Guide to Cisco Systems' VoIP Infrastructure Solution for SIP

Version 1.0

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

Text Part Number: OL-1002-01

C O N T E N T S

GLOSSARY

Guide to Cisco Systems' VoIP Infrastructure Solution for SIP

About this Guide

This section describes the objectives, audience, organization, and conventions of the *Guide to Cisco Systems' VoIP Infrastructure Solution for SIP*.

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Objectives

This guide is designed to help you understand and implement the Cisco Voice over IP (VoIP) Infrastructure Solution for the Session Initiation Protocol (SIP), Version 1.0.

Audience

This document is intended for system administrators who will install, configure, and manage a VoIP solution.

Organization

This document is divided into the following chapters:

Chapter	Title	Description
Chapter 1	Overview of the Session Initiation Protocol	Provides an overview of SIP, its components, and how it works.
Chapter 2	Overview of the Cisco VoIP Infrastructure Solution for SIP	Provides an overview of the Cisco VoIP Solution for SIP.
Chapter 3	Installing the Cisco VoIP Infrastructure Solution for SIP	Provides an overview of how to install the components of the Cisco VoIP Solution for SIP.
Chapter 4	Configuring the Cisco VoIP Infrastructure Solution for SIP	Provides scenario-based examples of how to configure the components of the Cisco VoIP Solution for SIP.
Chapter 5	Managing and Troubleshooting the Cisco VoIP Infrastructure Solution for SIP	Describes the tools that are available for managing and troubleshooting the Cisco VoIP Solution for SIP. This chapter also provides tips for problem isolation and recommendations for problem resolution.
Chapter 6	SIP Messages and Compliance Information for the Cisco VoIP Infrastructure Solution for SIP	Describes the methods and messages used by SIP and how the components of the solution handles these methods and messages.
Chapter 7	SIP Call Flow Process for the Cisco VoIP Infrastructure Solution for SIP	Illustrates how SIP messages are exchanged during the call process.
	Glossary	Provides definitions of the acronyms and terms used in this document.

Command Syntax Conventions

Table 1 describes the syntax used with the commands in this document.

Table 1   Command Syntax Guide

Convention	Description
boldface	Commands and keywords.
italic	Command input that is supplied by you.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x	x	x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. You must select one.
^ or Ctrl	Represent the key labeled *Control*. For example, when you read *^D* or *Ctrl-D*, you should hold down the Control key while you press the D key.
screen font	Examples of information displayed on the screen.
boldface screen font	Examples of information that you must enter.
< >	Nonprinting characters, such as passwords, appear in angled brackets.
[ ]	Default responses to system prompts appear in square brackets.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- 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 and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

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.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com 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.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, 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 Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.

- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.

- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

Overview of the Session Initiation Protocol

This chapter provides an overview of SIP. It includes the following sections:

- Introduction to SIP, page 1-1
- Components of SIP, page 1-2
- How SIP Works, page 1-3
- SIP Versus H.323, page 1-8

Introduction to SIP

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 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, location servers, a database application, RADIUS server, 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
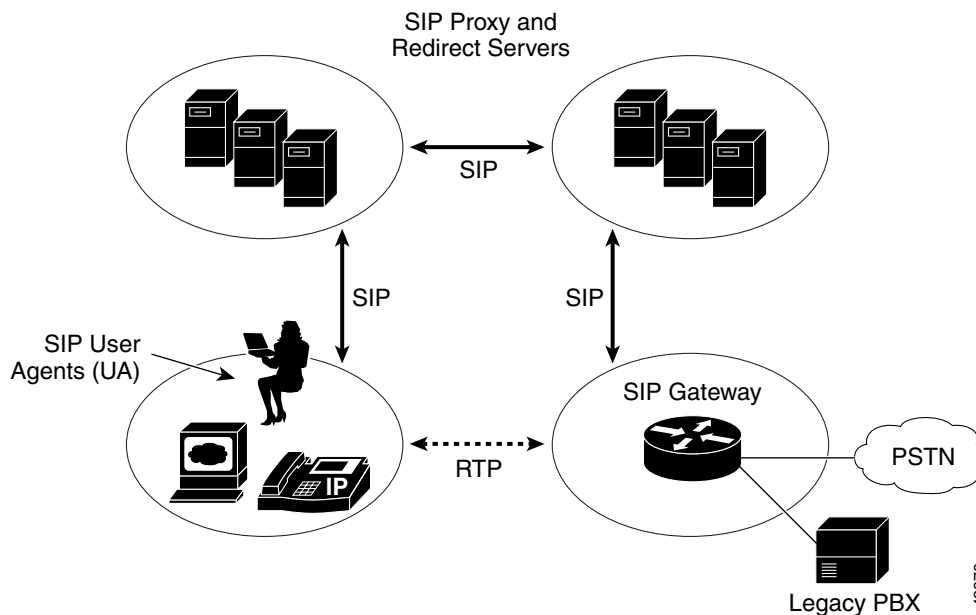
SIP Clients

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 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—Provides 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.

How SIP Works

SIP is a simple, ASCII-based protocol that uses requests and responses to establish communication among the various components in the network and to ultimately establish a conference between two or more end points.

Users in a SIP network are identified by unique SIP addresses. A SIP address is similar to an e-mail address and is in the format of sip:*userID@gateway*.com. The user ID can be either a user name or an E.164 address.

Users register with a registrar server using their assigned SIP addresses. The registrar server provides this information to the location server upon request.

When a user initiates a call, a SIP request is sent to a SIP server (either a proxy or a redirect server). The request includes the address of the caller (in the From header field) and the address of the intended callee (in the To header field). The following sections provide simple examples of successful, point-to-point calls established using a proxy and a redirect server.

Over time, a SIP end user might move between end systems. The location of the end user can be dynamically registered with the SIP server. The location server can use one or more protocols (including finger, rwhois, and LDAP) to locate the end user. Because the end user can be logged in at more than one station, it might return more than one address for the end user. If the request is coming through a SIP proxy server, the proxy server will try each of the returned addresses until it locates the end user. If the request is coming through a SIP redirect server, the redirect server forwards all the addresses to the caller in the Contact header field of the invitation response.

For more information, see RFC 2543—*SIP: Session Initiation Protocol*, which can be found at http://www.faqs.org/rfcs/.

Using A Proxy Server

If a proxy server is used, the caller UA sends an INVITE request to the proxy server, the proxy server determines the path, and then forwards the request to the callee (as shown in Figure 1-2).

Figure 1-2   SIP Request Through a Proxy Server
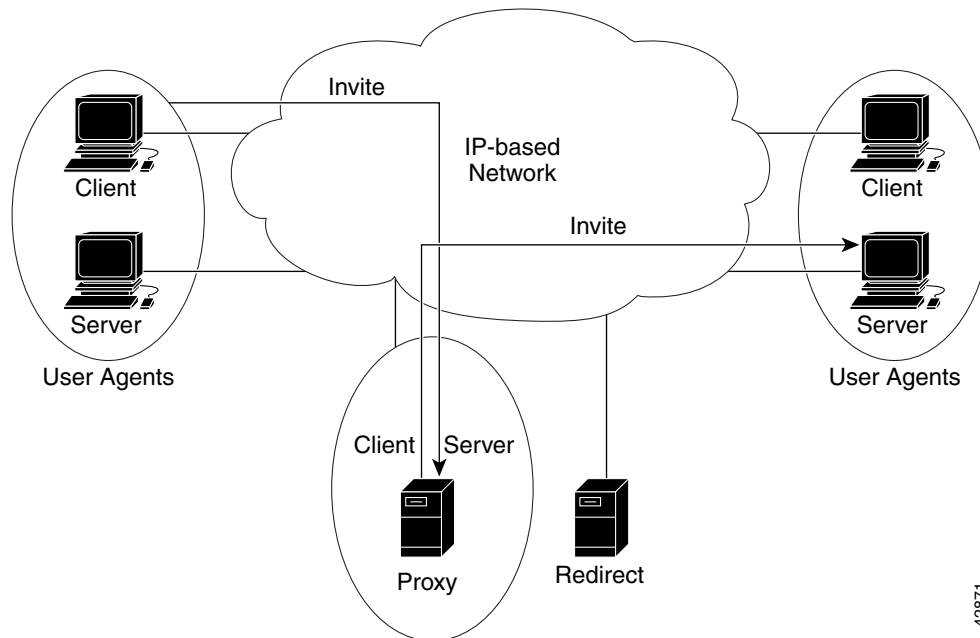
The callee responds to the proxy server, which in turn, forwards the response to the caller (as shown in Figure 1-3).

Figure 1-3   SIP Response Through a Proxy Server
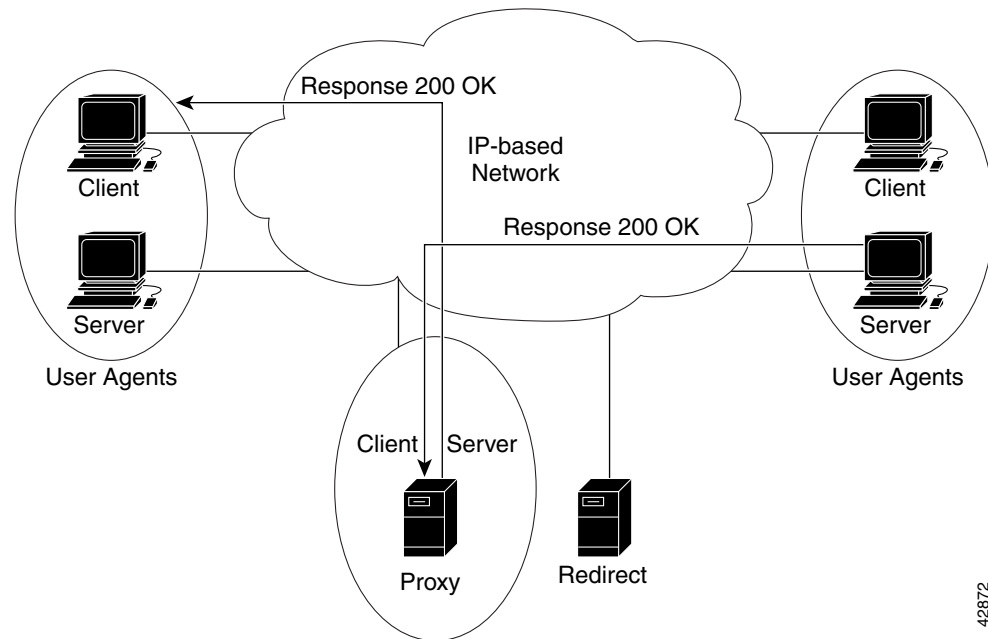
The proxy server forwards the acknowledgments of both parties. A session is then established between the caller and callee. Real-time Transfer Protocol (RTP) is used for the communication between the caller and the callee (as shown in Figure 1-4).

Figure 1-4   SIP Session Through a Proxy Server
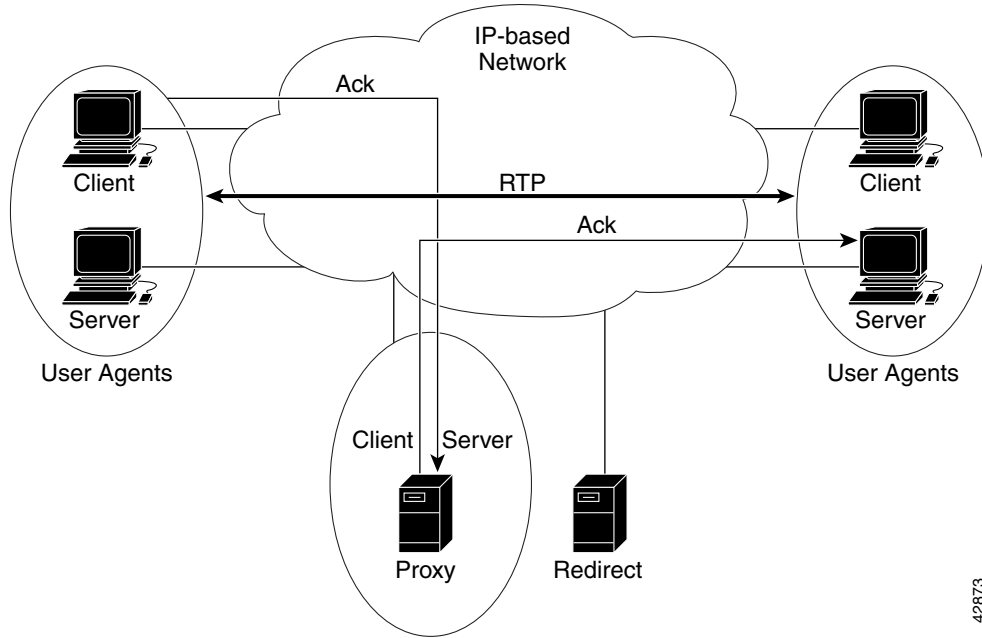
Using a Redirect Server

If a redirect server is used, the caller UA sends an INVITE request to the redirect server, the redirect server contacts the location server to determine the path to the callee, and then the redirect server sends that information back to the caller. The caller then acknowledges receipt of the information (as shown in Figure 1-5).

Figure 1-5   SIP Request Through a Redirect Server
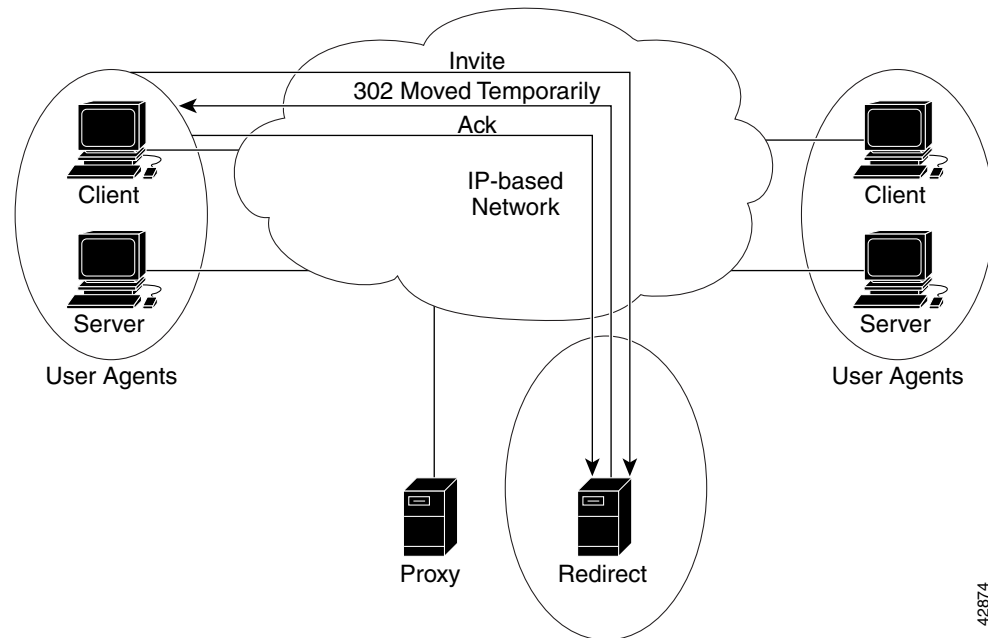
The caller then sends a request to the device indicated in the redirection information (which could be the callee or another server that will forward the request). Once the request reaches the callee, it sends back a response and the caller acknowledges the response. RTP is used for the communication between the caller and the callee (as shown in Figure 1-6).

Figure 1-6   SIP Session Through a Redirect Server
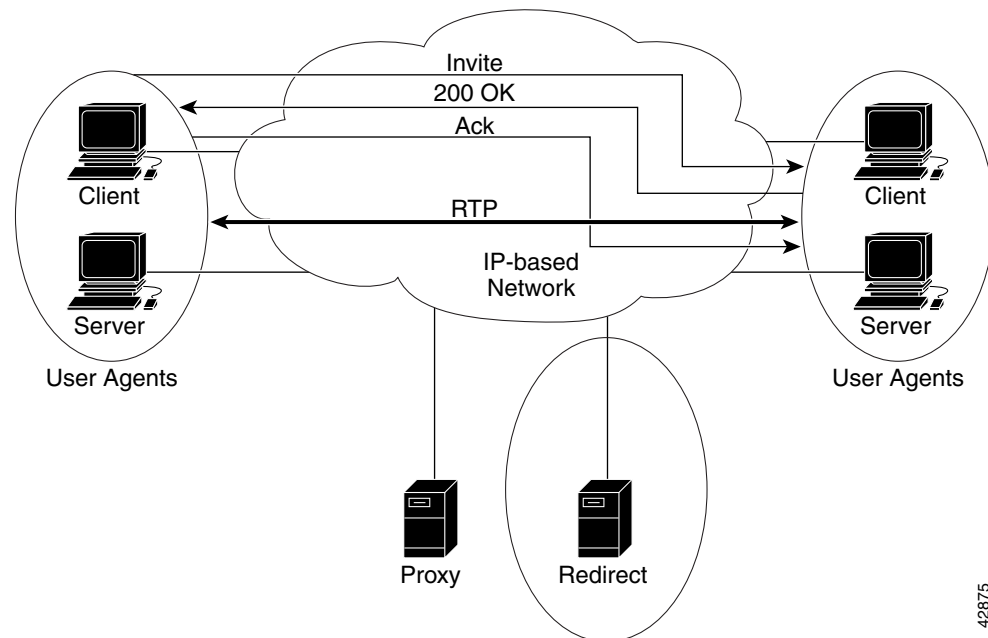
SIP Versus H.323

In addition to SIP, there are other protocols that facilitate voice transmission over IP. One such protocol is H.323. H.323 originated as an International Telecommunications Union (ITU) multimedia standard and is used for both packet telephony and video streaming. The H.323 standard incorporates multiple protocols, including Q.931 for signaling, H.245 for negotiation, and Registration Admission and Status (RAS) for session control. H.323 was the first standard for call control for VoIP and is supported on all Cisco Systems' voice gateways.

