP IP phone A to SIP proxy server	<p>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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> <li>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 email address (<i>user@host</i> where <i>user</i> is the telephone number and <i>host</i> 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 user name.</li> <li>Cisco SIP IP phone A is identified as the call session initiator in the From field.</li> <li>A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>The transaction number within a single call leg is identified in the CSeq field.</li> <li>The media capability User A is ready to receive is specified.</li> </ul>
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.

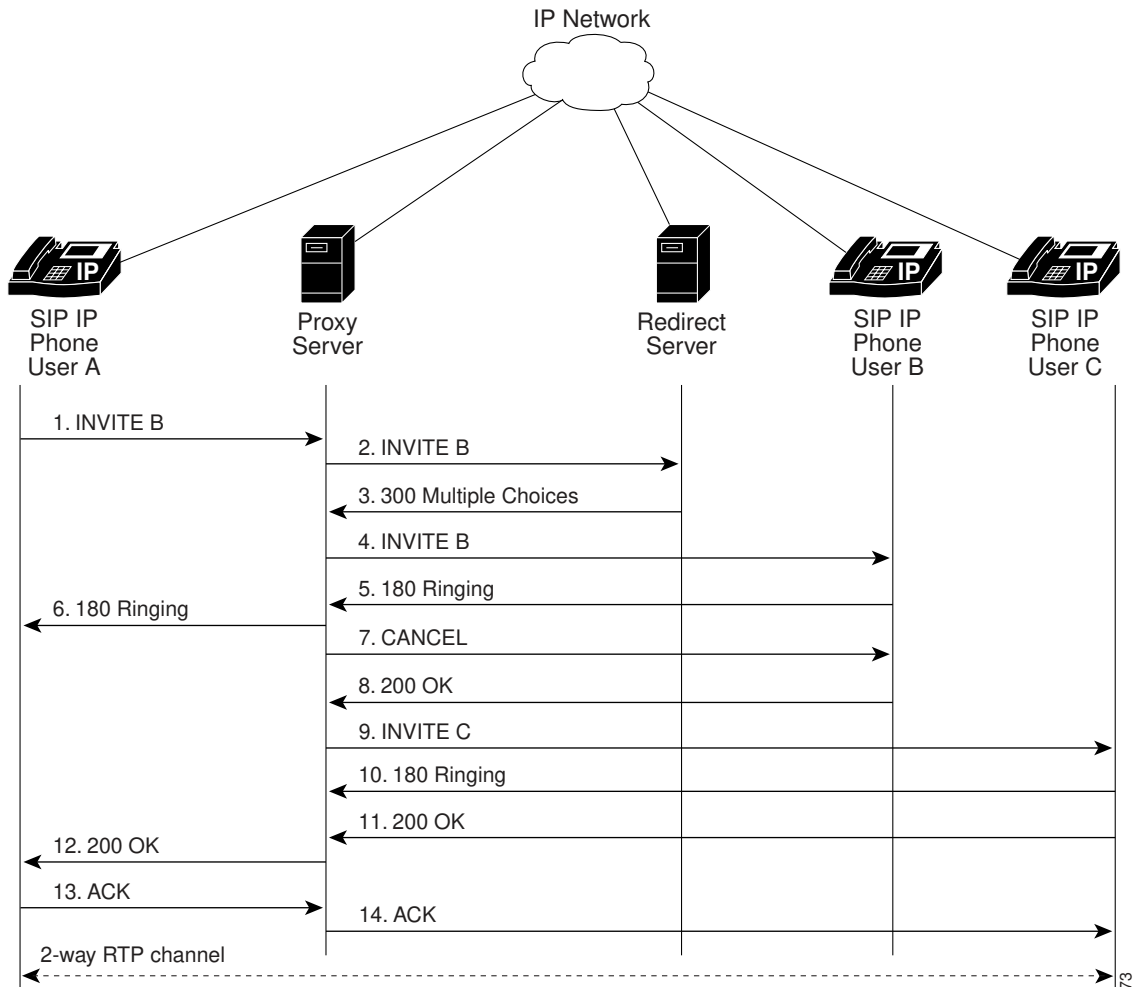
Step	Action	Description
5	486 Busy Here—Cisco SIP IP phone B to SIP proxy server	Cisco SIP IP phone B sends a 486 Busy here message to the SIP proxy server. The message indicates that Cisco SIP IP phone B is in use and the user is not willing or able to take additional calls.
6	ACK—SIP proxy server to 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
9	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.
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.
11	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 Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone C.
12	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.

## Cisco SIP IP Phone-to-Cisco SIP IP Phone Network Call Forwarding (No Answer)

Figure B-11 illustrates successful call forwarding between Cisco SIP IP phones in which User B has requested call forwarding from the network in the event 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 their 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.

**Figure B-11 Cisco SIP IP Phone-to-Cisco SIP IP Phone Network Call Forwarding (No Answer)**

Step	Action	Description
1	INVITE—Cisco SIP IP phone A to SIP proxy server	<p>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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> <li>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 email address (<i>user@host</i> where <i>user</i> is the telephone number and <i>host</i> 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 user name.</li> <li>Cisco SIP IP phone A is identified as the call session initiator in the From field.</li> <li>A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>The transaction number within a single call leg is identified in the CSeq field.</li> <li>The media capability User A is ready to receive is specified.</li> </ul>
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	180 Ringing—Cisco SIP IP phone B to SIP proxy server	Cisco SIP IP phone B sends a SIP 180 Ringing response to the SIP proxy server.

Step	Action	Description
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.
The timeout expires before the phone is answered.		
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.
13	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 Cisco SIP IP phone A has received the 200 OK response from Cisco SIP IP phone C.
14	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.