SIP and H.323 were designed to address session control and signaling functions in a distributed call control architecture. Although SIP and H.323 can also be used to communicate to limited intelligence end points, they are especially well-suited for communication with intelligent end points.

Table 1-1 provides a brief comparison of SIP and H.323.

Table 1-1   SIP versus H.323

Aspect	SIP	H.323
Clients	Intelligent	Intelligent
Network intelligence and services	Provided by servers (Proxy, Redirect, Registrar)	Provided by gatekeepers
Model used	Internet/WWW	Telephony/Q.SIG
Signaling protocol	UDP or TCP	TCP (UDP is optional in Version 3)
Media protocol	RTP	RTP
Code basis	ASCII	Binary (ASN.1 encoding)
Other protocols used	IETF/IP protocols, such as SDP, HTTP/1.1, IPmc, and MIME	ITU / ISDN protocols, such as H.225, H.245, and H.450
Vendor interoperability	Widespread	Widespread

Although SIP messages are not directly compatible with H.323, both protocols can coexist in the same packet telephony network if a device that supports the interoperability is available.

For example, a call agent could use H.323 to communicate with gateways and use SIP for inter-call agent signaling. Then, after the bearer connection is set up, the bearer information flows between the different gateways as an RTP stream.

Overview of the Cisco VoIP Infrastructure Solution for SIP

This chapter provides an overview of the Cisco VoIP Infrastructure Solution for SIP, Version 1.0. It includes the following sections:

- Introduction to the Cisco VoIP Infrastructure Solution for SIP, page 2-1
- Components of the Cisco VoIP Infrastructure Solution for SIP, page 2-11
- Related Documents, page 2-25

Introduction to the Cisco VoIP Infrastructure Solution for SIP

The Cisco VoIP Infrastructure Solution for SIP implements a voice-over-packet network design using SIP to provide telephony services. It lays the foundation for building a SIP-based VoIP solution, which is built using Cisco products. This is the first of a series of releases of this solution, which provides basic services and works with a number of enhanced services. In this first release, the components can be used to implement toll by-pass, effect Dedicated Access Line (DAL) replacement and to provide enhanced IP telephony services such as a scalable private number plan, and to provide desktop services such as call forwarding, call hold, and call transfer.

The solution includes a SIP IP phone (Cisco Systems' SIP IP Phone 7960), a SIP gateway (integrated with Cisco Systems' IOS software), a SIP proxy server (Cisco SIP Proxy Server), a unified messaging server (Cisco uOne Messaging System), a firewall (Cisco Secure PIX Firewall), and a VoIP solution for service providers (Cisco SS7 Interconnect for Voice Gateways Solution). These components work together to provide a SIP-based VoIP solution that can be integrated with existing telephony networks.

Illustrated Implementations

The following sections illustrate a possible "phased" implementation of the Cisco VoIP Infrastructure Solution for SIP from an intranetwork approach and an internetwork approach.

Intranetwork Phased Approach Implementation

This section illustrates a possible intranetwork "phased" implementation of the Cisco VoIP Infrastructure Solution for SIP.

Phase 1: Toll By-Pass and DAL Replacement

As a first step toward a total SIP-based VoIP solution, VoIP gateways configured to support SIP are implemented to replace the traditional DAL and by-pass carrier toll lines. In Figure 2-1, Cisco SIP gateways and an IP network have been introduced between the private branch exchanges (PBXs).

Figure 2-1   Toll By-pass and DAL Replacement
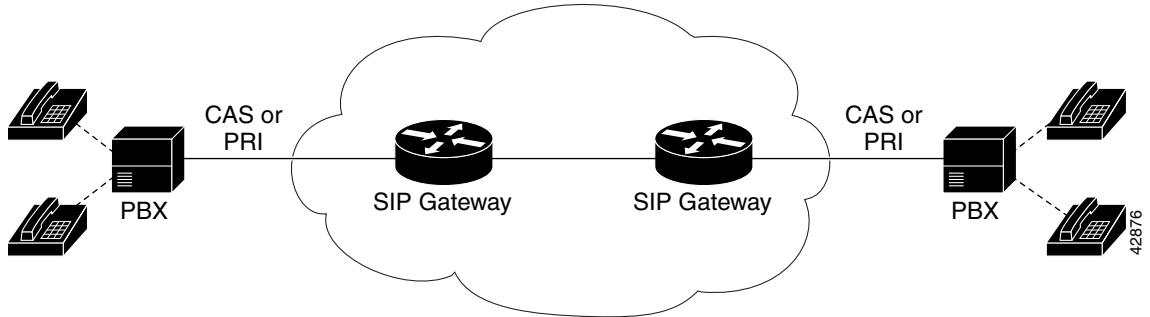
Phase 2: Scalable Number Plan Support

As the next step, SIP proxy servers are used to provide support for a scalable private number plan. In Figure 2-2, SIP proxy servers have been added to the IP network.

Figure 2-2   Scalable Private Number Plan Support
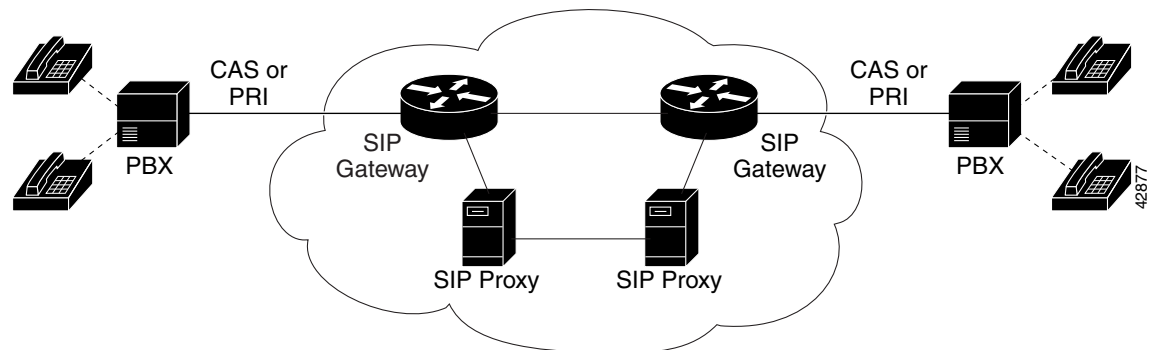
Phase 3: SIP IP Phone Support

As the next step, Cisco SIP IP phones are added. These phones connect directly to the IP network and, when used with the other SIP components, provide features such as call hold, call waiting, call transfer, and call forwarding. In Figure 2-3, Cisco SIP IP phones have been connected directly to the IP network.

Figure 2-3   Cisco SIP IP phone Support
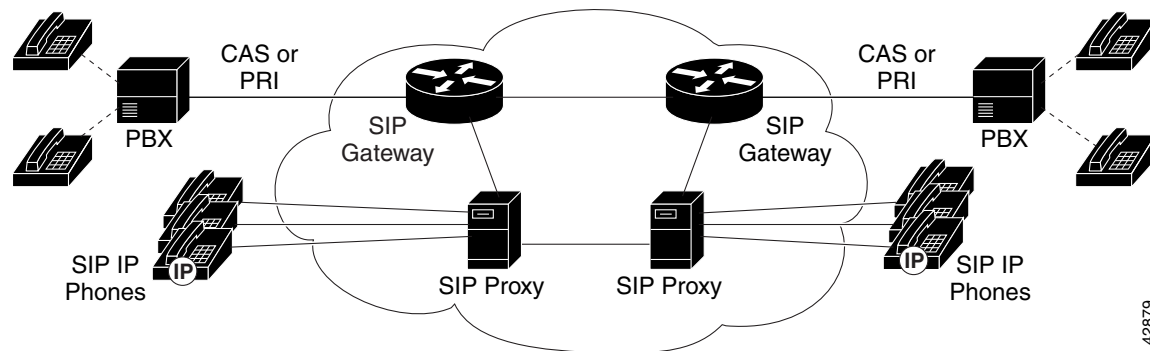
Phase 4: Application Services Support

As the next step, application services (such as a RADIUS server) are integrated with the SIP proxy servers. This enables the SIP proxy servers to perform authentication (via HTTP digest). It also provides the end customers with enhanced services, such as "find me" and call screening. The Cisco SIP gateways interface with the application services using AAA and RADIUS for billing purposes. In Figure 2-4, application servers have been added to the IP network to interface with the SIP proxy servers.

Figure 2-4   Application Services Support
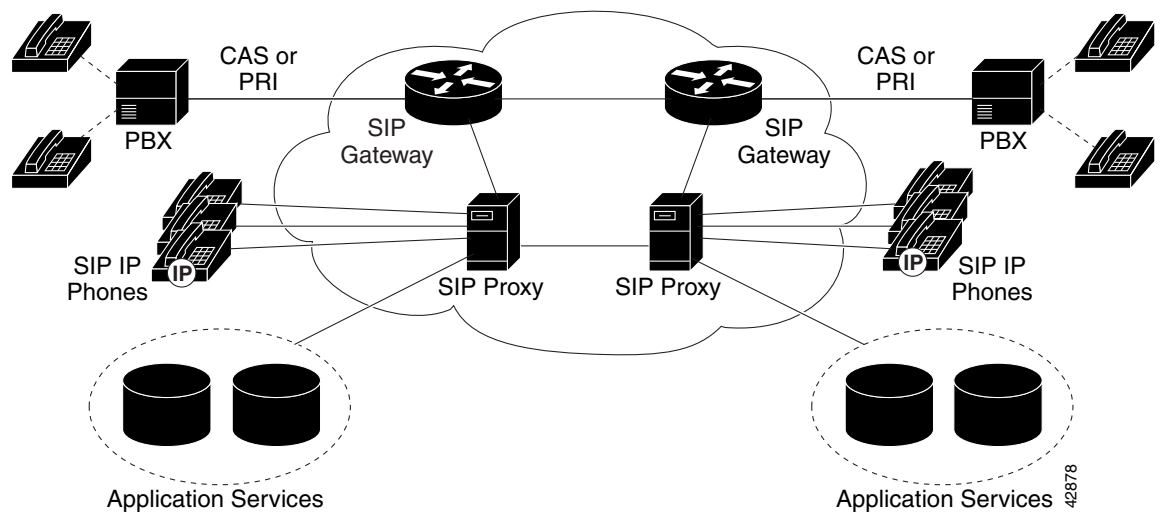
Phase 5: IP Telephony Services with Unified Messaging

As the next step, a unified messaging server is added to provide voice mail. In Figure 2-5, a unified messaging server has been added to the IP network.

Figure 2-5   IP Telephony Services with Unified Messaging
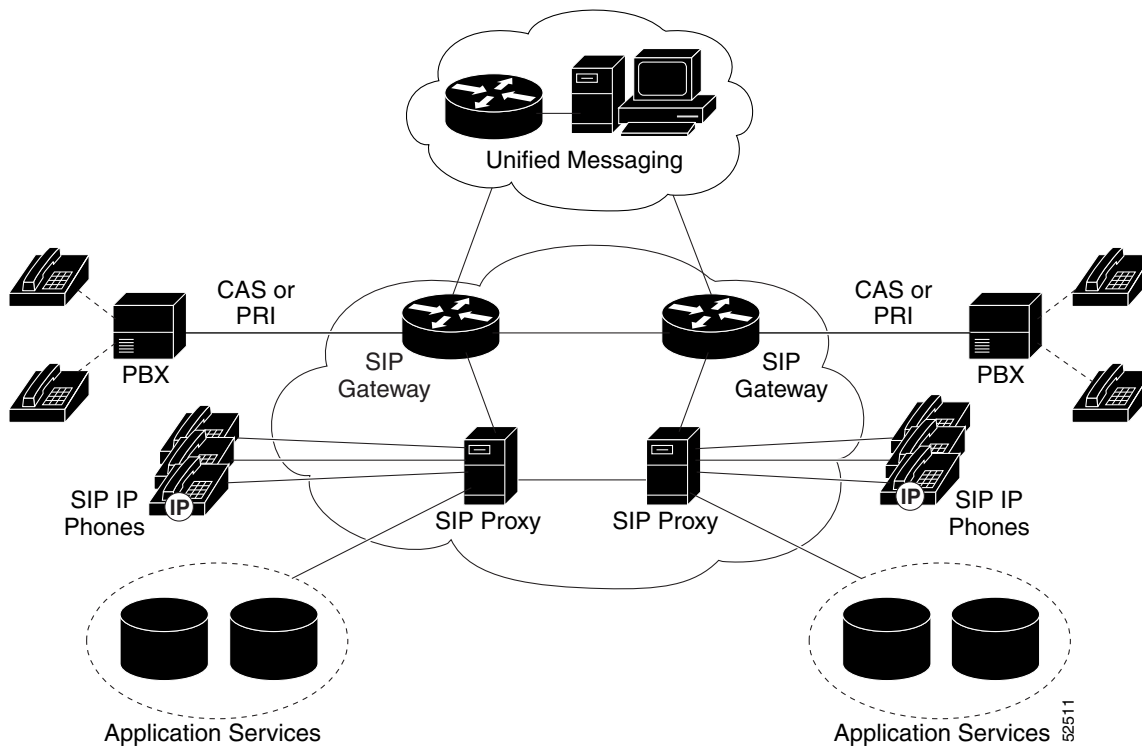
To summarize our final intranetwork phase:

- At the center is a QoS-enabled IP network using Cisco internetworking equipment with a set of Cisco SIP gateways and one or more SIP proxy servers.

- The Cisco SIP gateways are connected to the PBXs via T1 or E1 lines with channel associated signaling (CAS) or primary rate interface (PRI) signaling.

- Several traditional telephones or fax machines are connected to the PBXs.

- Cisco SIP IP phones are connected directly to the IP network.

- A server running a unified messaging application is also connected to the IP network.

- SIP is used for signaling (or session initiation) between the SIP clients, the Cisco SIP IP phones, the Cisco SIP gateways, and the SIP proxy servers.

- RTP/RTCP is used to transmit voice data between the SIP endpoints after sessions are established.

As this example shows, the Cisco VoIP Infrastructure Solution for SIP is designed not only to provide an alternative to traditional telephony equipment, but also to interact with existing equipment.

Internetwork Phased Approach Implementation

This section illustrates a possible internetwork "phased" implementation of the Cisco VoIP Infrastructure Solution for SIP for integrating a SIP enabled VoIP network with a public network (PSTN) infrastructure. This phased approach builds on an existing SIP VoIP network as outlined in the "Intranetwork Phased Approach Implementation" section on page 2-1.

Phase 6: Network Security Support

As the first step to an internetwork phased approach, Cisco Secure PIX Firewalls are added to the existing intranetwork for inside network security. In Figure 2-6, Cisco Secure PIX Firewalls have been added to the IP network.

Figure 2-6   The Cisco Secure PIX Firewall in a SIP Network.
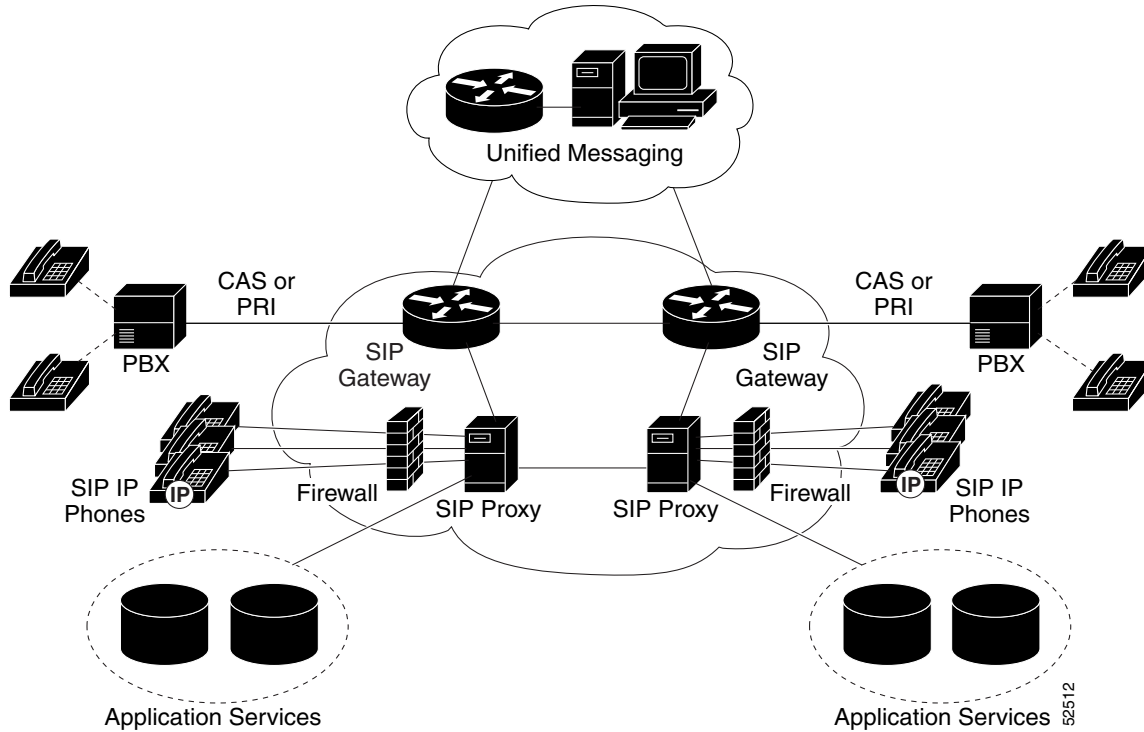
Phase 7: VoIP-to-PSTN Support

The final internetwork phase is to implement the Cisco SS7 Interconnect for Voice Gateways Solution for integrating the SIP enabled VoIP network with a public network infrastructure.

In Figure 2-7, Cisco SS7 Interconnect for Voice Gateways Solution components have been added.

Figure 2-7   Cisco SS7 Interconnect for Voice Gateways Solution Implemented with a SIP VoIP Network
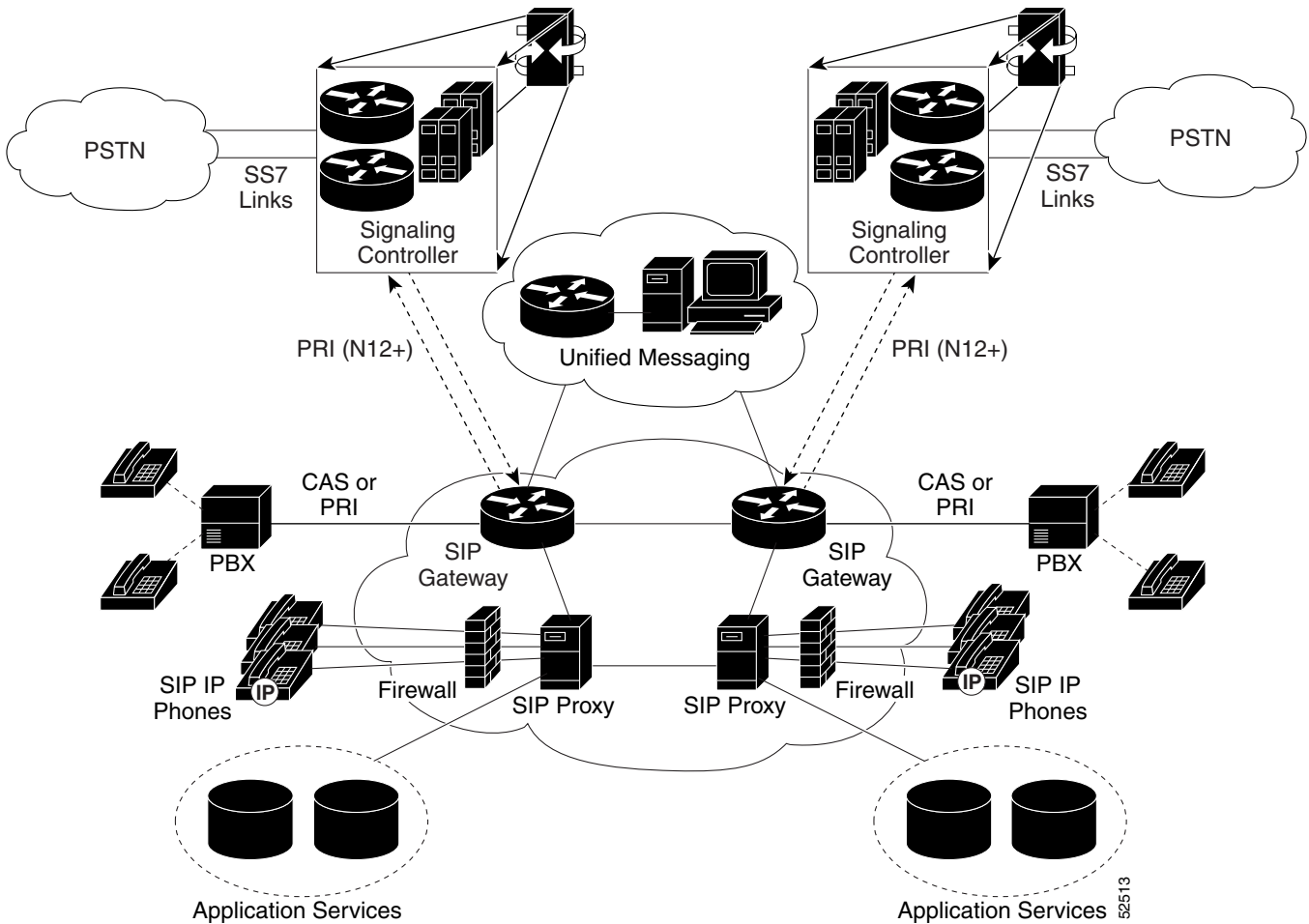
Processing Calls Within a Single SIP IP Telephony Network

When calls are made within a single SIP IP telephony network, the process typically involves the origination and destination phones and a single proxy server. Figure 2-8 is a simplified illustration of a call between Cisco SIP IP phones within the same SIP IP telephony network.

Figure 2-8   Calls Within a Single SIP IP Telephony Network
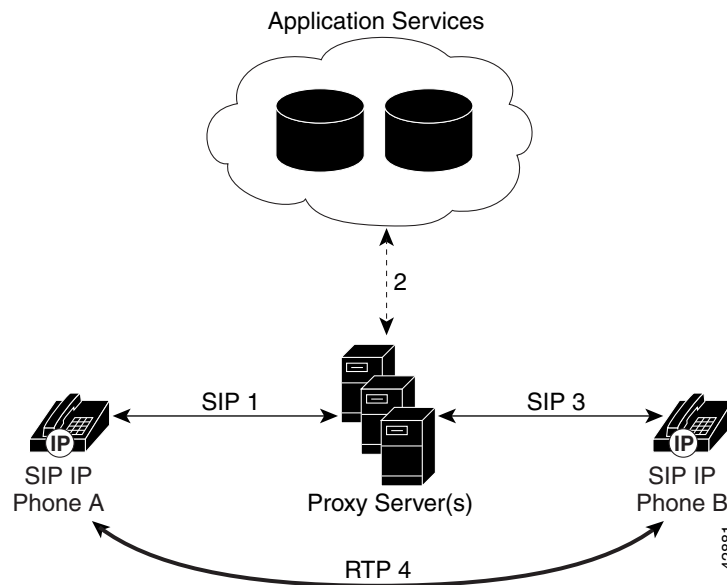
In this illustration:

1. Cisco SIP IP phone A initiates a call by sending an INVITE message to the SIP proxy server. (There can be more than one proxy server for redundancy.)

2. The SIP proxy server interacts with the location server and might interact with application services to determine user addressing, location or features.

3. The SIP proxy server then proxies the INVITE message to the destination phone.

4. After responses and acknowledgments are exchanged, an RTP session is established between Cisco SIP IP phones A and B.

For more information about the messages that are exchanged during call processes, see Chapter 7, "SIP Call Flow Process for the Cisco VoIP Infrastructure Solution for SIP."

Processing Calls Between SIP IP Telephony Networks

When calls are made between SIP IP telephony networks, the process typically involves the origination and destination phones as well as two or more proxy servers. Figure 2-9 is a simplified illustration of a call between Cisco SIP IP phones in different SIP IP telephony networks.

Figure 2-9   Calls Between SIP IP Telephony Networks
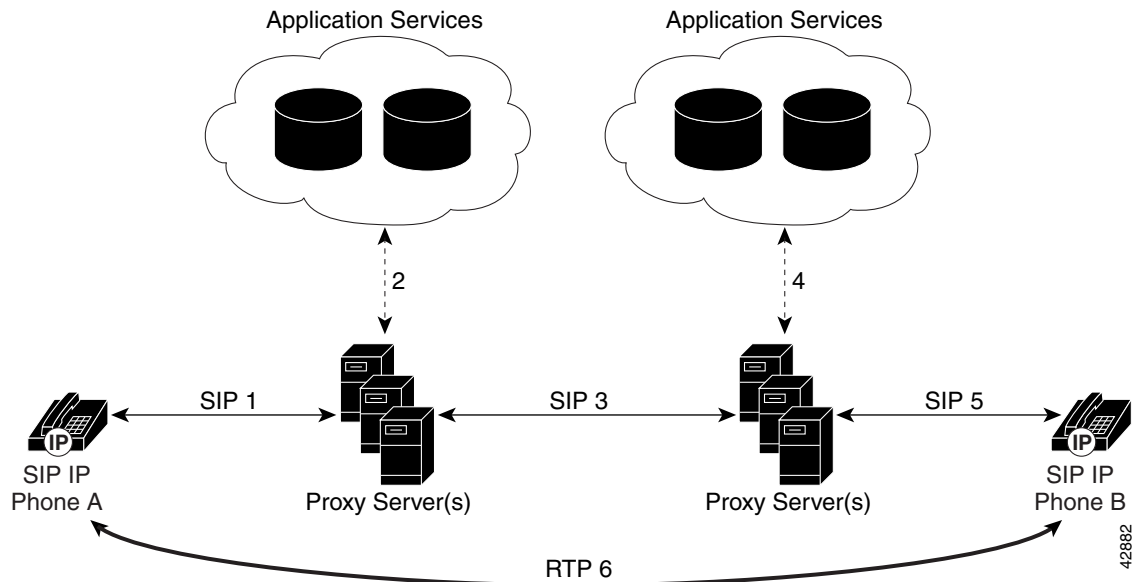
In this illustration:

1. Cisco SIP IP phone A initiates a call by sending an INVITE to the SIP proxy server. (There can be more than one proxy server for redundancy.)

2. The SIP proxy server might interact with application services, such as RADIUS, to obtain additional information.

3. The SIP proxy server in phone A's network contacts the SIP proxy server in phone B's network. The local proxy uses the domain name system (DNS) domain to determine if it should handle the call or route it to another proxy. The remote proxy is contacted based on the domain of the destination device.

4. The SIP proxy server in phone B's network might interact with application services to obtain additional information.

5. The SIP proxy server in phone B's network then contacts the destination phone (Cisco SIP IP phone B).

6. After responses and acknowledgments are exchanged, an RTP session is established between Cisco SIP IP phones A and B.

Note   SIP 200 OK, 180 Ringing, and 183 Session Progress messages will pass through the same set of proxies for they are in the same call sequence (cseq). SIP CANCEL or BYE requests sent by a terminating user agent might or might not pass through the same set of proxies.

For more information about the messages that are exchanged during call processes, see Chapter 7, "SIP Call Flow Process for the Cisco VoIP Infrastructure Solution for SIP."

Processing Calls Between a SIP IP Telephony Network and a Traditional Telephony Network

When calls are made between a SIP IP telephony network and a traditional telephony network, the process typically involves the origination phone, one or more proxy servers, a gateway, and a PBX or Public Switched Telephony Network (PSTN) device. Figure 2-9 is a simplified illustration of a call between a Cisco SIP IP phone and a traditional phone in a traditional telephony network.

Figure 2-10   Calls Between a SIP IP Telephony Network and a Traditional Telephony Network
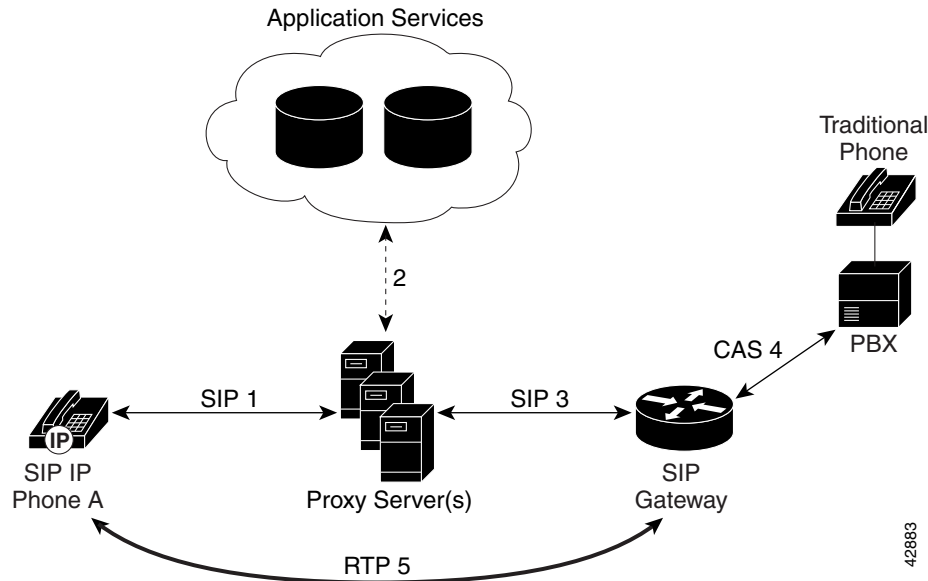
In this illustration:

1. Cisco SIP IP phone A initiates a call by sending an INVITE to the SIP proxy server. (There can be more than one proxy server for redundancy.)

2. The SIP proxy server might interact with application services, such as RADIUS, to obtain additional information.

3. The SIP proxy server proxies the INVITE to the Cisco SIP gateway.

4. The Cisco SIP gateway establishes communication with the traditional telephony network, in this case a PBX.

5. After responses and acknowledgments are exchanged, an RTP session is established between Cisco SIP IP phone and the Cisco SIP gateway. The signaling on the plain old telephone service (POTS) side of the gateway is translated into SIP messages on the IP network to provide proper ringback signaling to the end-user phones.

For more information about the messages that are exchanged during call processes, see Chapter 7, "SIP Call Flow Process for the Cisco VoIP Infrastructure Solution for SIP."

Cisco VoIP Infrastructure Solution for SIP Features

The Cisco VoIP Infrastructure Solution for SIP provides a variety of services. Table 2-1 lists various IP telephony services that are available with the Cisco VoIP Infrastructure Solution for SIP.

Table 2-1   Services of the Cisco VoIP Infrastructure Solution for SIP

Service	Description
Direct dialing based on digit dialing	Allows users to initiate or receive a call using a standard E.164 number format in a local, national, or international format.
Direct dialing based on email address	Allows users to initiate or receive a call using an email address instead of a phone number.
Private network dialing plan support	Allows administrators to implement private feature sets. The features allow for both originations and terminations from either the IP network or existing PSTN networks.
Direct inward dialing	Allows users from outside the SIP IP telephony network to dial a Cisco SIP IP phone number directly.
Direct outward dialing	Allows users within the SIP IP telephony network to obtain an outside line (for placing a call to a number outside the system) without the aid of a system attendant. This is typically accomplished by dialing a prefix number such as 8 or 9.
Consultation hold	Allows users to place a call from another user on hold.
Call forward network (unconditional, busy, and no answer)	Allows users to have the network forward calls. The user can request that all calls be forwarded (unconditional) or that only unanswered calls (busy or no answer) be forwarded.
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.
Three-way calling	Allows a user to receive a call and then add another user to the call. For example, user B receives a call from user A. User B then places user A on hold, contacts user C, and then reinstates the session with user A so that all three can participate in the call. User B acts as the bridge.
Call transfer with consultation (attended)	Allows users to transfer a call to another user. The transferring user places the other user on hold and calls the new number (equivalent to consultation hold). If the call is answered, the user can notify the new third user before the call is transferred.
Call transfer without consultation transfer (unattended)	Allows users to transfer a call to another user. The transferring user transfers the call to the new user without first contacting the third user.
Call waiting	Provides an audible tone to indicate that an incoming call is waiting. The user can then decide to terminate the existing call and take the new one or to route the unanswered Call Waiting call to another destination.

Service	Description
Multiple directory numbers	Allows an multiple directory numbers to be logically assigned to a terminal.
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.
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.

Components of the Cisco VoIP Infrastructure Solution for SIP

The Cisco VoIP Infrastructure Solution for SIP is composed of a SIP IP phone (Cisco Systems' SIP IP Phone 7960), a SIP gateway (integrated with Cisco Systems' IOS software), a SIP proxy server (Cisco SIP Proxy Server), a firewall (Cisco Secure PIX Firewall), and a VoIP solution for service providers (Cisco SS7 Interconnect for Voice Gateways Solution). This section contains an overview of each component and its role in the solution.

The Cisco SIP IP Phone 7960

The Cisco SIP IP phone (model 7960) is an IP telephony instrument that can be used in VoIP networks to send and receive calls using SIP. The phone complies with RFC 2543 and can be used for multimedia call session setup and control over IP networks. It is a business phone with an integrated SIP UA. The phone has more intelligence and autonomy than phones that use a master-slave call control protocol and provides a number of features that are typically implemented in a business style PBX, such as call hold and call transfer.

The Cisco SIP IP phone is a full-featured telephone that can be plugged (via its Ethernet interface) directly into your existing data network infrastructure and used very much like a standard PBX telephone. You can connect the phone to the 10BaseT/100BaseT interfaces of an Ethernet switch.

When used with a voice-capable Ethernet switch, the Cisco SIP IP phone eliminates the need for a traditional proprietary telephone set and key system or PBX. A *voice-capable Ethernet switch* is one that understands IP ToS bits and can prioritize VoIP traffic.

Cisco SIP IP Phone Features

The Cisco SIP IP phone provides the following operating features:

- 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 message)—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 (via the unsolicited NOTIFY message) is controlled by the voice-mail server.

- Speed dial to voice mail via the messages button

- Remote reset support (via the Event header in NOTIFY messages)

- In addition, the phone supports the following optional features:

    – 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 re-established.

    – 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 users to instruct the system to block their phone number or email address from phones that have caller identification capabilities.

    – Anonymous call blocking—Allows users to instruct the system to block any calls for which the identification is blocked.

Cisco SIP IP Phone Functional Areas

The Cisco SIP IP phone has seven functional areas (as shown in Figure 2-11).

Note   Round keys are called buttons and all other keys are referred to as keys.