## Cisco SIP IP Phone-to Cisco SIP IP Phone 3-Way Calling

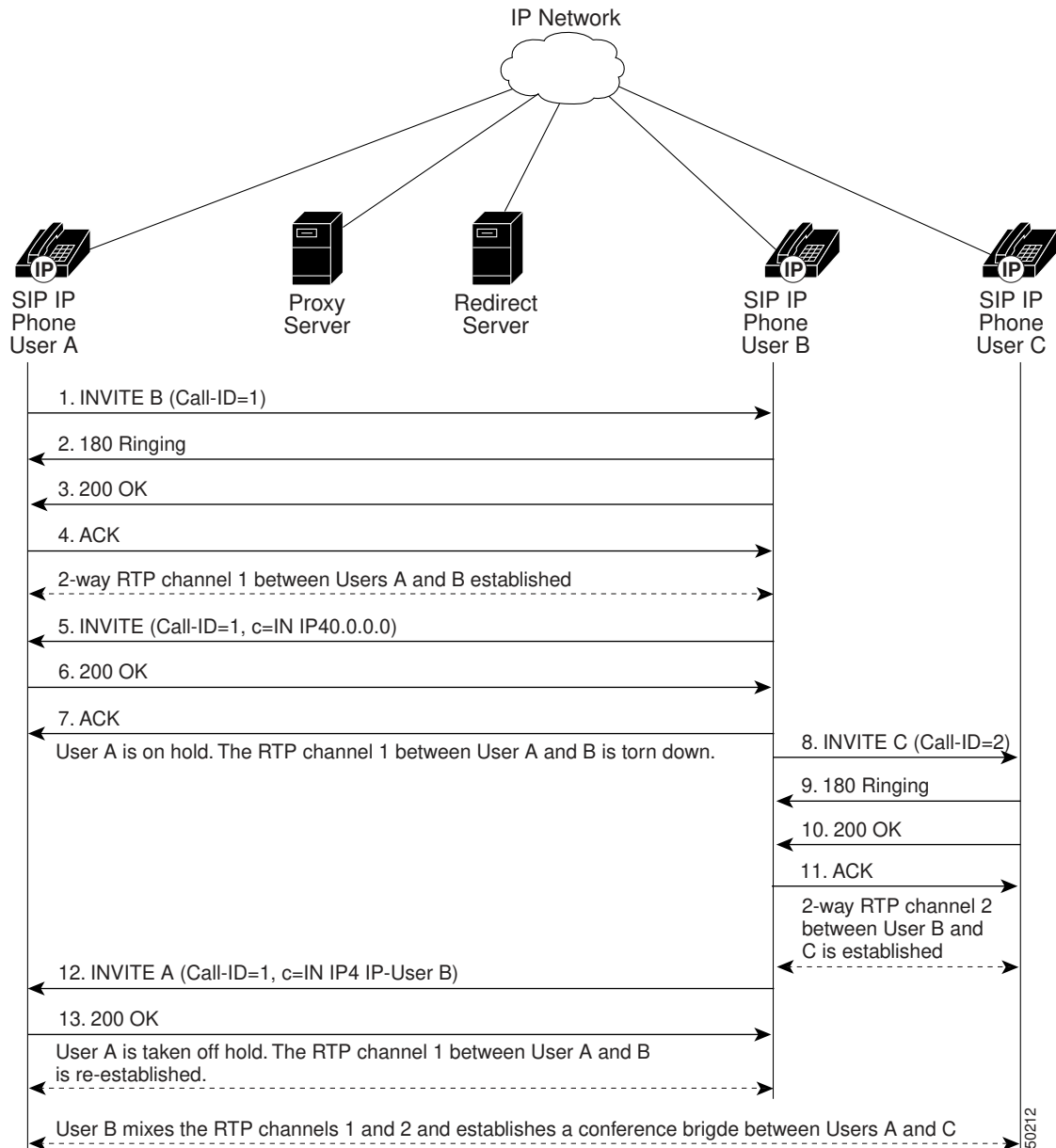
Figure B-11 illustrates successful 3-way calling between Cisco SIP IP phones in which User B mixes two RTP channels and therefore establishes a conference bridge between User A and User C. In this call flow scenario, the end users are User A, User B, and User C. They are all using Cisco SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:

5. User A calls User B.
6. User B answers the call.
7. User B puts User A on hold.
8. User B calls User C.
9. User C answers the call.
10. User B takes User A off hold.



Figure B-12 Cisco SIP IP Phone-to Cisco SIP IP Phone 3-Way Calling



Step	Action	Description
1	INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B	<p>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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> <li>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 email address (<i>user@host</i> where <i>user</i> is the telephone number and <i>host</i> 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 user name.</li> <li>Cisco SIP IP phone A is identified as the call session initiator in the From field.</li> <li>A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>The transaction number within a single call leg is identified in the CSeq field.</li> <li>The media capability User A is ready to receive is specified.</li> </ul>
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	Action	Description
3	200 OK—Cisco SIP IP phone B to Cisco SIP IP phone A	<p>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.</p> <p>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.</p>
4	ACK—Cisco SIP IP phone A to Cisco SIP IP phone B	<p>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.</p> <p>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.</p>
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 B to Cisco SIP IP phone A	<p>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.</p> <p>Call_ID=1 SDP: c=IN IP4 0.0.0.0</p> <p>The c= SDP field of the SIP INVITE contains an 0.0.0.0. This places the call in limbo.</p>
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.
7	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. User A is put on hold.		

Step	Action	Description
8	INVITE—Cisco SIP IP phone B to Cisco SIP IP phone C	<p>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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> <li>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 email address (<i>user@host</i> where <i>user</i> is the telephone number and <i>host</i> 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 user name.</li> <li>Cisco SIP IP phone B is identified as the call session initiator in the From field.</li> <li>A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>The transaction number within a single call leg is identified in the CSeq field.</li> <li>The media capability User B is ready to receive is specified.</li> </ul>
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.

Step	Action	Description
10	200 OK—Cisco SIP IP phone C to Cisco SIP IP phone B	<p>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.</p> <p>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.</p>
11	ACK—Cisco SIP IP phone B to Cisco SIP IP phone C	<p>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.</p> <p>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.</p>
A two-way RTP channel is established between SIP IP phone B and SIP IP phone C.		
12	INVITE—Cisco SIP IP phone B to Cisco SIP IP phone A	<p>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.</p> <p>Call_ID=1 SDP: c=IN IP4 181.23.250.2</p> <p>To reestablish the call between phone A and phone B, the IP address of phone B is inserted into the c= SDP field.</p>
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 Flow Scenarios for Failed Calls

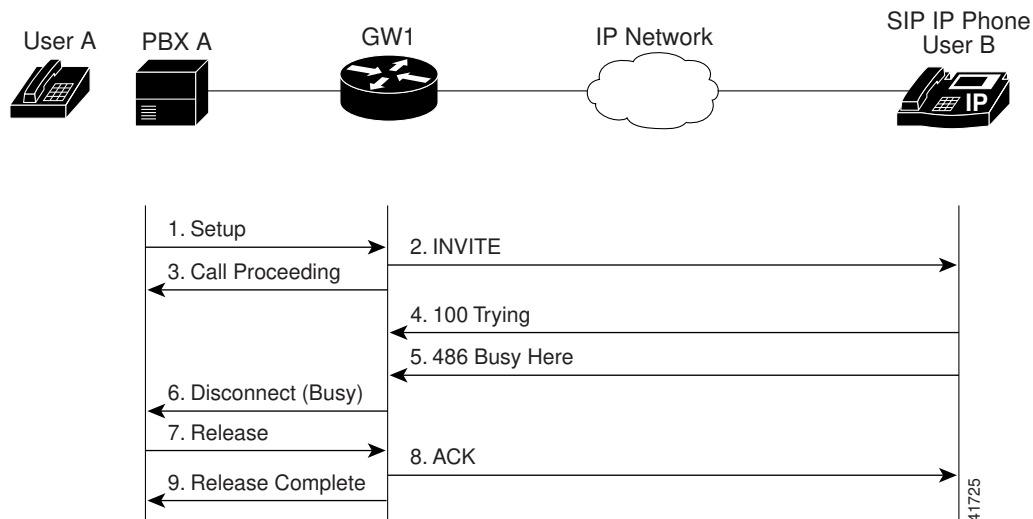
This section describes call flows for the following scenarios, which illustrate unsuccessful calls:

- Gateway-to-Cisco SIP IP Phone—Called User is Busy, page B-58
- Gateway-to-Cisco SIP IP Phone—Called User Does Not Answer, page B-60
- Gateway-to-Cisco SIP IP Phone—Client, Server, or Global Error, page B-63
- Cisco SIP IP Phone-to-Cisco SIP IP Phone—Called User is Busy, page B-66
- Cisco SIP IP Phone-to-Cisco SIP IP Phone—Called User Does Not Answer, page B-68
- Cisco SIP IP Phone-to-Cisco SIP IP Phone—Authentication Error, page B-70

### Gateway-to-Cisco SIP IP Phone—Called User is Busy

Figure B-13 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-13 Gateway-to-Cisco SIP IP Phone—Called User is Busy**



Step	Action	Description
1	Setup—PBX A to Gateway 1	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.
2	INVITE—Gateway 1 to Cisco SIP IP phone	<p>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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> <li>• The IP address of the Cisco SIP IP phone is inserted in the Request-URI field.</li> <li>• PBX A is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> <li>• The port on which the Gateway is prepared to receive the RTP data is specified.</li> </ul>
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 User B was not willing or was unable to take the call.

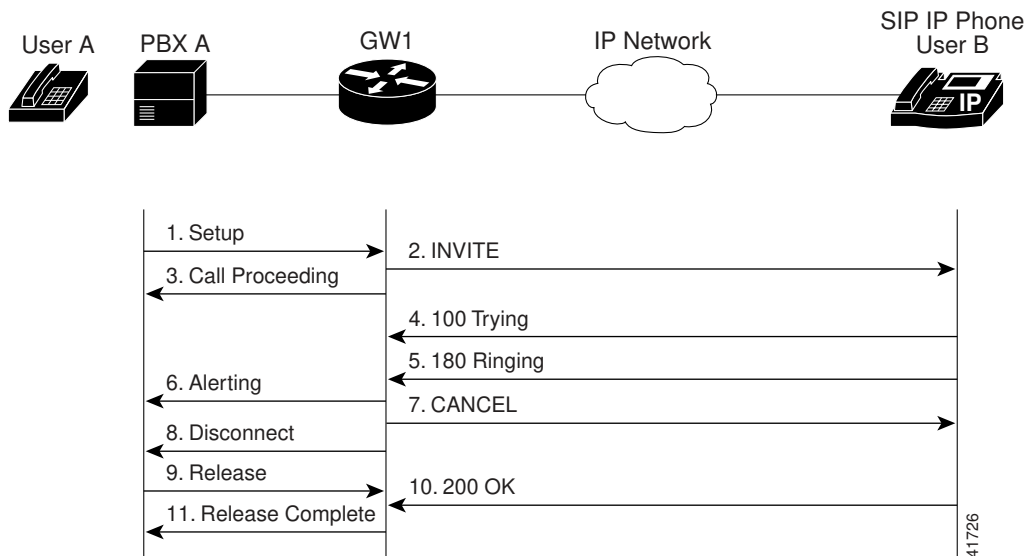
## Call Flow Scenarios for Failed Calls

Step	Action	Description
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.

## Gateway-to-Cisco SIP IP Phone—Called User Does Not Answer

Figure B-14 illustrates the call flow in which User A initiates a call to User B but User B does not answer.

**Figure B-14 Gateway-to-Cisco SIP IP Phone—Called User Does Not Answer**





Step	Action	Description
1	Setup—PBX A to Gateway 1	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.
2	INVITE—Gateway 1 to Cisco SIP IP phone	<p>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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> <li>• The IP address of the Cisco SIP IP phone is inserted in the Request-URI field.</li> <li>• PBX A is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> <li>• The port on which the Gateway is prepared to receive the RTP data is specified.</li> </ul>
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 PBX A.

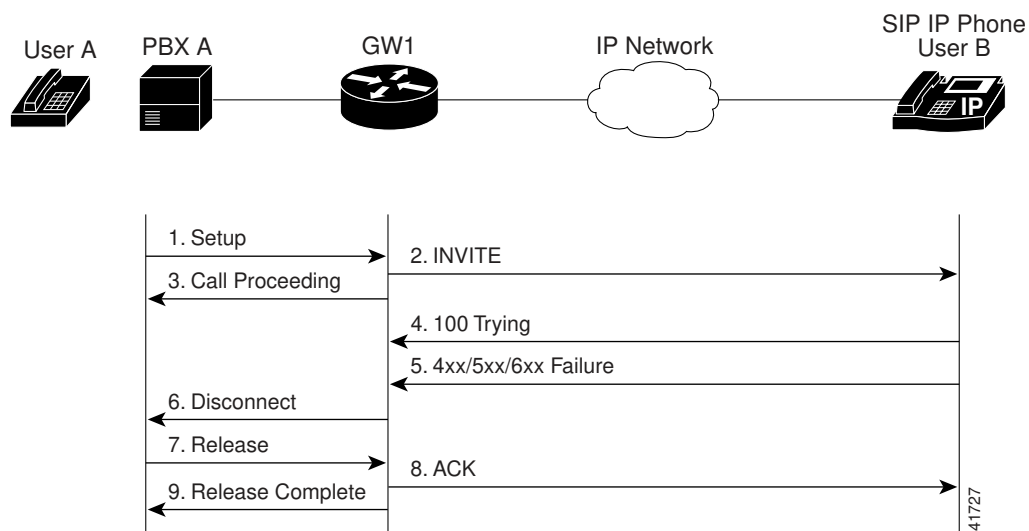
## Call Flow Scenarios for Failed Calls

Step	Action	Description
7	CANCEL (Ring Timeout)—Gateway 1 to Cisco SIP IP phone	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.
8	Disconnect—Gateway 1 to PBX A	Gateway 1 sends a Disconnect message to PBX A.
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.
10	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 confirms that User A has received the 486 Busy Here response. The call session attempt is now being terminated.
11	Release Complete—Gateway 1 to PBX A	Gateway 1 sends a Release Complete message to PBX A and the call session is terminated.