Figure 2-11   Cisco Systems' SIP IP Phone

The areas noted above are:

1. LCD screen—Displays information about your Cisco SIP IP phone.

2. Line buttons—Used to open a new line.

3. Information button and keys—Provides access to information about the phone. (Available in a future release.)

4. Volume key—Used to increase or decrease the volume of your handset, headset, or speaker phone. Press HEADSET, MUTE or SPEAKER to toggle those functions on or off.

5. Soft keys—Used to activate the function described in the text label, which is displayed directly above the soft key button on the LCD screen.

6. Dial pad buttons—Used to dial a phone number. Dial pad buttons work exactly like those on a standard telephone.

7. Handset—Acts the same as a handset on standard phones. To place a call, you simply lift the handset and press the dial pad numbers.

The Cisco SIP Gateway

The Cisco SIP gateway, introduced in Cisco IOS Release 12.1(1)T and enhanced in Cisco IOS Release 12.1(3)T and subsequent releases, enables a Cisco access platform to act as a SIP UA (client or server) to signal the setup of voice and multimedia calls over IP networks. This allows users to tie VoIP networks that use SIP to traditional telephony networks.

Cisco SIP Gateway Features

The Cisco SIP gateway provides the following operating features:

- Support for a variety of signaling protocols, including Integrated Services Digital Network (ISDN) PRI and CAS.

- Support for a variety of interfaces, including

    - Analog interfaces: FXS/FXO/E&M analog interfaces.

    - Digital interfaces: T1 CAS, E1 CAS, and PRI.

- Support for SIP redirection messages and interaction with SIP proxy servers. The gateway can redirect an unanswered call to another SIP gateway or SIP IP phone. In addition, the gateway supports proxy-routed calls.

- Interoperability with DNS servers including support for DNS SRV and "A" records to look up SIP URLs.

- Support for SIP over TCP and UDP network protocols.

- Support RTP/RTCP for media transport in VoIP networks.

- Support for the following codecs:

Codec	SDP
G711ulaw	0
G711alaw	8
G723r63	4
G726r16	2
G728	15
G729r8	18

- Support for Record-Route headers.

- Support for IP Security (IP Sec) for SIP signaling messages.

- AAA support. For accounting, the gateway device generates call data record (CDR) accounting records for export. For authentication, the Cisco SIP gateway sends validate requests to an AAA server. For authorization, the existing access lists are used.

- Support for call hold. A mid-call INVITE message is received, which requests that the remote endpoint stop sending media streams.

- Support for call transfer. A mid-call INVITE message is received, which requests that the remote endpoint stop sending media streams. The call is then transferred to another user and the remote endpoint resumes sending the media stream. The call transfer is done without consultation. This is called an unattended transfer. The transfer can be initiated by a remote SIP endpoint.

- Support for configurable expiration time for SIP INVITEs and maximum number of proxies or redirect servers that can forward a SIP request.

- Expanded support for the mapping of PSTN cause codes to SIP events.

- Ability to hide the calling party's identity based on the setting of the ISDN presentation indicator.

- Support for Third-Party Call Control (via INVITE without Session Description Protocol [SDP] information).

- CC-Diversion Header for Redirecting Number support.

- Support of early media from PSTN.

The Cisco SIP Proxy Server

The Cisco SIP Proxy Server Version 1.0 provides the primary capabilities required for call session management in a VoIP network and processes SIP requests and responses as described in RFC 2543. Powered by Apache[TM], the Cisco SIP Proxy Server can be configured to operate as a transaction stateful or stateless server. The Cisco SIP Proxy Server can also be configured to provide additional server modes and features. For example, the Cisco server can be configured to:

- Function as a redirect or registrar server

- Translate E.164 numbers to URL via location server protocols such as Telephone Number Mapping (ENUM)

- Perform gateway and Domain Name System (DNS) routing

Note   This Cisco SIP Proxy Server includes software developed by the Apache Software Foundation (http://www.apache.org/).

Cisco SIP Proxy Server Features

The Cisco SIP Proxy Server provides the following features:

- Ability to function as a transaction stateful or stateless proxy server, stateful or stateless redirect server, and registrar server

- Call forwarding

- MySQL subscriber database interface

- Address translation

    - Registry database (static registry entries for contact points)

    - Gatekeeper Transaction Message Protocol (GKTMP) interface with Cisco NAM for 1-800, 1-900, and LNP lookups as well as least-cost routing

    - E.164 to URL address translation (via location server protocols such as ENUM and GKTMP)

- Next-hop routing

    - Static E.164 routes (dial plans)

    - Static domain routes

    - DNS SRV routes

- Authentication and authorization via Hypertext Transfer Protocol (HTTP) Digest and MySQL or via CHAP-password and RADIUS

- Accounting via RADIUS

- Server farm support for sharing registry database information

- SIP over User Datagram Protocol (UDP) transport protocol support

- Inter operability with Cisco SIP gateways, SIP IP phones, and unified messaging

- IP security (IPSec) for SIP signaling messages

- Access and error logging

The Cisco uOne Messaging System

In the Cisco VoIP Infrastructure Solution for SIP, uOne provides voice mail services for the Cisco SIP IP phone users. With unified messaging, subscribers can record personalized greetings to be used when they are unable to answer their phone, callers can leave messages for unavailable subscribers, and subscribers can subsequently retrieve the messages and either save or delete them as desired.

The uOne unified messaging application for SIP consists of the gateserver, the messaging server, and the directory server.

uOne Gateserver

The uOne gateserver is a Sun computer with uOne 4.2s. The gateserver communicates with the other components to provide messaging deposit and retrieval services.

uOne Messaging Server

The uOne messaging server is a Sun computer with Netscape Messaging Server 4.1. uOne interfaces with the messaging server using IMAP and SMTP protocols. The primary use of the messaging server is to store subscriber messages.

It is also used for some administrative functions including: storing subscriber personal greetings and distribution list recorded names; temporary storage of faxes to be printed, messages which cause SMS notifications, and outbound AMIS-A messages. Administration of the messaging server is accomplished through vendor-supplied tools and Cisco-supplied tools. Cisco tools include:

- Subscriber Telephone Personal Administration—This feature of the uOne application allows subscribers to administer their personal preferences using the telephone interface.

- uOne Administration—This web-based tool allows a system administrator to manage special administrative accounts, broadcast lists and user mailbox security, administer subscribers and AMIS-A users, classes of service, and pager and SMS notification, and validate subscriber entries. uOne Administration updates both the directory and messaging servers.

- PMA—This web-based tool provides subscribers with the ability to personalize their service through the telephone as well as a PC interface.

- Bulk Add Tool—This command line tool allows a system administrator to conveniently add large groups of new users in a batch mode. This tool can be used when migrating users from a legacy system to uOne or when existing profiles reside in an existing database.

uOne Directory Server

The uOne messaging server is a Sun computer with Netscape Directory Server 4.0. uOne interfaces with the directory server using the LDAP protocol. The primary use of the directory server is to store user profile information.

Administration of the directory server is accomplished through the vendor-supplied tools and Cisco-supplied tools. Cisco tools include:

- Subscriber Telephone Personal Administration—This feature of the uOne application allows subscribers to administer their personal preferences using the telephone interface.

- uOne Administration—This web-based tool allows a system administrator to manage special administrative accounts, broadcast lists and user mailbox security, administer subscribers and AMIS-A users, classes of service, and pager and SMS notification, and validate subscriber entries. uOne Administration updates both the directory and messaging servers.

- PMA—This web-based tool provides subscribers with the ability to personalize their service through a PC interface as an alternative to the telephone interface.

- Bulk Add Tool—This command line tool allows a system administrator to conveniently add large groups of new users in a batch mode. This tool can be used when migrating users from a legacy system to uOne or when existing profiles reside in an existing database.

uOne Features

The services provided by uOne to telephone subscribers can be grouped into the following categories:

- Call answer and caller services (Table 2-2)
- Subscriber services (Table 2-3)

When implementing the uOne SIP system, be aware of the following:

- A uOne SIP system supports the following payloads:
  - G.711 mu-law
  - G.729
  - Dynamic AVT tones payload: 97—127
  - Cisco RTP DTMF relay payload: 121
- A uOne SIP system does not support CODEC switching within a call.
- The uOne SIP system does not support Single Number Reach (SNR) services.
- The SIP uOne implementation supports Netscape messaging and directory servers for Internet Message Access Protocol (IMAP) / Lightweight Directory Access Protocol (LDAP) servers.

Note   Table 2-2 list the features supported in the uOne 4.2(2)s SIP Edition. For a complete list of uOne call answer and caller services features, see the *uOne Product Description* for Release 4.2.

Table 2-2   uOne 4.2(2)s SIP Edition Call Answer and Caller Services

Feature	Description
Support for multiple system prompts	Multiple language prompts can be loaded on the same system. The default is to play the prompts in English.
	Prompts are played in the preferred language of the subscriber. If the subscriber does not specify a preferred language, then the application-defined prompts (.ini file) are played. If there are no application-defined prompts, then default prompts are played.
Support for multiple greetings	The subscriber's defined greeting is played when a caller is routed to the Call Answer Service. The subscriber can record greetings for the following conditions: • All Calls • No Answer • Busy • After Hours • Extended Absence In addition, subscribers can choose to use the default system greeting and record only their name, which is inserted into the greeting.
Option to playback a recorded message	When leaving a message, the caller can playback the recorded message from the beginning. This feature is not available after a message is sent.
Option to re-record a message	When leaving a message, the caller can delete the recorded message and re-record. This feature is not available after a message is sent.
Option to append to message	When leaving a message, the caller can append additional recordings to the end of the currently recorded message. This feature is not available after a message is sent.
Option to cancel a message	When leaving a message, the caller can delete the currently recorded message and exit the answering system. This feature is not available after a message is sent.
Support for inbound voice messages	uOne allows the caller to record a message for the called party (subscriber). • The maximum length of the message is configured by the Service Provider. • The end of message length warning is configured by the Service Provider. • The caller is informed if the subscriber's mailbox is full. • If the subscriber enables the extended absence greeting, the caller is not allowed to leave a message.
Support for multiple inbound voice messages	uOne allows callers to leave another message for the same or different subscriber. After leaving a message, the system prompts callers to specify whether they would like to leave another message.

Table 2-2   uOne 4.2(2)s SIP Edition Call Answer and Caller Services (continued)

Special handling of urgent and confidential messages	After recording a message, the system allows callers to set delivery options and tag a message as urgent or confidential. • When subscribers retrieve messages, messages tagged as urgent by the caller are inventoried first and announced as urgent messages. • When subscribers retrieve messages, messages tagged as confidential by the caller are announced as confidential messages and cannot be forwarded.
Flexible support for addressing	uOne allows a variable-length string of digits to be handled as a single telephone number. The maximum number of digits is configurable. The system translates all addressing to unique variable-length phone numbers based upon rules configured by the system administrator. Two models of addressing are supported: numeric and name. If desired, the caller can dial or address the subscriber by spelling a subscriber's last name and then first name. The caller can toggle between numeric and name models.

Table 2-3   Subscriber Services

Feature	Description
Subscriber login support	At the first login, subscribers are required to change their PIN and record their spoken name. Optionally, they can also record their personal greeting for all calls. The PIN can be of a fixed or variable length (from four to eight characters, depending on configured limits). The system allows multiple logins simultaneously to the same account. After the maximum number of consecutive failed login attempts in a single session, uOne disconnects the session. After the maximum number of consecutive failed login attempts across a configurable number of sessions, the system locks the caller out. The account can be reset only by the Service Provider. All failed login attempts are logged.

Table 2-3   Subscriber Services (continued)

Special handling of urgent and confidential messages	Urgent, new messages are inventoried first.
	Urgent, new voice and email messages are inventoried together and presented before standard messages.
	If subscribers choose not to listen to their urgent, new messages and skip to their standard messages (of any type), then the urgent messages are inventoried again as standard (of the right type). The headers include "urgent" as the message type.
	If the subscriber retrieves urgent messages immediately after urgent message inventory, all urgent messages are played in a "first in first out" order. Urgent messages are followed by new voice message inventory and, if configured, automatic retrieval of new voice messages.
	Confidential messages cannot be forwarded from the telephone. If the subscriber accesses the message from a PC, the subject line is tagged as confidential. They can forward the message as e-mail.
Standard voice message handling	Standard voice messages are played in a "first in first out" order.
	Messages remain new until the message is explicitly deleted or saved.
	If the subscriber sets headers on, the system plays the message header followed by the message itself. If headers are off, then only the message is played. In either case, the subscriber can press "5" to hear the message header of the current message.
	Undeliverable voice messages are returned with the original message attached. The message header will indicate that the voice message is undeliverable.
	If Message AutoPlay is on and new messages exist, the system plays the message inventory and then prompts the subscriber with the Message Type menu. If Message AutoPlay is off, the subscriber must also select the Get Messages option from the Main Menu to before the Message Type menu is played.
Message inventory handling	Standard voice messages are inventoried after urgent voice messages.
	When an inventory of a large number of messages takes some time to complete, the subscriber is periodically informed (at a configurable interval) that the inventory is still in progress.
	Optionally, the subscriber can interrupt the inventory at any time. This interrupt is not immediate; it takes effect after a configurable interval expires.
	If re-inventory is on, voice messages are re-inventoried when a subscriber returns to the main menu. If re-inventory is off, the voice messages are inventoried only once (at the beginning of a session).

Table 2-3   Subscriber Services (continued)

Options for message retrieval	Play/Replay message—Plays the message from the beginning.
	Play Header—Allows the subscriber to play the header of the current message. The header contains message type (urgent, confidential, forwarded, broadcast, undeliverable), who the message is from, and the date and time the message was left. The subscriber can choose whether the date and time is played in US or European format. The time zone is also configurable.
	Reply by voice mail—Allows the subscriber to send a voice message in reply to a sender's message. The original message is not attached in the reply. This feature is available only if the sender is also a subscriber.
	Forward message—Allows the subscriber to forward a message with or without a comment to one or more subscribers (including the use of distribution and broadcast lists).
	Rewind and Advance—Allows the subscriber to skip forward or backward three seconds during message play.
	Backup to previous message—Allows a subscriber to backup to the previous message even if it was deleted (during the same session).
	Save message—Saves the current message and skips to the next message.
	Delete message—Deletes the current message and skips to the next message.
	Undelete a message—Allows the subscriber to undelete a message (during the same session) by backing up to the deleted message and then saving it (or making it new).
	Subscribers can also flag a message in their mailbox (including current message, undeleted messages, and saved messages) as "new". The message is inventoried as a new message. If the message is new, the message waiting light remains on. If the message was a saved message that the user has flagged as new, the message light will not turn on.

Flexible Deployment Scenarios

The modular design of the uOne application allows maximum flexibility in distributed deployment scenarios. Depending on the business need, the service can be deployed completely centralized, completely distributed, or a hybrid hub and spoke scenario.

In a decentralized solution, Service Providers can provide local call access. Local call access is the ability to dial into the closest Gateserver to access subscriber services. For example, subscribers who normally work in New York City would dial from their telephones the local 212 access number to get their messages. When they are visiting San Francisco, they would dial the local 415 access number to get their messages. The messages would be pulled across the IP infrastructure, perhaps from a messaging server in New York. This is similar to the way PCs access their Internet Service Provider or online services, such as America Online.

Figure 2-12 illustrates a centralized set of backend servers with distributed VoIP telephony access. Gateways are generally deployed at the points of presence and provide local call access and subsequent conversion to H.323 for access to uOne services over an IP network.

Figure 2-12   Centralized Solution
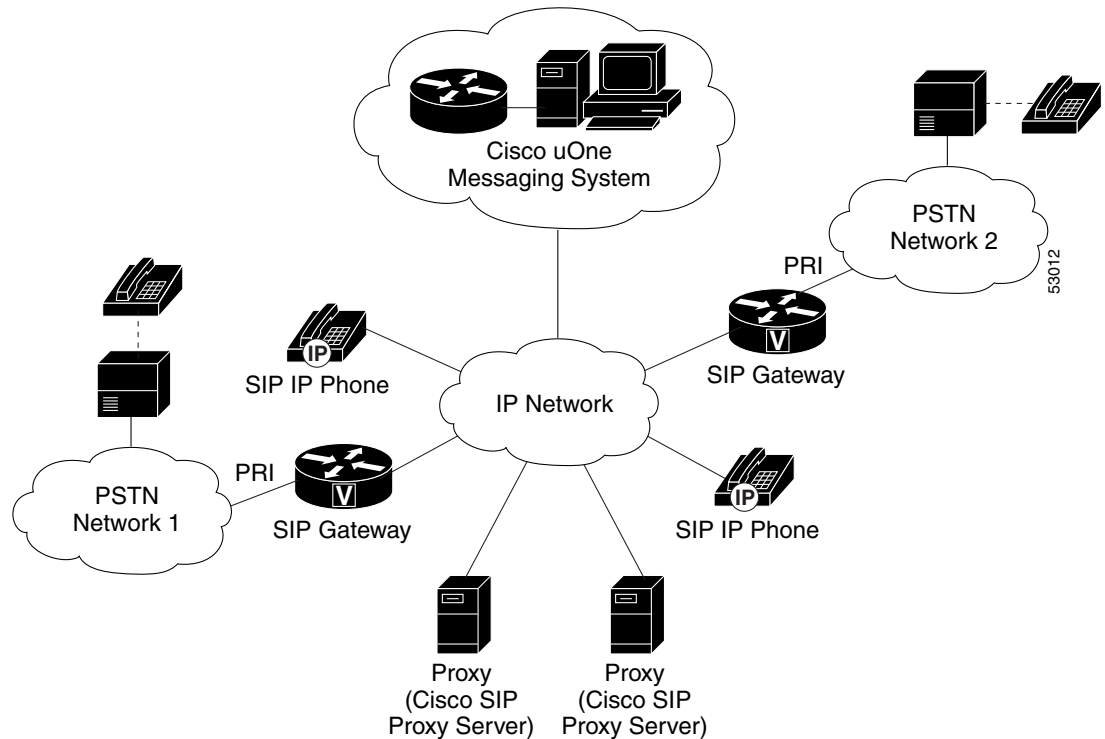
The Cisco Secure PIX Firewall

The Private Internet Exchange (PIX) Firewall provides full firewall protection that conceals the architecture of an internal network from the outside world. The PIX Firewall allows secure access to the Internet from within existing private networks and the ability to expand and reconfigure TCP/IP networks without being concerned about a shortage of IP addresses. With PIX Firewall, users can take advantage of larger address classes than they may have been assigned by the Internet's Network Information Center (NIC). PIX Firewall provides this access through its Network Address Translation (NAT) facility as described by RFC 1631.

Cisco Secure PIX Firewall Features

The PIX Firewall has the following features:

- Firewall capability that keeps intruders out of your internal network while permitting regulated conduit access through the firewall for services such as electronic mail, Telnet, FTP, SNMP, and HTTP (World Wide Web) use.

- Network translation services that let a site share one or more NIC-registered IP addresses among many users.

- An Identity feature that lets NIC-registered IP addresses pass through the firewall without address translation, while still retaining Adaptive Security.

- Better performance than competing firewalls. The PIX Firewall gains speed through a patent-pending process called Cut-Through proxies, which is the fastest way for a firewall to authenticate a user. Unlike a proxy server that must analyze every packet at layer seven of the OSI model, a time- and processing-intensive function, the PIX Firewall first queries a TACACS+ or RADIUS server for authentication. Once approved, the PIX Firewall then establishes a data flow and all traffic thereafter flows directly and quickly between the two parties. This Cut-Through capability allows the PIX Firewall to perform dramatically faster than proxy-based servers while maintaining session state.

- Support for SNMP MIB-II gets and traps.

- Simplified configuration and system management with an HTML interface.

- Support for Telnet, FTP, and HTTP access using RADIUS (Remote Authentication Dial-In User Service) and TACACS+ security systems. PIX Firewall authenticates users in conjunction with the security systems that Cisco routers support. The security clients run on Cisco routers and send authentication requests to a central security server, which contains all user authentication and network service access information.

- Failover capability that permits a secondary PIX Firewall unit to take over firewall communications if the primary unit fails.

- Support for 10BaseT and 100BaseTX networking.

Cisco Secure PIX Firewall SIP Configuration Guidelines

When using the Cisco Secure PIX Firewall with SIP, be aware of the following:

- If a firewall proxy is placed outside the firewall in the demilitarized zone (DMZ) network with Record-Route enabled, the list of allowed IP addresses from the outside SIP proxy server's IP address should be small and manageable, thus allowing for manageable security.

- Outside callers cannot make calls to inside the firewall unless they have been defined as an allowed device.

The Cisco SS7 Interconnect for Voice Gateways Solution

The Cisco SS7 Interconnect for Voice Gateways Solution is a distributed system that provides SS7 connectivity for VoIP access gateways using the Cisco Signaling Controller (also referred to as the Cisco SC2200 product) and the access gateways as a bridge from the SIP IP network to the PSTN network. This solution interacts over the IP network with other Cisco SIP VoIP access gateways. In addition, the Cisco SS7 Interconnect for Voice Gateways Solution can interoperate with SIP endpoints, using non-SS7 signaling such as ISDN PRI and channelized T1.

The Cisco SS7 Interconnect for Voice Gateways Solution consists of the following:

- Cisco Signaling Controller Host (Cisco SC2200), which operates as an SS7 to ISDN protocol converter front-end to the Cisco access gateways.

- Cisco Signaling Link Terminal (Cisco SLT), which is used for physical SS7 link termination.

- Cisco Access Gateway (Cisco AS5300), which is used for bearer channel termination.

- LAN Switch (Cisco Catalyst Switch Family), which extends VLANs across platforms through backbone Fast Ethernet, Gigabit, or ATM connections, when necessary. Connects multiple Cisco SLTs to the active and standby hosts within the SC node. Connects the Network Access Servers with their controlling SC node. Connects the originating SC zone to the terminating SC node between SC zones.

Cisco SS7 Interconnect for Voice Gateways Solution Features

The Cisco SS7 Interconnect for Voice Gateways Solution provides the following features:

- Directly connects access gateways to PSTN in a peer-to-peer interconnect, which reduces network costs and allows users to interconnect with more favorable tariffs and rates

- Provides SS7 connectivity for SIP endpoints

- Support for co-located and distributed access gateways

- Terminates and originates switching-system functions

- Provides worldwide protocol support using Cisco Message Definition Language (MDL)

- Provides a reliable IP link between signaling controllers and access gateways with Redundant Link Manager (RLM)

- Support for RADIUS or TACACS+ AAA functions, including authentication based on calling or called number

- Provides call detail records (CDR) for PSTN billing

- Provides a RADIUS Proxy (GRS)

- Provides facility associated signaling through the Cisco SLTs, which means it grooms the bearer channels and then delivers, or hairpins, them to the access gateway. It also backhauls MTP-3 to the signaling controller over Reliable User Datagram Protocol (RUDP)/IP

- Provides a fault-tolerant platform (no more than 6 seconds of downtime per year) and a continuous service platform (established calls are maintained upon failover)

Related Documents

The following documents provide additional information about the components of the Cisco VoIP Infrastructure Solution for SIP:

- *Cisco SIP IP Phone 7960 Administrator Guide, Version 2.0*

- *Getting Started Cisco 7960 IP Phone*

- *Cisco SIP Proxy Server Administrator Guide, Version 1.0*

- *CD Installation Guide for the Cisco SIP Proxy Server on Linux*

- *CD Installation Guide for the Cisco SIP Proxy Server on Solaris*

- *Enhancements for the Session Initiation Protocol for VoIP on Cisco Access Platforms*

- *Session Initiation Protocol Gateway Call Flows* (as implemented for Cisco IOS Release 12.1(5) XM)

- *Cisco IOS Multiservice Applications Command Reference*

- *Cisco IOS Multiservice Applications Configuration Guide*

- *Getting Started with uOne 4.2(2)s*

- *uOne Administration Manual, Release 4.2(2)s*

- *uOne Back End Servers Reference Manual, Release 4.2(2)s*

- *uOne Gateserver Installation and Configuration Manual, Release 4.2(2)s*

- *uOne Operations Manual, Release 4.2(2)s*

- *uOne User's Guide, Release 4.2(2)s*

- *uOne 4.2(2)s Quick Start User Guide* (Available in .pdf format only.)

- *uOne 4.2(x)s Release Notes*

- *Getting Started with uOne 4.2(2)s, SIP Edition*

- *Installing and Configuring uOne 4.2(2)s, SIP Edition*

- *SIP Compliance and Signaling Call Flows for uOne 4.2(2)s, SIP Edition*

- *Providing Operations Support of uOne 4.2(2)s, SIP Edition*

- *Using uOne 4.2(2)s, SIP Edition*

- *uOne 4.2(2)s SIP Edition Release Notes*

- *Installation Guide for the Cisco Secure PIX Firewall, Version 6.0*

- *Configuration Guide for the Cisco Secure PIX Firewall, Version 6.0*

- *System Log Messages for the Cisco Secure PIX Firewall, Version 6.0*

- *Cisco SS7 Interconnect for Voice Gateways Solution Overview*

- *Cisco Media Gateway Controller Hardware Installation Guide, Release 9*

- *Cisco MGC Software Release 9 Installation & Configuration Guide*

- *SS7 Interconnect for Access Servers/Voice Gateways Gateway Guide*

- *SS7 Interconnect for Access Servers/Voice Gateways Provisioning Guide*

- *Cisco MGC Software Provisioning Guide, Release 9*

- *Cisco MGC Software Release 9 Reference Guide, Release 9*

- *Cisco MGC Operations, Maintenance, and Troubleshooting Guide, Release 9*

Installing the Cisco VoIP Infrastructure Solution for SIP

This chapter provides an overview of how to install the components of the Cisco VoIP Infrastructure Solution for SIP. It includes the following sections:

- Equipment Requirements, page 3-1
- Installing the SIP Gateway, page 3-7
- Installing the SIP IP Phone, page 3-7
- Installing the SIP Proxy Server, page 3-8
- Installing the Cisco uOne Messaging System, page 3-9
- Installing the Cisco Secure PIX Firewall, page 3-10
- Installing the SS7 Interconnect for Voice Gateways Solution, page 3-10

Equipment Requirements

To implement the Cisco VoIP Infrastructure Solution for SIP, you must start with a functional IP network. Then, depending on which phase of the solution (as described in Illustrated Implementations, page 2-1) you want to implement, you must have the following (components that are not provided as part of the solution are italicized):

Phase	Solution Equipment Required

1	Cisco Enterprise Gateway (Cisco 2600 series, Cisco 3600 series, or Cisco AS5300 router) with:
	
	• Minimum voice card for the selected router
	   – 5300:AS53-T1-48VOXD
	   – 36xx/26xx: NM-HDV-2T1-24
	
	• Cisco IOS Software Release 12.1(5)XM or later
	   – c*xxxx*-is-mz
	   – c*xxxx*-is56i-mz
	   – c*xxxx*-js-mz
	   – c*xxxx*-js56i-mx
	
	Where *xxxx* identifies the model of router.

Phase	Solution Equipment Required

2	Cisco Enterprise Gateway (Cisco 2600 series, Cisco 3600 series, or Cisco AS5300 router) with:
	
	• Appropriate voice card for the selected router
	   – 5300:AS53-T1-24VOX
	   – 36xx/26xx: NM-HDV-2T1-24
	• Cisco IOS Software Release 12.1(5)XM
	   – c*xxxx*-is-mz
	   – c*xxxx*-is56i-mz
	   – c*xxxx*-js-mz
	   – c*xxxx*-js56i-mx
	Where *xxxx* identifies the model of router.
	
	Plus:
	
	Cisco SIP Proxy Server, Version 1.0
	• Solaris platform:
	   – Workstation—Sparc or UltraSparc server class machine with a minimum of 256 MB of RAM and 1 GB of disk space
	   – Solaris 2.6 Operating Environment or later
	• Linux platform:
	   – PC—Intel Pentium III processor operating with a minimum of 128 MB of RAM and 1 GB of disk space
	   – Linux Kernel 2.2.13 or later

3	Cisco Enterprise Gateway (Cisco 2600 series, Cisco 3600 series, or Cisco AS5300 router) with:
	
	• Appropriate voice card for the selected router
	   – 5300:AS53-T1-24VOX
	   – 36xx/26xx: NM-HDV-2T1-24
	• Cisco IOS Software Release 12.1(5)XM
	   – c*xxxx*-is-mz
	   – c*xxxx*-is56i-mz
	   – c*xxxx*-js-mz
	   – c*xxxx*-js56i-mx
	Where *xxxx* identifies the model of router.
	
	Cisco SIP Proxy Server, Version 1.0 (see Phase 2 for specifics)
	
	Plus:
	
	Cisco SIP IP Phones 7960, Version 2.0

Phase	Solution Equipment Required
4	Cisco Enterprise Gateway (Cisco 2600 series, Cisco 3600 series, or Cisco AS5300 router) with: • Appropriate voice card for the selected router – 5300:AS53-T1-24VOX – 36xx/26xx: NM-HDV-2T1-24 • Cisco IOS Software Release 12.1(5)XM – c*xxxx*-is-mz – c*xxxx*-is56i-mz – c*xxxx*-js-mz – c*xxxx*-js56i-mx Where *xxxx* identifies the model of router. Cisco SIP Proxy Server, Version 1.0 (see Phase 2 for specifics) Cisco SIP IP Phones 7960, Version 2.0 **Plus:** *Application servers and databases*

Phase	Solution Equipment Required
5	Cisco Enterprise Gateway (Cisco 2600 series, Cisco 3600 series, or Cisco AS5300 router) with: • Appropriate voice card for the selected router – 5300:AS53-T1-24VOX – 36xx/26xx: NM-HDV-2T1-24 • Cisco IOS Software Release 12.1(5)XM – c*xxxx*-is-mz – c*xxxx*-is56i-mz – c*xxxx*-js-mz – c*xxxx*-js56i-mx Where *xxxx* identifies the model of router. *Ecosystem partner proxy server* *Application servers and databases* Cisco SIP Proxy Server, Version 1.0 (see Phase 2 for specifics) Cisco SIP IP Phones 7960, Version 2.0 **Plus:** uOne Messaging System, Service Provider Products, Release 4.2(2)s, SIP Edition • uOne messaging server: – Sun computer (A26-AA-R) – Solaris 2.6 – Netscape Messaging Server 4.1 • uOne directory server – Sun computer (A26-AA-R) – Solaris 2.6 – Netscape Directory Server 4.0 • uOne gateserver – Sun Sparc server class host with 512 MB RAM and a 4GB disk, dual CPU 300 MHz (N03-UEC2-9N-512AE) – Solaris 2.6 – uOne gateserver software, version 4.2 **Note** For uOne fax support, see the IOS Compatibility section of the Release Notes for uOne.

Phase	Solution Equipment Required
6	Cisco Enterprise Gateway (Cisco 2600 series, Cisco 3600 series, or Cisco AS5300 router) with:

- Appropriate voice card for the selected router
  - 5300:AS53-T1-24VOX
  - 36xx/26xx: NM-HDV-2T1-24
- Cisco IOS Software Release 12.1(5)XM
  - c*xxxx*-is-mz
  - c*xxxx*-is56i-mz
  - c*xxxx*-js-mz
  - c*xxxx*-js56i-mx

Where *xxxx* identifies the model of router.

Ecosystem partner proxy server

Application servers and databases

Cisco SIP Proxy Server, Version 1.0 (see Phase 2 for specifics)

Cisco SIP IP Phones 7960, Version 2.0

Cisco uOne Messaging System, Service Provider Products, Release 4.2(2)s, SIP Edition (see Phase 5 for specifics)

Plus:

Cisco PIX Firewall, Version 6.0 (PIX 535, PIX 525, PIX 515, PIX 506, or PIX 520 or earlier model)

Phase	Solution Equipment Required
7	Cisco Enterprise Gateway (Cisco 2600 series, Cisco 3600 series, or Cisco AS5300 router) with:
	• Appropriate voice card for the selected router
	– 5300:AS53-T1-24VOX
	– 36xx/26xx: NM-HDV-2T1-24
	• Cisco IOS Software Release 12.1(5)XM
	– c*xxxx*-is-mz
	– c*xxxx*-is56i-mz
	– c*xxxx*-js-mz
	– c*xxxx*-js56i-mx
	Where *xxxx* identifies the model of router.
	Ecosystem partner proxy server
	Application servers and databases
	Cisco SIP Proxy Server, Version 1.0 (see Phase 2 for specifics)
	Cisco SIP IP Phones 7960, Version 2.0
	Cisco uOne Messaging System, Service Provider Products, Release 4.2(2)s, SIP Edition (see Phase 5 for specifics)
	Cisco PIX Firewall, Version 6.0
	Plus:
	SS7 Interconnect for Voice Gateways Solution
	• Cisco Signaling Link Terminal (Cisco SLT)
	– Cisco 2600 Services Router
	– Cisco IOS Release 12.1(1)T
	• Cisco Signaling Controller Host (Cisco SC2200), Release 7.4
	– Sun Netra t 1400, Netra t 1405, Netra t 1120, Netra t 1125, or E450
	– Solaris 2.6
	• Cisco Network Access Server
	– Cisco AS5300 Universal Access Server Router
	• Catalyst Switch (customer premise hardware)

In addition to the components previously listed, you should have the following installed and operational in your network:

- TFTP server—To download the SIP firmware for the SIP IP phone and update IOS images.

- DHCP server—To provide IP addresses and other parameters to the SIP IP phone.

- DNS server—(optional) To resolve addresses for the components, particularly the SIP IP phone.

Installing the SIP Gateway

Install your Cisco 2600 Series, 3600 Series, or AS5300 router per the instructions that accompanied the router. Ensure that the appropriate network cards are installed and that the routers are running the correct release of Cisco IOS Software.

For the	Reference
Cisco 2600 Series Router	*Cisco 2600 Series Hardware Installation Guide*
	WAN Interface Cards Hardware Installation Guide
Cisco 3600 Series Router	*Cisco 3600 Series Hardware Installation Guide*
	WAN Interface Cards Hardware Installation Guide
Cisco AS5300 Router	*Cisco AS5300 Chassis Installation Guide*
	Cisco AS5300 Module Installation Guide

Installing the SIP IP Phone

Use the following procedure to connect the cables to your Cisco SIP IP phone.

Step 1   Place your Cisco SIP IP phone on a flat surface with the LCD side down. On the rear of your Cisco SIP IP phone there are several jacks. Review the Figure 3-1 to determine the use of each jack.