## Gateway-to-Cisco SIP IP Phone—Client, Server, or Global Error

Figure B-15 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-15 Gateway-to-Cisco SIP IP Phone—Client, Server, or Global Error**



# Call Flow Scenarios for Failed Calls

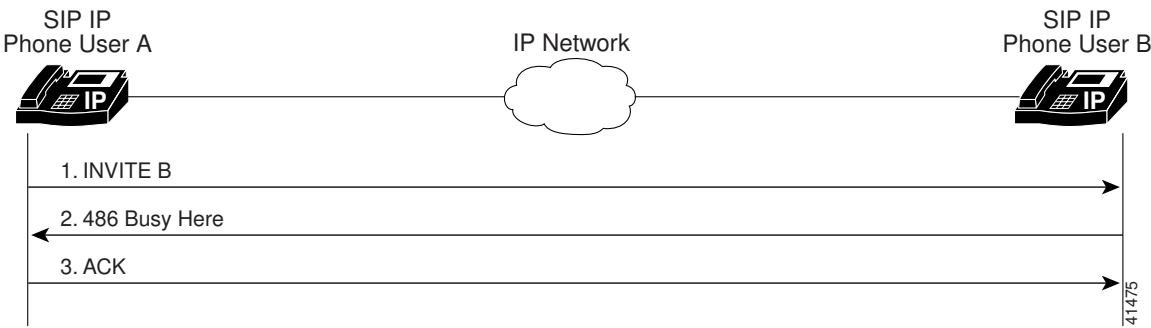
Step	Action	Description
1	Setup—PBX A to Gateway 1	Call Setup is initiated between PBX A and Gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.
2	INVITE—Gateway 1 to Cisco SIP IP phone	<p>Gateway 1 maps the SIP URL phone number to a dial-peer. 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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> <li>• The IP address of the Cisco SIP IP phone is inserted in the Request-URI field.</li> <li>• PBX A is identified as the call session initiator in the From field.</li> <li>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>• The transaction number within a single call leg is identified in the CSeq field.</li> <li>• The media capability User A is ready to receive is specified.</li> <li>• The port on which the Gateway is prepared to receive the RTP data is specified.</li> </ul>
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.

Step	Action	Description
5	4xx/5xx/6xx Failure—Cisco SIP IP phone to Gateway 1	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
6	Disconnect—Gateway 1 to PBX A	Gateway 1 sends a Release 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.

# Cisco SIP IP Phone-to-Cisco SIP IP Phone— Called User is Busy

Figure B-16 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-16 Cisco SIP IP Phone-to-Cisco SIP IP Phone—Called User is Busy

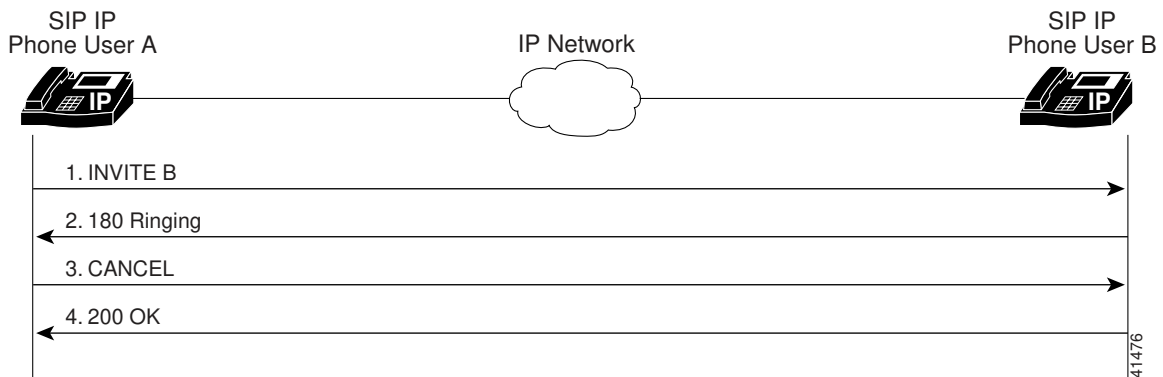


Step	Action	Description
1	INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B	<p>Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> <li>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 email address (<i>user@host</i> where <i>user</i> is the telephone number and <i>host</i> 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 user name.</li> <li>Cisco SIP IP phone A is identified as the call session initiator in the From field.</li> <li>A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>The transaction number within a single call leg is identified in the CSeq field.</li> <li>The media capability User A is ready to receive is specified.</li> </ul>
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.

## Cisco SIP IP Phone-to-Cisco SIP IP Phone—Called User Does Not Answer

Figure B-17 illustrates an unsuccessful call in which User A initiates a call to User B but User B does not answer.

**Figure B-17** Cisco SIP IP Phone-to-Cisco SIP IP Phone—Called User Does Not Answer



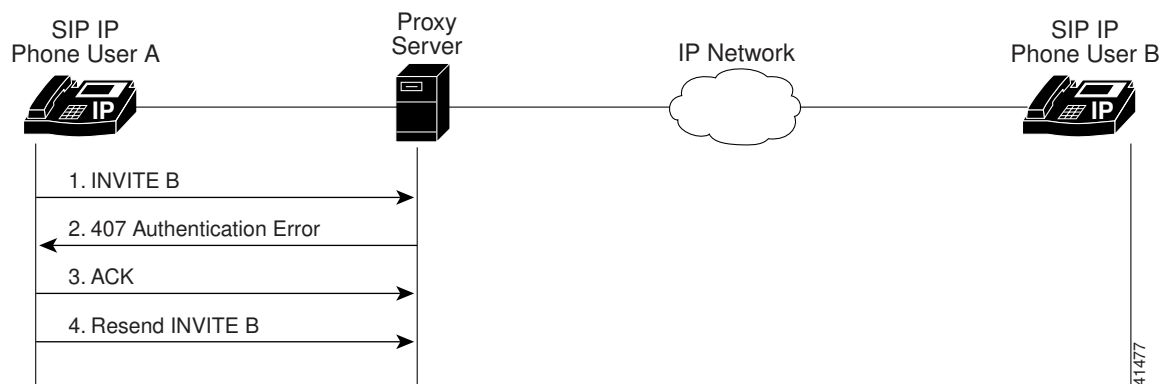


Step	Action	Description
1	INVITE—Cisco SIP IP phone A to Cisco SIP IP phone B	<p>Cisco SIP IP phone A sends a SIP INVITE request to Cisco SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> <li>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 email address (<i>user@host</i> where <i>user</i> is the telephone number and <i>host</i> 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 user name.</li> <li>Cisco SIP IP phone A is identified as the call session initiator in the From field.</li> <li>A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>The transaction number within a single call leg is identified in the CSeq field.</li> <li>The media capability User A is ready to receive is specified.</li> </ul>
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.
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 response confirms receipt of the cancellation request.

## Cisco SIP IP Phone-to-Cisco SIP IP Phone— Authentication Error

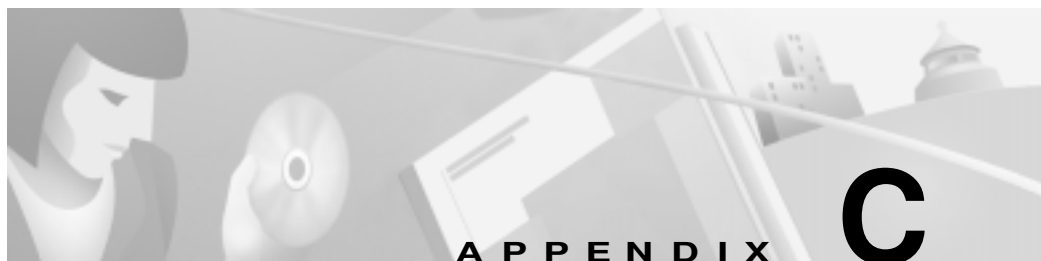
Figure B-18 illustrates an unsuccessful call in which User A initiates a call to User B but is prompted for authentication credentials by the proxy server. User A's SIP IP phone then reinitiates the call with an SIP INVITE request that includes it's authentication credentials.

**Figure B-18 Cisco SIP IP Phone-to-Cisco SIP IP Phone—Authentication Error**



Step	Action	Description
1	INVITE—Cisco SIP IP phone A to SIP proxy server	<p>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.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> <li>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 email address (<i>user@host</i> where <i>user</i> is the telephone number and <i>host</i> 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 user name.</li> <li>Cisco SIP IP phone A is identified as the call session initiator in the From field.</li> <li>A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>The transaction number within a single call leg is identified in the CSeq field.</li> <li>The media capability User A is ready to receive is specified.</li> </ul>
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

---

This appendix provides physical and operating environment and cable technical specifications for the Cisco SIP IP phones. This appendix also provides the connection specifications of your Cisco SIP IP phone.


### Physical and Operating Environment Specifications

The following table lists the physical and operating specifications of the Cisco SIP IP phone.

**Table C-1** Cisco SIP IP Phone Operational and Physical Specifications

Specification	Value or Range
Operating temperature	32 to 104 ° F (0 to 40 ° C)
Operating relative humidity	10 to 95% (noncondensing)
Storage temperature	14 ° to 140 ° F (-10 to 60 ° C)
Height	8 in. (210 mm)
Width	10.5 in. (265 mm)
Depth	2.4 in. (60 mm) <i>includes base in wall mount position</i>
Weight	3.5 lb (1.6 kg)

**Table C-1 Cisco SIP IP Phone Operational and Physical Specifications (continued)**

Specification	Value or Range
Power	48 VDC, supplied locally at the desktop using an optional AC-to-DC power supply
Regulatory	CE Marking IC CS-03 FCC Part 15 Class A FCC (CFR47) Part 68 FCC Part 68 EN 55022 Class A UL 1459 CSA-C22.2 No. 225-M90 EN 60950: 1992 IEC 950 AS/NZS 3260 TS001
Safety	UL-1950 EN 60950 CSA-C22.2 No. 950 IEC 950 AS.NZS 3260 TS001  <b>Note</b> See also Appendix D, “Translated Safety Warnings”.
EMC	FCC (CFR) Part 15 Class B ICES-003 Class B EN55022 Class B CISPR22 Class B AS.NZS 3548 Class B VCCI Class B
Certification	CD Marking

**Table C-1 Cisco SIP IP Phone Operational and Physical Specifications (continued)**

Specification	Value or Range
Cables	Two (2) pair of Category 3 for 10 Mbps cables Two (2) pair of Category 5 for 100 Mbps cables
Distance Requirements	As supported by the Ethernet Specification, it is assumed that most sets that are deployed in the field will be within 100 m (330 ft.) of a phone closet.

## 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 .1 inches (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.

## 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 “Connecting the Phone” section on page 2-16.







## Translated Safety Warnings

---

This appendix repeats in multiple languages the warnings that appear in 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 virtalähteeseen.

**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.

**Varning!** 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.

**Avvertenza** L'eliminazione finale di questo prodotto deve essere eseguita osservando le normative italiane vigenti in materia.

**Advarsel** Endelig disponering av dette produktet må skje i henhold til nasjonale lover og forskrifter.

**Aviso** A descartagem final deste produto deverá ser efectuada de acordo com os regulamentos e a legislação nacional.

**¡Advertencia!** El desecho final de este producto debe realizarse según todas las leyes y regulaciones nacionales.

**Varning!** Slutlig kassering av denna produkt bör skötas i enlighet med landets alla lagar och föreskrifter.

## 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 te ontkoppelen.

**Varoitus** Älä työskentele järjestelmän parissa äläkä yhdistä 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.

**Varning!** Vid åska skall du aldrig utföra arbete på systemet eller ansluta eller koppla loss kablar.

## SELV Circuit Warning (other versions available)



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.

**Varoitus** Jotta välttyt sähköiskulta, älä kytke pienjännitteisiä SELV-suojapiirejä puhelinverkkojännitettä (TNV) käyttöviin virtapiireihin. LAN-portit sisältävät SELV-piirejä ja WAN-portit puhelinverkkojännitettä käyttäviä piirejä. Osa sekä LAN- että WAN-porteista käyttää RJ-45-liittimiä. Ole varovainen kytkiessäsi kaapeleita.

**Attention** Pour éviter une électrocution, ne raccordez pas les circuits de sécurité basse tension (Safety Extra-Low Voltage ou SELV) à des circuits de tension de réseau téléphonique (Telephone Network Voltage ou TNV). Les ports du réseau local (LAN) contiennent des circuits SELV et les ports du réseau longue distance (WAN) sont munis de circuits TNV. Certains ports LAN et WAN utilisent des connecteurs RJ-45. Raccordez les câbles en prenant toutes les précautions nécessaires.

**Warnung** Zur Vermeidung von Elektroschock die Sicherheits-Kleinspannungs-Stromkreise (SELV-Kreise) nicht an Fernsprechnetzzspannungs-Stromkreise (TNV-Kreise) anschließen. LAN-Ports enthalten SELV-Kreise, und WAN-Ports enthalten TNV-Kreise. Einige LAN- und WAN-Ports verwenden auch RJ-45-Steckverbinder. Vorsicht beim Anschließen von Kabeln.

**Avvertenza** Per evitare scosse elettriche, non collegare circuiti di sicurezza a tensione molto bassa (SELV) ai circuiti a tensione di rete telefonica (TNV). Le porte LAN contengono circuiti SELV e le porte WAN contengono circuiti TNV. Alcune porte LAN e WAN fanno uso di connettori RJ-45. Fare attenzione quando si collegano cavi.