Figure 3-1   Rear of the SIP IP Phone
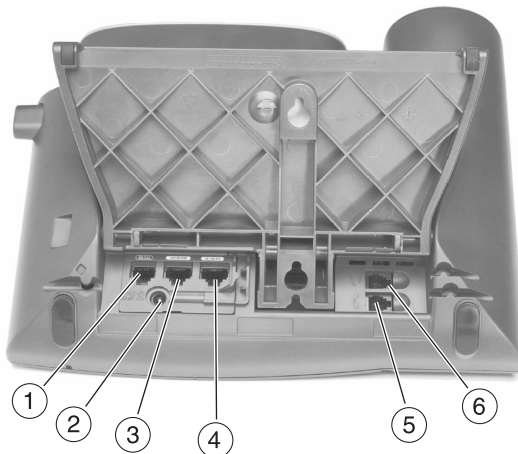
1. RJ-11/RS-232 (This jack is not used.)

2. AC Adapter port

3. LAN-to-phone jack (This jack is labeled 10/100 SW.)

4. PC-to-phone jack (This jack is labeled 10/100 PC.)

5. Handset jack

6. Headset jack

Step 2   Plug one end of the AC adapter cord into the back of your Cisco SIP IP phone and the other end into an electrical outlet. There is an AC adapter power brick in the path.

Step 3   Plug one end of your RJ-45 LAN cable into the LAN-to-phone jack and the other end into your LAN RJ-45 port.

Step 4   Plug one end of your RJ-45 PC cable into the PC-to-phone jack and the other end into the RJ-45 port on your PC.

Step 5   Plug one end of the handset cord into the handset jack on the back of the Cisco SIP IP phone and the other end into your handset.

Step 6   If you use a headset (not supplied) plug one end of the headset cord into the headset jack on the back of the Cisco IP phone and your headset is ready for use.

Note   For complete information about installing the Cisco SIP IP phone, see the *Cisco SIP IP Phone 7960 Administrator Guide, Version 2.0*.

Installing the SIP Proxy Server

There are two versions of the Cisco SIP Proxy Server: a version that runs on Linux and a version that runs on Solaris. Before installing the Cisco SIP Proxy Server, ensure that the Sun Sparc server or PC server platform on which the proxy server will be run is installed and connected to your network per the instructions that accompanied the system.

The following sections describe how to install the Cisco SIP Proxy Server on each platform:

- Installing the Cisco SIP Server Linux Software, page 3-8
- Installing the Cisco SIP Proxy Server Solaris Software, page 3-9

Installing the Cisco SIP Server Linux Software

There is a Cisco SIP Proxy Server software binary image and a Red Hat Package Manager (RPM) image.

To install the Cisco SIP Server Linux software, complete the following tasks:

Step 1   Mount the Cisco SIP Proxy Server CD-ROM.

Step 2   Install the Cisco SIP Proxy Server by complete the following:

a.   Log in as **root**.

b.   Change directories to the directory in which the Cisco SIP Proxy Server software images are located.

c. To decompress and install the Cisco SIP Proxy Server binary image into the */usr/local/sip* directory, issue the following command:

```
gunzip -d -c sip-server-1.0-linux.tar.gz | tar xvfP -
```

To install the Cisco RPM image into the */usr/local/sip* directory, issue the following command:

```
rpm -i sip-server-1.0-linux.i386.rpm
```

Step 3 Unmount the Cisco SIP Proxy Server CD-ROM.

Note For complete information about installing the Cisco SIP Proxy Server on Linux, see the *CD Installation Guide for the Cisco SIP Proxy Server on Linux*.

Installing the Cisco SIP Proxy Server Solaris Software

To install the Cisco SIP Server Solaris software, complete the following tasks:

Step 1 Mount the Cisco SIP Proxy Server CD-ROM.

Step 2 Install the Cisco SIP Proxy Server by complete the following:

a. Log in as **root**.

b. Change directories to the directory in which the Cisco SIP Proxy Server software image is located.

c. Decompress and install the Cisco SIP Proxy Server software image into the */opt/sip* directory by issuing the following command:

```
gunzip -d -c sip-server-1.0-solaris.tar.gz | tar xvfP -
```

Step 3 Unmount the Cisco SIP Proxy Server CD-ROM.

Note For complete information about installing the Cisco SIP Proxy Server on Linux, see the *CD Installation Guide for the Cisco SIP Proxy Server on Solaris*.

Installing the Cisco uOne Messaging System

The uOne Messaging System is composed of three components: a gateserver and two backend servers (the directory server and the message server). These components run on a Sun Sparc server. Before installing the Cisco uOne system software, ensure that the Sun Sparc server and operating system is configured per the instructions that accompanied the platform.

To install the Cisco uOne system software, complete the following tasks:

	Task	References
Step 1	Install the uOne 4.2(2)s files on the directory server.	*uOne BackEnd Servers Reference Manual, Release 4.2(2)s*
Step 2	Install the uOne 4.2(2)s files on the messaging server.	
Step 3	Configure the gateserver host operating system are recommended.	*uOne Gateserver Installation and Configuration Manual, Release 4.2(2)s*
Step 4	Install the uOne 4.2(2)s software packages on the gateserver.	*Installing and Configuring uOne 4.2(2)s, SIP Edition* *uOne Gateserver Installation and Configuration Manual, Release 4.2(2)s*

Installing the Cisco Secure PIX Firewall

Any Cisco Secure PIX Firewall model running Version 6.0 can be used in the Cisco VoIP Infrastructure Solution for SIP. Install and connect the Cisco Secure PIX Firewall per the instructions that accompanied the device.

Note   For complete information about installing the Cisco Secure PIX Firewall, see the latest version of the *Installation Guide for the Cisco Secure PIX Firewall*.

Installing the SS7 Interconnect for Voice Gateways Solution

Install your Cisco 2600 Series router and your SC2200 media gateway controller per the instructions that accompanied the devices. Ensure that the appropriate network cards are installed and that the devices are running the correct release of software.

For the	Reference
Cisco 2600 Series Router	*Cisco 2600 Series Hardware Installation Guide* *WAN Interface Cards Hardware Installation Guide*
Cisco SC2200	*Cisco Media Gateway Controller Hardware Installation Guide* *Cisco MGC Software Release 9 Installation & Configuration Guide*
Cisco AS5300 Router	*Cisco AS5300 Chassis Installation Guide* *Cisco AS5300 Module Installation Guide*
Catalyst Switch	Documentation that shipped with the Catalyst switch. The switch is customer premises equipment.

Configuring the Cisco VoIP Infrastructure Solution for SIP

This chapter provides scenario-based examples of how to configure the components of the Cisco VoIP Infrastructure Solution for SIP. It includes the following sections:

Configuring the Routers

Before you can configure your access server or router to use VoIP, you must first complete the following tasks:

- Install the voice feature card (VFC) or a voice network module (VNM) into the appropriate bay of your Cisco access server or router. For more information about the physical characteristics and capacity, memory requirements, or installation instructions for the VNM or VFC, refer to the installation documentation supplied with your VNM or VFC.

- Complete basic configuration for your router or access server. For more information about these basic configuration tasks, refer to the software installation and configuration guide that shipped with your device. For more information about configuring IP, refer to the "IP Overview," "Configuring IP Addressing," and "Configuring IP Services" chapters in the *Cisco IOS IP and IP Routing Configuration Guide*.

- Complete your company dial plan.

- Establish a working telephony network based on your company dial plan.

- Integrate your dial plan and telephony network into your existing IP network topology. How you merge your IP and telephony networks depends on your particular network topology. In general, we recommend the following suggestions:

  - Use canonical numbers wherever possible. It is important to avoid situations where numbering systems are significantly different on different routers or access servers in your network.

  - Make routing or dialing transparent to the user—for example, avoid secondary dial tones from secondary switches, where possible.

- Contact your PBX vendor for instructions about how to reconfigure the appropriate PBX interfaces.

- For each Cisco AS5300 access server installed in your solution that will connect to the Cisco SS7 Interconnect for Voice Gateway Solution, configure the access gateway by performing the tasks listed in the "Configuring the Cisco AS5300 Universal Access Server" section on page 4-26.

Configuring VoIP Support

After you have configured your router or access server for basic IP support, you are ready to configure the device to support VoIP. To configure basic VoIP, perform the following tasks:

- Configure IP networks for real-time voice traffic (required)

- Configure VoIP over Frame Relay (optional)

- Configure analog voice ports (required)

- Configure digital voice ports (required)

- Configure dial peers (required)

- Configure number expansion (optional)

- Optimize dial peer and network interface configurations (optional)

- Simulate a trunk connection (optional)

Note   For complete information about configuring VoIP, see the "Configuring Voice over IP" chapter of the *Cisco IOS Multiservice Applications Configuration Guide*.

Configuring the Cisco SIP Gateway

After you have configured the basic VoIP support, you must configure the router or access server to function as a Cisco SIP gateway. To configure SIP support, perform the following tasks:

- Configure the session transport type to use SIP across all dial peers.

- Configure each dial peer as follows:

  - Specify **sipv2** as the session protocol type.

  - Specify the global SIP server as the session target.

Note   Cisco Systems VoIP routers support a standard numbering scheme. This scheme complies to the ITU-T E.164 recommendations. For example, in North America, the North American Numbering Plan (NANP) is used, which consists of an area code, an office code, and a station code. Area codes are assigned geographically, office codes are assigned to specific switches, and station codes identify a specific port on that switch. The format in North America is 1Nxx-Nxx-xxxx, where N = digits 2 through 9 and x = digits 0 through 9. Internationally, each country is assigned a one- to three-digit country code; the country's dialing plan follows the country code.

However, by default, the SIP gateway tags called numbers that have 11 or more digits as "unknown" when sending SETUP messages to the PSTN switch.

To accommodate such situations, you must define translation rules on the outbound POTS dial peer to convert the "type of number" to the correct value. Translation rules manipulate the called number digits and the "type of number" value associated with the called digits.

Note   For complete information about configuring SIP on your router or access server, see the *Enhancements for the Session Initiation Protocol for VoIP on Cisco Access Platforms* feature documentation for Cisco IOS Software Release 12.1(3)T.

Configuring the Cisco SIP IP Phones

The Cisco SIP IP phones obtain their configuration parameters from network devices during their boot-up process. Network parameters can be configured manually or obtained from a DHCP server. SIP parameters can be configured manually or obtained from a TFTP server.

Before you configure the Cisco SIP IP phones, you should obtain the following files from Cisco's Connection Online (CCO) and place them in 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.
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.

P0S3*xxyy*.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.

Note   For complete information about configuring the Cisco SIP IP phone, see the *Cisco SIP IP Phone 7960 Administration Guide, Version 2.0.*

Configuring Startup Network Parameters

Network parameters are the parameters that are required for the phone to connect to the network. They can be configured manually or obtained from a DHCP server. We recommend that you use the DHCP server to distribute network parameters.

If you use DHCP to configure the network parameters, ensure that the following DHCP options have been configured on your DHCP server before you connect your Cisco SIP IP phone:

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

Configuring SIP Parameters

The SIP parameters are the parameters that the IP phone needs to operate in a SIP environment. The firmware image version that the phone should be running is also defined in the configuration file. Each phone must have its own configuration file.

Upon startup or reboot, Cisco SIP IP phones request their configuration files from the TFTP server. If a configuration file is unavailable on the TFTP server, the phone will use the SIP parameters that were last stored in Flash (as described in the "Configuring the Phone's SIP Settings" section of the *Cisco SIP IP Phone 7960 Administration Guide*).

There are two types of configuration files:

- Parameters that are common to all phones can be specified in the default configuration file (SIPDefault.cnf). These parameters can include the image version, the preferred codec, and the address of the proxy server.

- Parameters that are specific to a phone, such as the URL or E.164 number assigned to each line, should be specified in a phone-specific configuration file. The name of the phone-specific configuration file must be SIP*XXXXYYYYZZZZ*.cnf, where *XXXXYYYYZZZZ* is the MAC address of the phone. All characters in the file name must be capitalized and the extension (.cnf) must be lower case.

Using an ASCII text editor, edit the default configuration file and specify the desired parameters. Then, using an ASCII text editor, create a configuration file for each phone that you plan to install. You can define settings for up to six lines.

The SIP phone system parameters (typically defined in the default configuration file) are as follows:

- **image_version**—Firmware version that the Cisco SIP IP phone should run.

  Enter the name of the image version (as 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**—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**—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**—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_OVERIDE)
  - 5 (IP_CRITIC)

  The default is 5.

- **preferred_codec**—CODEC to use when initiating a call. Valid values are g711alaw, g711ulaw, and g729a. The default is g711ulaw.

- **dtmf_inband**—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**—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**—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-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.

- **dtmf_avt_payload**—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**—Lowest value (in milliseconds) of the retransmission timer for SIP messages. The valid value is any positive integer. The default is 500.

- **timer_t2**—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**—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**—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**—Maximum number of times an INVITE request will be retransmitted. The valid value is any positive integer. The default is 6.

- **proxy_register**—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 re-initiate 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 line*x*_authname and line*x*_password parameters (where *x* is a number 1 through 6) in the phone-specific configuration file.

- **timer_register_expires**—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**—Number to call to check voice mail. This number will be called when the **Messages** key is pressed.

- Date, Time, and Daylight Savings Time parameters:
  - **sntp_mode**—Mode in which the phone will listen for the SNTP server.
  - **sntp_server**—IP address of the SNTP server from which the phone will obtain time data.
  - **time_zone**—Time zone in which the phone is located.
  - **dst_offset**—Offset from the phone's time when DST is in effect.
  - **dst_start_month**—Month in which DST starts.

- **dst_start_day**—Day of the month on which DST begins.

- **dst_start_day_of_week**—Day of the week on which DST begins.

- **dst_start_week_of_month**—Week of month in which DST begins.

- **dst_start_time**—Time of day on which DST begins.

- **dst_stop_month**—Month in which DST ends.

- **dst_stop_day**—Day of the month on which DST ends.

- **dst_stop_day_of_week**—Day of the week on which DST ends.

- **dst_stop_week_of_month**—Week of month in which DST ends.

- **dst_stop_time**—Time of day on which DST ends.

- **dst_auto_adjust**—Whether or not DST is automatically adjusted on the phones.

- **dnd_control**—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 turned on locally via the phone's user interface.

  - **1**—The Do Not Disturb feature is on by default, but can be turned 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**—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**—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 feature 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**—Path to the TFTP subdirectory in which phone-specific configuration files are stored.

- **network_media_type**—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**—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 phone's 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.

The SIP phone-specific parameters (typically defined in the phone-specific configuration file) are as follows:

- **line*x*_name**—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.

- **line*x*_shortname**—Name or number associated with the line*x*_name as you want it to display on the phone's LCD if the line*x*_name length exceeds the allowable space in the display area. For example, if the line*x*_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 line*x*_name variable is displayed.

- **line*x*_authname**—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 line*x*_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.

- **line*x*_password**—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 line*x*_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.

- **line*x*_displayname**—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 displayed on the callee end instead. If a value is not specified for this parameter, nothing is used.

- **dnd_control**—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 locally via the phone's user interface.
  - 1—The Do Not Disturb feature is on by default, but can be turned 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.

Note For complete information about creating and modifying configuration files, see the *Cisco SIP IP Phone 7960 Administration Guide, Version 2.0.*

Configuring the Cisco SIP Proxy Server

You configure the Cisco SIP Proxy Server by defining directives in a main configuration file. The Cisco SIP Proxy Server main configuration file is sipd.conf. A default sipd.conf configuration file is copied into */usr/local/sip/conf/* when installed on Linux platforms and copied into */opt/sip/conf* on Solaris platforms. This default configuration file should be customized to your environment.

Before beginning any of the configuration tasks in this chapter, change to the directory in which the sipd.conf file is located and open the file using vi or any text editor.

Note For complete information about configuring the Cisco SIP Proxy Server, see the *Cisco SIP Proxy Server Administrator Guide*.

Similar to the Apache Server, the Cisco SIP Proxy Server directives can be grouped into major categories. The major categories of Cisco SIP Proxy Server directives are:

- Server global directives—Define the overall operation of the Cisco SIP Proxy Server.

- Host-specific directives—Define the basic configuration of the main Cisco SIP Proxy Server which will respond to requests that are not handled by a *virtual host*.

  The term virtual host refers to maintaining more than one server on a single machine, as differentiated by their hostname. For example, companies sharing a web server can have their own domains (www.company1.com and www.company2.com) and access to the web server. Virtual hosts are not supported in Cisco SIP Proxy Server Version 1.0.

- Core SIP server directives—Define the primary SIP functionality of the Cisco SIP Proxy Server; SIP message handling. If a core SIP server directive is not specified, the server will use the default.

- SIP server module directives—Define the Cisco SIP Proxy Server interfaces and additional functionality on a per module basis.

Configuring Global Directives

The server global directives are as follows:

- **ServerRoot**—Directory in which the Cisco SIP Proxy Server configuration, error, and log files reside (*bin/*, *conf/* and *logs/*). On Linux, the default directory for these subdirectories is */usr/local/sip*. On Solaris, the default directory is */opt/sip*. Do not add a forward slash (/) to the end of the directory path.

- **LockFile**—Path to the lockfile used when the Cisco SIP Proxy Server is compiled with either USE_FCNTL_SERIALIZED_ACCEPT or USE_FLOCK_SERIALIZED_ACCEPT. Typically, this directive is left at its default value. The main reason for changing it is if the logs directory is NFS mounted, since the lockfile must be stored on a local disk. The PID of the main server process is automatically appended to the filename. The default is *logs/accept.lock*.

- **PidFile**—Path and file to which the Cisco SIP Proxy Server records its process ID when it is started. If the filename does not begin with a forward slash (/), it is assumed to be relative to the ServerRoot. The default is *logs/sipd.pid*.

- **ScoreBoardFile**—Memory-mapped file in which to store internal server process information. The ScoreBoardFile is automatically created if your architecture requires it. If this file is automatically created, ensure that no two servers share the same file. The default is *logs/apache_runtime_status*.