**Advarsel** Unngå å koble lavspenningskretser (SELV) til kretser for telenettspenning (TNV), slik at du unngår elektrisk støt. LAN-utganger inneholder SELV-kretser og WAN-utganger inneholder TNV-kretser. Det finnes både LAN-utganger og WAN-utganger som bruker RJ-45-kontakter. Vær forsiktig når du kobler kabler.

**Aviso** Para evitar choques eléctricos, não conecte os circuitos de segurança de baixa tensão (SELV) aos circuitos de tensão de rede telefónica (TNV). As portas LAN contêm circuitos SELV e as portas WAN contêm circuitos TNV. Algumas portas LAN e WAN usam conectores RJ-45. Tenha o devido cuidado ao conectar os cabos.

**¡Advertencia!** Para evitar la sacudida eléctrica, no conectar circuitos de seguridad de voltaje muy bajo (safety extra-low voltage = SELV) con circuitos de voltaje de red telefónica (telephone network voltage = TNV). Los puertos de redes de área local (local area network = LAN) contienen circuitos SELV, y los puertos de redes de área extendida (wide area network = WAN) contienen circuitos TNV. En algunos casos, tanto los puertos LAN como los WAN usan conectores RJ-45. Proceda con precaución al conectar los cables.

**Varning!** För att undvika elektriska stötar, koppla inte säkerhetskretsar med extra låg spänning (SELV-kretsar) till kretsar med telefonnätspänning (TNV-kretsar). LAN-portar innehåller SELV-kretsar och WAN-portar innehåller TNV-kretsar. Vissa LAN- och WAN-portar är försedda med RJ-45-kontakter. Iaktta försiktighet vid anslutning av kablar.

## Circuit Breaker (15A) Warning



### Warning

**This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).**

**Waarschuwing** Dit produkt is afhankelijk van de installatie van het gebouw voor kortsluit- (overstroom)beveiliging. Controleer of er een zekering of stroomverbreker van niet meer dan 120 Volt wisselstroom, 15 A voor de V.S. (240 Volt wisselstroom, 10 A internationaal) gebruikt wordt op de fasegeleiders (alle geleiders die stroom voeren).

**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).

**Warnung** Dieses Produkt ist darauf angewiesen, daß im Gebäude ein Kurzschluß- bzw. Überstromschutz installiert ist. Stellen Sie sicher, daß eine Sicherung oder ein Unterbrecher von nicht mehr als 240 V Wechselstrom, 10 A (bzw. in den USA 120 V Wechselstrom, 15 A) an den Phasenleitern (allen stromführenden Leitern) verwendet wird.

**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 strømbryter som ikke er større enn 120 VAC, 15 A (USA) (240 VAC, 10 A internasjonalt) på faselederne (alle strømførende ledere).

**Aviso** Este produto depende das instalações existentes para protecção contra curto-circuito (sobrecarga). Assegure-se de que um fusível ou disjuntor não superior a 240 VAC, 10A é 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).

**Varning!** 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 (iUSA 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.

---

## **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**

### **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).

## **DSP**

Digital signal processor.

## **DTMF**

Dual tone multi-frequency.

---

## 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**

Integrated 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 location(s). Location services are offered by location servers.

---

**M****MF**

Multi-frequency 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 PDUs from one source to many destinations. The actual mechanism (that is, IP multicast, multi-unicast, and so forth) for this process might be different for LAN technologies.

**multipoint-unicast**

A process of transferring PDUs (Protocol Data Units) where an endpoint sends more than one copy of a media stream to different endpoints. This can be necessary in networks which 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 co-located 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, which generally refers to Cisco's standards based (for example H.323) approach to IP voice traffic.







---

## Numerics

- 10/100 PC port **1-14**
- 10/100 SW port **1-14**
- 1xx responses **A-4**
- 2xx responses **A-4**
- 3xx responses **A-5**
- 4xx responses **A-5**
- 5xx responses **A-10**
- 6xx responses **A-10**

---

## A

- Accept-Encoding header field **A-10**
- Accept header field **A-10**
- Accept-Language header field **A-10**
- accessing
  - firmware version **3-33**
  - network statistics **3-31**
  - status messages **3-31**
- access port **1-14**
- address
  - proxy server **3-20**
  - TFTP server **3-4**
- adjusting, phone placement **2-18**

- administrative VLAN ID parameter **3-4**
- Allow header field **A-10**
- Also header field **A-10**
- alternate TFTP server, enabling **3-5**
- authentication
  - name, configuring **3-16**
  - services **1-3**
- Authorization header field **A-11**

---

## B

- billing services **1-3**
- book
  - objectives **x**
  - organization **x**
  - overview **ix**
- buttons
  - information **1-6**
  - line **1-6**
  - volume **1-7**

**C**

## cables

- connecting 2-16
- specifications C-3

## call flows B-1

- successful B-2
- unsuccessful B-58

## call forward 1-9

## call forward 1-9

## call hold 1-9

## Call-ID header field A-11

## call transfer 1-9

## call waiting 1-9

## circuit breaker (15A) warning D-6

## clients

- gateways 1-4
- phones 1-4
- SIP 1-4

## codec, specifying 3-9, 3-20

## common parameters 3-8

## compliance information A-1

## configuration, erasing 3-5

## configuration files

- default
  - creating 2-7
  - example 3-15
  - modifying 3-8
- guidelines 2-6

## phone-specific 2-6, 2-10

- creating 2-9
- example 3-18
- modifying 3-15
- naming convention 2-6

## SIPDefault.cnf 2-7

## storing 2-7

## configuration mode

- entering into 3-1
- locking 3-2
- unlocking 3-2

## configuring

## lines

- authentication name 3-16
- name 3-16
- password 3-16
- short name 3-16

## network parameters 2-13

- manually 2-14
- via DHCP 2-14

## SIP parameters

- manually 2-11
- via TFTP 2-6

## connections 1-13, 2-16

## Contact header field A-11

## Content-Encoding header field A-11

## Content-Length header field A-11

Content-Type header field **A-11**  
 conventions, document **xi**  
 Cseq header field **A-11**

---

## D

Date header field **A-11**  
 default configuration file **2-6, 2-7**  
   example **2-9, 3-15**  
   guidelines **2-6**  
   modifying **3-8**  
   SIPDefault.cnf **2-4**  
 default router parameters **3-4**  
 DHCP  
   description **1-10**  
   enabling **3-4**  
   options  
     default IP gateway **2-14**  
     DNS server **2-14**  
     domain name **2-14**  
     IP address **2-14**  
     IP subnet mask **2-14**  
     TFTP server **2-14**  
   releasing address **3-4**  
   server parameter **3-3**  
 dialing pad **1-7**  
 directory services **1-3**

DNS  
   description **1-10**  
   server parameters **3-4**  
 documentation  
   conventions **xi**  
   related **xi**  
 domain name parameter **3-3**  
 Domain Name System (DNS) **1-10**  
 do not disturb **1-9**  
 downloading required files **2-4**  
 DTMF  
   DB level **3-10**  
   inband **3-10**  
   outofband **3-10, 3-20**  
 Dynamic Host Control Protocol (DHCP) **1-10**

---

## E

enabling  
   alternate TFTP server **3-5**  
   DHCP **3-4**  
   registration **3-11, 3-21**  
 Encryption header field **A-11**  
 endpoint, SIP **1-3**  
 erasing  
   configuration **3-5**  
   parameters **3-28**  
   settings **3-28**

## example

- default configuration file 3-15
- phone-specific configuration file 3-18

Expires header field A-11

---

**F**

## features

- call forward 1-9
- call hold 1-9
- call transfer 1-9
- call waiting 1-9
- do not disturb 1-9
- secondary directory number 1-9
- URL dialing 1-10

## file

- default 3-15
- phone-specific 3-18

## files

- audio 2-4
- dual boot 2-4
- firmware image 2-4
- OS79XX.txt 2-4
- RINGLIST.DAT 2-4
- SIPDefault.cnf 2-4

## firmware

- image 2-4
- updating 3-33
- version, viewing 3-33

footstand adjustment 1-6

From header field A-11

## functions

- proxy server A-2
- redirect server A-2
- UAC A-2
- UAS A-2

---

**G**

- gateways 1-4
- guidelines 2-13

---

**H**

- handset 1-7
- header fields A-10
- headset
  - supported types 1-15
  - using 1-15
- headset and speaker toggle 1-7
- Hide header field A-11
- host name parameter 3-3

---

**I**

- ICMP, description 1-11
- image version 3-9
- information button 1-6

initialization process **2-1**  
 installation **2-3**  
     downloading required files **2-4**  
     network parameters **2-13**  
     safety warnings **D-1, D-3**  
     SIP parameters **2-5**  
     task summary **2-3**  
 Internet Control Message Protocol  
     (ICMP) **1-11**  
 Internet Protocol (IP) **1-11**  
 INVITE  
     retransmission expiration **3-10**

IP  
     address parameter **3-3**  
     description **1-11**

---

## K

keys  
     on-screen mode **1-7**  
     scroll **1-7**  
     soft **1-6**

---

## L

LCD screen **1-6**  
 line buttons **1-6**

lines, configuring  
     authentication name **3-16**  
     name **3-16**  
     password **3-16**  
     short name **3-16**  
 linex\_authname parameter **3-16**  
 linex\_name parameter **3-16**  
 linex\_password parameter **3-16**  
 linex\_shortcode parameter **3-16**  
 locking, configuration mode **3-2**

---

## M

MAC address parameter **3-3**  
 manually configuring  
     SIP parameters **3-18**  
 Max-Forwards header field **A-11**  
 messages, status **3-31**  
 message URI parameter **3-20**  
 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 **3-8, 3-15**  
 mute toggle **1-7**

## N

name, configuring **3-16**  
 naming convention, phone-specific  
     configuration file **2-6**  
 network  
     connections **1-13**  
     parameters  
         administrative VLAN ID **3-4**  
         alternate TFTP **3-5**  
         configuring via DHCP **2-14**  
         default router **3-4**  
         DHCP address release **3-4**  
         DHCP enable **3-4**  
         DHCP server **3-3**  
         domain name **3-3**  
         erase configuration **3-5**  
         guidelines **2-13**  
         host name **3-3**  
         IP address **3-3**  
         MAC address **3-3**  
         operational VLAN ID **3-4**  
         subnet mask **3-3**  
         TFTP server **3-4**

port **1-14**  
 statistics **3-31**  
 network connections  
     access port **1-14**

## O

on-screen mode keys **1-7**  
 operating environment specifications **C-1**  
 operational VLAN ID parameter **3-4**  
 Organization header field **A-11**  
 OS79XX.txt **2-4**  
 Out of Band DTMF parameter **3-20**  
 overview  
     book **ix**  
     Cisco SIP IP phone **1-5**  
     initialization process **2-1**  
     product **1-1**  
     SIP **1-1**

## P

parameters  
     common **2-7, 3-8**  
     configuring  
         network **2-13**  
         SIP **2-5**  
     erasing **3-28**  
     network **2-13**

- administrative VLAN ID 3-4
- alternate TFTP 3-5
- default routers 3-4
- DHCP address release 3-4
- DHCP enable 3-4
- DHCP server 3-3
- DNS server 3-4
- domain name 3-3
- erase configuration 3-5
- guidelines 2-13
- host name 3-3
- IP address 3-3
- MAC address 3-3
- modifying 3-2, 3-3
- operational VLAN ID 3-4
- subnet mask address 3-3
- TFTP server 3-4
- required 2-10
- SIP
  - Authentication Name 3-19
  - Authentication Password 3-19
  - dtmf\_db\_level 3-10
  - dtmf\_outofbound 3-10
  - image\_version 3-9
  - linex\_authname 3-16
  - linex\_name 3-16
  - linex\_password 3-16
  - linex\_shortcode 3-16
  - Message URI 3-20
  - Name 3-19
  - Out of Band DTMF 3-20
  - Preferred Codec 3-20
  - preferred\_codec 3-9
  - proxy\_register 3-11
  - proxy1\_address 3-9
  - proxy1\_port 3-9
  - Proxy Address 3-20
  - Proxy Port 3-20
  - Register Expires 3-21
  - Register with Proxy 3-21
  - required 2-8
  - Short Name 3-19
  - sip\_invite\_retx 3-11
  - sip\_retx 3-11
  - timer\_invite\_expires 3-10
  - timer\_register\_expires 3-11
  - timer\_t1 3-10
  - timer\_t2 3-10
  - tos\_media 3-9
- password
  - configuring 3-16
  - line 3-16
- phone 3-8
  - adjusting placement 2-18
  - connecting 2-16