- **prefork MPM module**—How the Cisco SIP Proxy Server child processes will operate. When configured, child processes are monitored. When necessary, additional child processes are spawned to process incoming SIP requests and responses. When the monitor determines that too few requests and responses are taking place, it tears down some of the idle child processes.

Note The maximum and minimum values for the following prefork MPM module directives are dependent on your available platform resources. Modify as required. The prefork module directives are ignored if the Cisco SIP Proxy Server has been configured to run in single-process mode.

To configure the prefork module, specify values for the following directives:

- **StartServers**—Number of child processes to create when the Cisco SIP Proxy Server starts. The default is 5.

- **MinSpareServers**—Minimum number of idle child processes (not handling requests). The default is 5.

- **MaxSpareServers**—Maximum number of idle child processes (not handling requests). Idle child processes that exceed this number are torn down. Do not set this parameter to a large number. The default is 10.

- **MaxClients**—Maximum number of simultaneous requests that can be supported; no more than this number of child processes will be created. The default is 20.

- **MaxRequestsPerChild**—Maximum number of requests that a child process can process. If this number is exceeded, the child process will be torn down. The default is 0.

- **Listen**—Whether the server should listen to more than one IP address or port; by default it responds to requests on all IP interfaces, but only on the port specified in the Port directive.

Configuring Host-Specific Directives

The server host-specific directives are as follows:

- **Port**—Port on which the Cisco SIP Proxy Server listens. The default is the well known SIP port 5060. If this directive is set to a value less than 1023, the Cisco SIP Proxy Server (sipd daemon) initially must be run as root.

- **User**—Name or number of the user the sipd process will be run as when sipd is started by the root user.

- **Group**—Name or number of the group the sipd process will be run as when sipd is started by the root user.

- **ServerName**—Hostname of the server used by clients in Request-URIs that is different than the standard name the server would recognize as its own. If this directive is not specified, the server attempts to deduce it from its IP address.

- **HostnameLookups**—Whether client DNS host names or IP addresses are logged. Valid values are on (log host names) or off (log IP addresses). The default is Off.

- **ErrorLog**—Name of the file to which the Cisco SIP Proxy Server will log debug and error messages. The default is *logs/error_log*.

- **LogLevel**—Verbosity of messages recorded in the error logs. Valid values (in order of decreasing significance) are:

  - emerg—Emergencies; system is unusable.

  - alert—Action must be taken immediately.

- crit—Critical conditions.

- error—Error conditions.

- warn—Warning conditions.

- notice—Normal but significant condition.

- Info—Informational.

- debug—debug-level messages.

The default is warn.

- **LogFormat**—Format of the default logfile named by the CustomLog directive.

- **CustomLog**—Name and location of the access log file. The default is *logs/access_log common*.

- **TransferLog**—With what frequency (in seconds) to rotate Cisco SIP Proxy Server logs without having to tear down the Cisco SIP Proxy Server (sipd daemon). To specify a value for this directive, specify the path to the log file and the rotation time.

    You can specify a value similar to `/user/local/sip/bin/rotatelogs /usr/local/sip/logs/request_log 86400` in this directive to have access records such as a REGISTER request logged to both the access_log and request_log.0974732040 (number extension is calculated and added based on the current time stamp and the specified rotation frequency). If the CustomLog directive is commented out, access records are logged to the file specified in the TransferLog directive.

Configuring Core Configuration Directives

The server core configuration directives are as follows:

- **ProxyDomain**—DNS domain of the Cisco SIP Proxy Server. The DNS domain suffix must be entered in a standard Fully Qualified Domain (FQDN) format "mydomain.com" or "company.mydomain.com." There is no default for this directive.

- **StatefulServer**—Whether the Cisco SIP Proxy Server will be a transaction stateful or transaction stateless server.

    When configured to function as a stateful server, on receiving a SIP request, the Cisco SIP Proxy Server creates a TCB in which it maintains a transaction state.

    As a stateful proxy server, from the time a SIP request is received until the final response is one transaction. Stateful proxy servers do not originate any SIP requests except for the SIP CANCEL request or an ACK for a non-200 OK final response. When configured to function as stateless proxy server, the Cisco SIP Proxy Server forwards every request downstream and every response upstream.

    As a stateful redirect server, the Cisco SIP Proxy server looks up its registry database on receiving a SIP request and returns a 302 response upstream. As a stateless redirect server, the Cisco SIP Proxy Server returns a final response on receiving any request and does not forward any response or request.

    Valid values are On and Off. The default is On.

- **SipResolveLocalContactsInRedirectMode**—Whether to return next hop routing information when the Cisco SIP Proxy Server is configured to function as a redirect server. A redirect server typically returns the contact location it knows about. However, if this directive is set to On, next hop routing will occur and the contact information may be updated before returning the SIP 3xx response. Valid values are On and Off. The default is Off.

- **ServerType**—Whether the Cisco SIP Proxy Server will function as a proxy or redirect server. As a proxy server, the Cisco SIP Proxy Server will process and route SIP requests. As a redirect server, the Cisco SIP Proxy Server will provide contact information via SIP redirect responses (3xx). Possible values are Proxy and Redirect. The default is Proxy.

- **UseCallerPreferences**—Whether to use user-defined or administrator-defined preferences when handling requests. Request handling preferences are controlled by a server administrator but can be overridden by a UAC. Preferences include decisions such as whether to proxy or redirect a request, whether to fork a request (sequential or parallel), whether to recursively search, and to which URI to proxy or redirect a request. Valid values are On (use user-defined preferences) or Off (ignore user-defined preferences). The default is On.

- **Recursive**—Whether the Cisco SIP Proxy Server will recursively try addresses returned in a SIP 3xx redirection response or use the lowest-numbered address. Valid values are On (the server will recursively try addresses) or Off (the server will use the lowest-numbered response). The default is On.

- **MaxForks**—Maximum number of branches that can be forked when the Cisco SIP Proxy Server is configured to function as a stateful server. The range is 1 to 6. The default is 5.

- **NumericUsernameInterpretation**—Lookup order for numeric user information in the Request-URI header field when the ";user=usertype" parameter is missing.

  Valid values are:

  - IP_164—Process the Request-URI entries as URLs first and then as E.164 numbers.

  - E164_IP—Process the Request-URI entries as E.164 numbers first and then as URLs.

  - IP—Process the Request-URI entries as URLs only.

  - E164—Process the Request-URI entries as E.164 numbers.

  The default is E164_IP.

- **NumericUsernameCharacterSet**—Set of characters used to determine whether the user information portion of the Request-URI is in a category of users that will be applied to the "NumericUsernameInterpretation" processing step. The default is +0123456789.-() (global phone number combinations). For more information on this directive, see the sipd.conf file.

- **SrvForFqdnOnly**—Whether to perform DNS Server (SRV) lookups only for hosts that are FQDNs. If the host portion of the Request-URI header field does not contain an IP address, but contains a period, the Cisco SIP Proxy Server determines the host to be an FQDN. Valid values are On (perform DNS SRV lookups only on FQDN hosts) or Off (perform DNS SRV lookups for any host that does not contain a target port). The default is Off.

- **SipT1InMs**—Amount of time (in milliseconds) after which a request is first retransmitted. The default is 500.

- **SipT2InMs**—Amount of time (in milliseconds) after which the backoff interval for non-INVITE requests no longer increases exponentially. The default is 4000.

- **SipT3InMs**—Amount of time (in milliseconds) the Cisco SIP Proxy Server will wait after receiving a provisional response when processing an INVITE request. The default value is 60000.

- **SipMaxT3InMs**—Maximum amount of time (in milliseconds) the Cisco SIP Proxy Server will wait after receiving a provisional response when processing an INVITE request. The default value is 180000.

- **SipT4InMs**—Amount of time (in milliseconds) that the TCB will be maintained after a final response to a SIP INVITE is proxied. The default is 32000.

- **MaxInviteRetxCount**—Maximum number of times that a SIP INVITE request can be retransmitted by the Cisco SIP Proxy Server. The range is 0 to 6. The default is 6.

- **MaxNonInviteRetxCount**—Maximum number of times that a SIP request other than an INVITE request can be retransmitted. The range is 0 to 10. The default is 10.

- **SharedMemorySize**—Shared memory size to be allocated for transaction control block (TCB). The valid range is 1,024,000 to the maximum DRAM on the machine. The default is 32 MB.

- **RegistryCleanupRate**—Interval (in milliseconds) at which the entries are deleted from the registry. The default is 180000 milliseconds.

- **AddRecordRoute**—Whether the Cisco SIP Proxy Server will add the Record-Route header field to an initial SIP INVITE message. The Record-Route header field contains a globally reachable Request-URI that identifies that proxy server. When a proxy server adds the Request_URI to the Record-Route field in SIP messages, the proxy server will be kept in the path of subsequent requests for the same call leg. Valid values are On (add the Record-Route field) and Off (do not add the Record-Route field). The default is Off. The ServerType directive must be set to Proxy for this directive to be applied.

- **Sip_Token_Port**—Port that will be used by the sychronization server on the Cisco SIP Proxy Server. This port must be identical for all servers in a farm.The default is 22794.

- **Sip_Services_Port**—Port on the sychronization server. The default is 52931.

- **Accounting**—Whether or not the SIP server will log accounting information on a RADIUS account server. Possible values are On (accounting is enabled) and Off (accounting is disabled). The default is Off.

- **AccountingRecordFormat**—Record format being used to log accounting information. The valid value is RADIUS.

- **PrimaryRadiusAcctIp**—IP address or host name of the primary RADIUS server to be used for accounting.

- **PrimaryRadiusAcctPort**—Destination port number of the primary RADIUS server to be used for accounting.

- **PrimaryRadiusAcctSecret**—Secret text string shared between the Cisco SIP Proxy Server and the primary RADIUS account server.

- **SecondaryRadiusAcctIp**—IP address or host name of the secondary RADIUS server to be used for accounting.

- **SecondaryRadiusAcctPort**—Destination port number of the secondary RADIUS server to be used for accounting.

- **SecondaryRadiusAcctSecret**—Secret text string shared between the Cisco SIP Proxy Server and the secondary RADIUS account server.

- **UseIpAddrInPathHeaders**—Whether the server will use its IP address or FQDN in the Via and Record-Route header fields. Possible values are On (use the IP address) and Off (use the FQDN). The default is On.

- **IPAddrInPathHeaders**—Which IP address will be used in the Via and Record-Route header fields when the UserIpAddrInPathHeaders field is set to On. If an address is not defined in this directive, the first value returned via gethostbyname is used.

- **IgnoreProxyRequire**—Proxy-sensitive feature that can be ignored when servicing clients.

- **SIPStatsLog**—Whether the Cisco SIP Proxy Server will print statistics to the stats_log file. The default is On.

- **SIPStatsInterval**—Interval (in seconds) at which statistics are logged. The default is 3600.

- **DebugFlag**—Whether to enable the printing of mod_sip module debug messages to *logs/error_log*. Valid values are StateMachine On (print messages) or StateMachine Off (do not print messages). The default is StateMachine Off.

Configuring SIP Module Directives

The server module directives are as follows:

- mod_sip_db_mysql

  - **DB_MySQL**—Enable or disable the interface to the MySQL database. Enabling the interface will establish a TCP connection with the database. Valid values are On (enable the interface) or Off (disable the interface). The default is Off.

  - **DB_MySQL_HostName**—Host name or IP address of the machine on which the MySQL database resides.

  - **DB_MySQL_DB**—Name of the database in which the subscriber table is stored and maintained.

  - **DB_MySQL_Username**—Login username to the database account.

  - **DB_MySQL_Password**—Login password to the database account.

  - **DB_MySQL_SubscriberTable**—Name of the table in which the subscriber entries will be stored.

  - **DB_MySQL_*XXX*_Field**—Name equivalent in an existing MySQL database subscriber table. Use these directives as necessary to map the field names being used by the Cisco SIP Proxy Server to the equivalent entry in an existing MySQL subscriber table.

> **Note** For a call to be forwarded appropriately, the following DB_MySQL_XXX_Field subscriber record fields must be populated: DEST_URL_CFNA, DEST_URL_CFUNC, DEST_URL_CFB, DEST_URL_CFUNV. These subscriber fields define the destination URL for the different call forwarding scenarios (no answer, unconditionally, busy, and unavailable). For more information, see the instructions in the sipd.conf file.

  - **DebugFlag**—Whether to enable the printing of all mod-sip-db-mysql debug messages to *logs/error_log*. Valid values are DBMySQL On (print messages) or DBMySQL Off (do not print messages). The default is DBMySQL Off.

- Number Expansion (mod_sip_numexpand)

  - **Cisco_Numexpand**—Whether to use number expansion on the Cisco SIP Proxy Server. Valid values are On (use number expansion) or Off (do not use number expansion). The default is Off.

  - **Cisco_Numexpand_DEBUG**—Whether to enable the printing of all number expansion-related debug messages. Valid values are On (print messages) or Off (do not print messages). The default is Off.

  - Define the number plan as follows:

    ```
    <NumberPlan mycompany.com>
        NumExp    2....    +1919555....
        NumExp    6....    +1408554....
        NumExp    7....    +1408553....
        NumExp    4....    +1978555....
        NumExp    3....    408556
    </NumberPlan>
    ```

- Authentication and Authorization (mod_sip_authen)

  - **Authentication**—Whether the proxy server will require users be authenticated before servicing their transactions. Valid values are On (user must be authenticated) or Off (user does not have to be authenticated). The default is Off.

  - **AuthRealm**—Realm used in authentication response headers. The default is Cisco.

  - **AuthScheme**—Type of authentication method to be used when users are required to obtain authentication before receiving service from the Cisco SIP Proxy Server. Possible values are HTTP_Digest or HTTP_CHAP. The default is HTTP_Digest.

  - **RadiusAuthSkew**—Amount of time (in seconds) that a challenge is valid. The default is 30.

  - **PrimaryRadiusAuthIp**—IP address or host name of the primary RADIUS server to be used for user authentication.

  - **PrimaryRadiusAuthPort**—Destination port number of the primary RADIUS server to be used for user authentication.

  - **PrimaryRadiusAuthSecret**—Secret text string shared between the Cisco SIP Proxy Server and the primary RADIUS authentication server.

  - **SecondaryRadiusAuthIp**—IP address or host name of the backup RADIUS server to be used for user authentication.

  - **SecondaryRadiusAuthPort**—Destination port number of the backup RADIUS server to be used for user authentication.

  - **SecondaryRadiusAuthSecret**—Secret text string shared between the Cisco SIP Proxy Server and the backup RADIUS authentication server.

- Call Forwarding Unconditional (mod_sip_call_forward)

  - **CallForwardUnconditional**—Whether to forward calls unconditionally. Possible values are On (forward calls unconditionally) or Off (do not forward calls unconditionally).

  - **CallForwardNoAnswer**—Whether to forward calls when a call is not answered. Possible values are On (forward calls when a call is not answered) or Off (do not forward calls when a call is not answered).

  - **CallForwardBusy**—Whether to forward calls when a SIP 486 Busy Here response is received. Possible values are On (forward calls) or Off (do not forward calls).

- **CallForwardUnavailable**—Whether to forward calls when a UAC is unavailable. Possible values are On (forward calls) or Off (do not forward calls).

- **CallForwardNoAnswerTimer**—Time (in milliseconds) after which to forward a call when a call goes unanswered. The default is 24000. The setting for this directive is valid only when the CallForwardNoAnswer directive is set to On.

- **CallForwardUnavailableTimer**—Time (in milliseconds) after which to forward a call when a UAC is unavailable. The default is 24000. The setting for this directive is valid only when the CallForwardUnavailable directive is enabled.

- **AddDiversionHeader**—Whether the CC-Diversion header will be included in the SIP messages. Inclusion of the CC-Diversion header enables conveying call-redirection information during a call setup phase. Possible values are On (include the CC-Diversion header) and Off (exclude the CC-Diversion header). The default is On if call forwarding is enabled.

- Registry Services (mod_sip_registry)

  - **Cisco_Registry**—Whether registry services are enabled or disabled on the Cisco SIP Proxy Server. Possible values are On (function as a registrar server) or Off (do not function as a registrar server).

  - **Cisco_Registry_Shared_Memory_Address**—Memory location of the registration table. The default is the platform address.

  - **Cisco_Registry_Rendezvous_Name**—Rendezvous name of the database containing registration information. The default is a null value.

  - **Cisco_Registry_Rendezvous_Directory**—Location of the registration database.

  - **Cisco_Registry_Remote_Update_Port**—Port number of the registration database server for all members of a farm of servers. The value for this directive must be identical for all members of the farm. The default is 22913.

  - **Cisco_Registry_Farm_Members**—Names of the Cisco SIP Proxy Servers that you wish to be members of the farm of Cisco SIP Proxy Servers. This list must be defined identically on all the Cisco SIP Proxy Servers identified as part of a farm.

  - **Cisco_Registry_Max_DB_Age_on_Boot**—Maximum age (in seconds) of the database backing store file when starting. If the age of the database backing store file exceeds this age, the file will be deleted. The default is 86400. The value specified in this directive must be greater than that specified in the RegistryCleanupRate core directive.

  - **DebugFlag**—Whether to enable the printing of mod_sip_registry module debug messages to *logs/error_log*. Valid values are Registry On (print messages) or Registry Off (do not print messages). The default is Registry Off.