- connections 1-13
  - access port 1-14
  - network 1-13
  - network port 1-14
- features
  - dialing pad 1-7
  - footstand adjustment 1-6
  - handset 1-7
  - headset 1-15
  - headset and speaker toggle 1-7
  - information button 1-6
  - LCD screen 1-6
  - line buttons 1-6
  - mute toggle 1-7
  - on-screen mode keys 1-7
  - physical 1-6
  - scroll key 1-7
  - soft keys 1-6
  - volume buttons 1-7
- installing 2-3
- interfaces 1-5
- mounting to wall 2-18
- overview 1-5
- prerequisites 1-12
- secondary directory number 1-9
- supported features 1-7
- supported protocols 1-10
  - DHCP 1-10
  - DNS 1-10
  - ICMP 1-11
  - IP 1-11
  - RTP 1-11
  - SDP 1-11
  - SNTP 1-11
  - TFTP 1-12
  - UDP 1-12
- telephony features
  - telephony 1-9
- URL dialing 1-10
- verifying startup 2-20
- phone-specific configuration file
  - creating 2-10
  - example 2-9, 3-18
  - modifying 3-15
- physical specifications C-1
- port
  - access 1-14
  - network 1-14
  - proxy server 3-20
- power source
  - Cisco Catalyst switches 1-14
  - external 1-14
- prerequisites 1-12
- Priority header field A-11
- product
  - overview 1-1
- product disposal warning D-2
- protocols 1-10



- DHCP 1-10
  - DNS 1-10
  - ICMP 1-11
  - IP 1-11
  - RTP 1-11
  - SDP 1-11
  - SNTP 1-11
  - TFTP 1-12
  - UDP 1-12
  - Proxy-Authenticate header field A-11
  - Proxy-Authorization header field A-11
  - proxy port
    - specifying 3-9
  - Proxy-Required header field A-11
  - proxy server 1-5
    - address 3-20
    - port 3-20
    - registration, enabling 3-11, 3-21
    - specifying 3-9
- 
- ## R
- Real-Time Transport Protocol (RTP) 1-11
  - ReBy header field A-11
  - Record-Route header field A-11
  - redirect server 1-5
  - registrar server 1-5
  - registration
    - enabling 3-11
    - timer 3-11, 3-21
  - related documentation xi
  - release, DHCP address 3-4
  - request methods B-1
  - Require header field A-11
  - resetting
    - network statistics 3-32
  - Response-Key header field A-11
  - responses A-3
    - global (6xx) A-10
    - information (1xx) A-4
    - redirection (3xx) A-5
    - request failure (4xx) A-5
    - server failure (5xx) A-10
    - successful (2xx) A-4
  - retransmission timers 3-10
  - Retry-After header field A-11
  - RFC
    - 2131 1-10
    - 2543 1-1, 1-5
    - 768 1-12
    - 791 1-11
    - 792 1-11
  - RINGLIST.DAT 2-4
  - Route header field A-11
  - RTP, description 1-11

## S

safety warnings, translated **D-1**

    circuit breaker (15A) warning **D-6**

    installation warning **D-1**

    lightning activity warning **D-3**

    product disposal warning **D-2**

    SELV circuit warning **D-4**

scroll key **1-7**

SDP, description **1-11**

SDP, usage **A-12**

secondary directory number **1-9**

SELV circuit warning **D-4**

server

    alternate TFTP **3-5**

    proxy **1-5**

    redirect **1-5**

    registrar **1-5**

Server header field **A-12**

Session Description Protocol (SDP) **1-11**

settings, erasing **3-28**

short name, configuring **3-16**

Simple Network Time Protocol (SNTP) **1-11**

SIP

    architecture **1-4**

    call flows **B-1**

        successful **B-2**

        unsuccessful **B-58**

clients **1-3, 1-4**

    gateways **1-4**

    phones **1-4**

compliance information **A-1**

components **1-3**

    UAC **1-3**

    user agent server **1-3**

default configuration file, example **2-9**

dtmf\_inband **3-10**

end point **1-3**

functions **A-2**

gateways **1-4**

header fields **A-10**

IP phone, overview **1-5**

methods **A-2**

overview **1-1**

parameters

    Authentication Name **3-19**

    Authentication Password **3-19**

    manually configuring **3-18**

    Message URI **3-20**

    Name **3-19**

    Out of Band DTMF **3-20**

    phone-specific configuration file **2-6**

    Preferred Codec **3-20**

    Proxy Address **3-20**

    Proxy Port **3-20**

- Register Expires **3-21**
- Register with proxy **3-21**
- Short Name **3-19**
- request methods **B-1**
- responses **A-3**
  - global (6xx) **A-10**
  - information (1xx) **A-4**
  - redirection (3xx) **A-5**
  - request failure (4xx) **A-5**
  - server failure (5xx) **A-10**
  - successful (2xx) **A-4**
- SDP usage **A-12**
- servers
  - proxy **1-5**
  - redirect **1-5**
  - registrar **1-5**
- services
  - authentication **1-3**
  - billing **1-3**
  - directory **1-3**
- SIPDefault.cnf **2-4, 2-7**
- SIP parameters
  - configuring manually **3-18**
  - configuring via TFTP server **2-6**
- SNTP, description **1-11**
- soft keys **1-6**
- specifications **C-1**
  - cable **C-3**
  - connections **C-3**
  - operating environment **C-1**
  - physical **C-1**
- specifying **3-9**
  - codec **3-9, 3-20**
  - DTMF level **3-10**
  - DTMF signaling **3-10**
  - image version **3-9**
  - proxy port **3-9**
  - proxy server **3-9**
  - retransmission timers **3-10**
  - TOS media **3-9**
- specifying out of bound **3-20**
- startup, verifying **2-20**
- statistics, network **3-31**
- status information
  - accessing **3-30, 3-31, 3-33**
- Subject header field **A-12**
- subnet mask parameter **3-3**

---

**T**

- technical specifications **C-1**
  - cablet **C-3**
  - operating environment **C-1**
  - physical **C-1**
- TFTP, description **1-12**
- TFTP server parameter **3-4**

timer  
     registration 3-11, 3-21  
     retransmission 3-10  
 timer\_t2 3-10  
 timers, retransmission 3-10  
 Timestamp header field A-12  
 toggle  
     headset and speaker 1-7  
     mute 1-7  
 To header field A-12  
 TOS media  
     specifying 3-9  
 translated safety warnings D-1  
     circuit breaker (15A) warning D-6  
     installation warning D-1  
     lightning activity warning D-3  
     product disposal warning D-2  
     SELV circuit warning D-4  
 Trivial File Transfer Protocol (TFTP) 1-12

## U

UAC 1-3  
 UDP, description 1-12  
 unlocking, configuration mode 3-2  
 Unsupported header field A-12  
 updating  
     firmware 3-33  
 URL dialing 1-10

user  
     agent server 1-3  
 User-Agent header field A-12  
 User Datagram Protocol (UDP) 1-12

## V

verifying startup 2-20  
 Via header field A-12  
 viewing firmware version 3-33  
 VLAN  
     administrative 3-4  
     operational 3-4  
 volume  
     buttons 1-7

## W

wall mounting  
     phone 2-18  
 Warning header field A-12  
 WWW-Authenticate header field A-12