  - Define the static registry contact entries as follows:

```
<StaticRegistry 10.1>
Static_Registry_User_Type           IP
Static_Registry_User                jdoe
Static_Registry_Contact             0015155551212@mycompany.com
Static_Registry_Contact_User_Type   PHONE
Static_Registry_ContactPort         5060
Static_Registry_TransportProtocol   UDP
Static_Registry_ContactAge          Permanent
Static_Registry_Delete_or_Add       ADD
</StaticRegistry>
```

- E.164 to Request-URI Address Translation (mod_sip_enum)

    - **Cisco_Enum**—Whether E.164 to Request-URI translation is enabled. Possible values are On (translate) or Off (do not translate). The default is On.

    - **Cisco_Enum_Domain**—Private search domain for a private ENUM number plan. If a Request-URI user begins with the plus (+) character, this directive is not used because the plus character indicates that the number is part of a global ENUM number plan, which is e164.arpa.

    - **Cisco_Enum_Global_Domain**—Domain to use when the Request-URI user begins with a plus (+) character (indicating a global domain) or to use when a value is not specified for the Cisco_Enum_Domain directive. The default is to use e164.arpa.

    - **DebugFlag**—Whether to enable the printing of mod_sip_enum API debug messages to *logs/error_log*. Valid values are Enum On (print messages) or Enum Off (do not print messages). The default is Enum Off.

- GKTMP Interface (mod_sip_gktmp)

    - **GktmpConnection**—Whether the GKTMP interface is enabled or disabled. Possible values are On (interface is enabled) or Off (interface is disabled). The default is Off.

    - **MasterServerHostname**—Hostname of the primary NAM server.

    - **MasterServerIpAddress**—IP address of the primary NAM server.

    - **MasterServerPort**—Destination port number of the primary NAM server to be used for 800/900 and LNP lookup services.

    - **SecondaryServerHostname**—Hostname of the secondary NAM server.

    - **SecondaryServerIpAddress**—IP address of the secondary NAM server.

    - **SecondaryServerPort**—Destination port number of the secondary NAM server.

    - **Debug Flag**—Whether to enable the printing of mod_sip_gktmp module debug messages to *logs/error_log*. Valid values are Gktmp On (print messages) or Gktmp Off (do not print messages). The default is Gktmp Off.

    - **DebugFlag**—Whether to enable the printing of mod_sip_gktmp API debug messages to *logs/error_log*. Valid values are Gktmp API On (print messages) or GktmpAPI Off (do not print messages). The default is GktmpAPI Off.

- Next Hop Routing (mod_sip_routing)

    - **Cisco_Routing**—Whether next hop routing is enabled or disabled on the Cisco SIP Proxy Server. Possible values are On (next hop routing is enabled) or Off (next hop routing is disabled). The default is On.

    - **Cisco_Routing_Shared_Memory_Address**—Memory location of the routing table. If the value of this directive is a null value, the default address of the platform will be used.

    - **Cisco_Routing_Rendezvous_Name**—Rendezvous name of the database containing routing information. The default is a null value.

    - **Cisco_Routing_Rendezvous_Directory**—Location of the routing database.

    - **Cisco_Routing_Remote_Update_Port**—Port number of the routing database server for all members of a farm of servers. The value for this directive must be identical for all members of the farm. The default is 22913.

    - **Cisco_Routing_Use_Domain_Routing**—Whether to use domain next hop routing. Domain next hop routing uses the host portion of the Request-URI as the key in obtaining the next hop or hops for a request. Valid values are On (use domain routing) or Off (do not use domain routing). The default is Off.

- **Cisco_Routing_Max_DB_Age_on_Boot**—Maximum age (in seconds) of the database backing store file when starting. If the age of the database backing store file exceeds this age, the file will be deleted. The default is 0.

- **DebugFlag**—Whether to enable the printing of all mod-sip-routing module debug messages to *logs/error_log*. Valid values are Routing On (print messages) or Routing Off (do not print messages). The default is Routing Off.

- Define the static route entries as follows:

```
<StaticRoute 1>
Static_Route_Destination Pattern        001555666....
Static_Route_Type                       PHONE
Static_Route_NextHop                    sip_gw1.mycompany.com
Static_Route_NextHopPort                5060
Static_Route_TransportProtocol          UDP
Static_Route_Priority                   0
Static_Route_Delete_or_Add              Add
</StaticRoute>
```

- Number Services (sip_numserv)

  - **Cisco_Number_Services**—Whether or not numbering services is enabled or disabled on the Cisco SIP Proxy Server. Possible values are On (enabled) or Off (disabled).

  - **Cisco_Number_Services_Shared_Memory_Address**—Memory location of the number services table. The default is the platform address.

  - **Cisco_Number_Services_Rendezvous_Name**—Rendezvous name of the number services database. The default is numserv_db.

  - **Cisco_Number_Services_Rendezvous_Directory**—Location of the number services database.

  - **Cisco_Number_Services_Remote_Update_Port**—TCP port number of the number services for all members of a farm of servers. The value for this directive must be identical for all members of the farm. The default is 22913.

  - **Cisco_Number_Services_Max_DB_Age_on_Boot**—Maximum age (in seconds) of the database backing store file when starting. If the age of the database backing store file exceeds this age, the file will be deleted. The default is 0.

  - **DebugFlag**—Whether to enable the printing of all mod_sip_numserv module debug messages to *logs/error_log*. Valid values are Numserv On (print messages) or Numserv Off (do not print messages). The default is Numserv Off.

  - Define the static number service entries as follows:

```
<Number_Services 1>
Number_Services_Contact                         911
Number_Services_Priority                        EMERGENCY
<Number_Services_Route 10>
Static_Number_Services_Route_Target             proxyserver@company.com
Static_Number_Services_Route_OriginationPattern 515555
Static_Number_Services_TransportPortocol        UDP
Static_Number_Services_ContactPort              5060
</Number_Services_Route>
</Number_Services>
```

Note   For complete information about creating and modifying the sipd.conf file, see the *Cisco SIP Proxy Server Administration Guide*.

Configuring the Cisco uOne Messaging System

There are multiple components that make up the uOne Messaging System. Configuration of the system requires configuration of each of its components.

When implementing the uOne SIP system, be aware of the following:

- A uOne SIP system supports the following payloads:
  - G.711 mu-law
  - G.729
  - Dynamic AVT tones payload: 97—127
  - Cisco RTP DTMF relay payload: 121

- A uOne SIP system does not support CODEC switching within a call.

- The uOne SIP system does not support Single Number Reach (SNR) services.

- The SIP uOne implementation supports Netscape messaging and directory servers for Internet Message Access Protocol (IMAP) / Lightweight Directory Access Protocol (LDAP) servers.

Note For complete information about configuring the Cisco uOne Messaging System, see the *uOne BackEnd Servers Reference Manual, Release 4.2(2)s*, the *uOne Gateserver Installation and Configuration Manual, Release 4.2(2)s*, and the *Installing and Configuring uOne 4.2(2)s, SIP Edition* document.

To configure the uOne system, perform the following tasks:

	Task	References
Step 1	Run the Quick Config tool to perform the initial uOne configuration tasks on the gateserver: • Configure the uOne system for calls • Setup the uOne Subscriber Administration tool • Setup the uOne Manager and/or the uOne database	*Installing and Configuring uOne 4.2(2)s, SIP Edition* *uOne Gateserver Installation and Configuration Manual, Release 4.2(2)s*
Step 2	Make any configuration changes on the gateserver necessary for your operating environment.	*Installing and Configuring uOne 4.2(2)s, SIP Edition* *SIP Compliance and Call Flows for uOne 4.2(2)s* *uOne Gateserver Installation and Configuration Manual, Release 4.2(2)s* *uOne Administration Manual, Release 4.2(2)s*

	Task	References
Step 3	Configure the directory server for uOne.	*uOne Back End Servers Reference Manual, Release 4.2(2)s*
Step 4	Configure the messaging server for uOne.	
Step 5	Configure the paging server for uOne.	
Step 6	If desired, set up communities of interest.	*uOne Administration Manual, Release 4.2(2)s*
		uOne Back End Servers Reference Manual, Release 4.2(2)s
Step 7	Set up classes of service.	
Step 8	Provision subscribers.	
Step 9	Create broadcast lists	
Step 10	If necessary, set up additional greeting and/or fax administrators.	

Configuring the Cisco Secure PIX Firewall

To configure the Cisco Secure PIX Firewall, perform the following tasks:

	Task	References
Step 1	Obtain a console terminal, download the most current software, and configure network routing.	*Configuration Guide for the Cisco Secure PIX Firewall Version 6.0*
Step 2	Start the PIX Firewall configuration mode.	
Step 3	Identify each interface.	
Step 4	Create a default route outside.	
Step 5	Permit ping access.	
Step 6	Store image in Flash memory and reboot.	

In addition, perform the following tasks:

- Enable the SIP protocol on the appropriate interface or interfaces (via the **fixup protocol sip 5060** command)

- If necessary, customize the SIP inactivity timer (via the **timeout sip** *hh:mm:ss* command) and the SIP media timer used for SIP RTP/RTCP with SIP UDP media packets instead of the UDP inactivity timeout (via the **timeout sip_media** *hh:mm:ss* command).

- Create a list of "allowed" external devices for all outside devices you wish to be able to call inside the firewall (outside callers cannot make calls to inside the firewall unless they have been defined as an allowed device).

Configuring the Cisco SS7 Interconnect for VoIP Gateways Solution

There are numerous components that make up the Cisco SS7 Interconnect for VoIP Gateways Solution. The configuration tasks for each component in the solution are briefly described in the following sections:

- Configuring the Signaling Controller, page 4-22
- Configuring the Cisco AS5300 Universal Access Server, page 4-26

> **Note**   For complete information about configuring the Cisco SS7 Interconnect for VoIP Gateways Solution, see the *Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide*, the *Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Provisioning Guide*, and the *Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Media Gateway Guide*.

Configuring the Signaling Controller

Configuring the signaling controller software consists of three tasks:

- Configuring the Signaling Controller
- Configuring the Cisco SLT
- Configuring the LAN Switch (Optional)

> **Caution**   Always use the Cisco signaling controller CMM tool or MML commands to create, modify, manage, and deploy your configuration files on the signaling controller. We do not recommend modifying the configuration files directly on the signaling controller.

Configuring the Signaling Controller

To configure the signaling controller, perform the following tasks:

	Task	Reference
Step 1	Prepare the following: • Bearer routes to other switches • Signaling point links (the connection between an MGC and a SIP server) • Network access server control links • Trunks, trunk groups, and routes (for incoming SIP calls) • Dial plans	*Cisco Media Gateway Controller Software Release 9 Provisioning Guide* *Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide*
Step 2	Configure the SS7 signaling routes to external switches by completing the following tasks: • Add the OPC in your network. • Add the DPC to identify the destination switch. • Add the APCs to identify the STPs with which the signaling controller communicates signaling information. • Add linksets to connect the Cisco SLTs to the STPs. • Add the SS7 subsystem to identify the mated STPs. • Add the SS7 routes for each signaling path from the signaling controller to the destination switch. • Add the SS7 signaling service from the signaling controller to the destination switch.	*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Provisioning Guide*

	Task	Reference
Step 3	Provision the signaling links by completing the following tasks: • Add the Ethernet adapters (cards) in the SC host that carry signaling to and from the Cisco SLTs. • Add Ethernet interfaces for the cards in the host. • Add C7 IP links for each SS7 link from the signaling controller to the SS7network (through the Cisco SLT).	*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Provisioning Guide*
Step 4	Configure the access gateway control links by completing the following tasks: • Add external nodes for the access gateways in your network. • Add NAS signaling services for each access gateway. • Add IP links for each access gateway to each Ethernet card in the SC host.	*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Provisioning Guide*
Step 5	Configure trunks, trunk groups, and routes.	*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Provisioning Guide*
Step 6	Provision black and white trunk screening.	
Step 7	Build and deploy the configuration.	

Configuring the Cisco SLT

To configure the Cisco SLTs, perform the following tasks:

	Task	Reference
Step 1	Identify the serial WAN interface card on your Cisco SLT and connect cable to card.	*Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide*
Step 1	Install the Cisco SLT image software.	
Step 2	Configure the basic parameters and SS7 links for the Cisco SLT.	
Step 3	Configure Session Manager and RUDP.	
Step 4	Save the new configuration as the startup configuration, and then reload the Cisco SLT.	

Configuring the LAN Switch (Optional)

This section describes the task of configuring LAN switches (Cisco Catalyst Switch family) for your solution. The LAN switch connects the SC hosts to the access gateways or the Cisco SLTs. The LAN switch is used in the SC node to extend VLANs across platforms through backbone Fast Ethernet, Gigabit, or ATM connections, when necessary. The LAN switch is not provided with the SC host.

To configure the LAN switch, complete the following tasks:

	Task	Reference
Step 1	Make sure that you have virtual LAN assignments and IP address assignments for solution devices.	*Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide*
Step 2	Configure basic system information.	
Step 3	Configure the logical interface.	
Step 4	Configure SNMP information.	
Step 5	Configure the virtual LANs (VLANs).	
Step 6	Configure module and port parameters.	
Step 7	Configure spanning-tree parameters.	
Step 8	Configure the standby ports.	
Step 9	Configure the ISL connections between switches.	
Step 10	Configure the Switch Port Analyzer.	
Step 11	Configure the Route Switch Module.	

Configuring the Cisco AS5300 Universal Access Server

The Cisco AS5300 Universal Access Server is a required Cisco SIP Gateway when implementing the VoIP Infrastructure Solution for SIP with the Cisco SS7 Interconnect for Voice Gateways Solution.

In addition to the configuration prerequisites described in the "Configuring the Routers" section on page 4-1, for each AS5300 access server installed in your solution that will connect to the Cisco SS7 Interconnect for Voice Gateway Solution, configure the access gateway by performing the following tasks:

	Task	Reference
Step 1	Configure the switch type to NI2, using the **isdn switch-type primary-ni** command. (This command enables the connection between the access gateway and the virtual switch controller.)	*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Media Gateway Guide*
Step 2	Configure the access server for channelized T1 or E1 lines.	
Step 3	Enable POTS and VoIP dial peers.	
Step 4	Enable VoIP functionality.	"Configuring VoIP Support" section on page 4-2.
Step 5	Configure the SIP support on the gateway.	"Configuring the Cisco SIP Gateway" section on page 4-2.

Configuration Example

Figure 4-1 illustrates an example of a simple implementation of the Cisco VoIP Infrastructure Solution for SIP. The example configurations in this section pertain to this illustration.

Figure 4-1   Simple Implementation Example
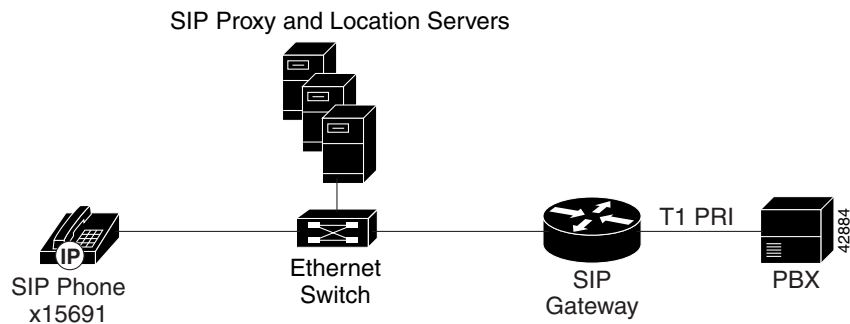
Example Cisco SIP Gateway Configuration

To configure the Cisco router or access server as a VoIP SIP gateway as shown in Figure 4-1, we must perform the following tasks:

Task	Command
Configure the serial interface used for voice data and enter interface configuration mode.	**interface serial** *slot*/*port*
Specify the central office switch type on the ISDN interface.	**isdn switch-type** *switch_type*

Task	Command
Specify how incoming voice calls are to be handled.	For the Cisco 2600 and 3600: **isdn incoming-voice voice** For the Cisco AS5300: **isdn incoming-voice modem** [**56** | **64**]
Exit interface configuration mode.	**exit**
Configure the parameters of the T1 or E1 line that is connected to the PBX and enter controller configuration mode.	**controller** {**t1** | **e1**} *slot*/*port*
Select the frame type for the T1 or E1 data line.	For a T1 line: **framing** {**sf** | **esf**} For an E1 line: **framing** {**crc4** | **no-crc4**}
Configure the line coding for T1 lines.	**linecoding** { **b8zs** | **ami** }
Configure the ISDN PRI.	**pri-group timeslots** *range*
Exit controller configuration mode.	**exit**
Configure the VoIP dial-peers, which are used to handle outgoing calls from the gateway, and enter dial-peer configuration mode.	**dial-peer voice** *number* **voip**
Enable the session application. This is required for call-transfer.	**application session**
Specify the range of destination numbers that this dial peer will handle.	**destination-pattern** *string*
Specify that the dial-peer is to use SIP for all call signaling.	**session protocol sipv2**
Specify that all outbound calls are to be routed to the SIP proxy.	**session target sip-server**
Specify the codec to be used for outbound calls. This information is included in the SDP body of the INVITE.	**codec** {**g711alaw** | **g711ulaw** | **g723r63** | **g726r16** | **g728** | **g729r8**}
Exit VoIP dial-peer configuration mode.	**exit**
Configure the POTS dial-peers, which are used to handle incoming calls to the gateway, and enter dial-peer configuration mode.	**dial-peer voice** *number* **pots**
Enable the session application. This is required for call-transfer.	**application session**
Specify the range of destination numbers that this dial peer will handle.	**destination-pattern** *string*
Specify that direct inward dialing is to be used (there is no secondary dial tone).	**direct-inward-dial**
Specify that all calls that match the destination pattern should be routed to the specified voice port.	**port** *slot*/*port*:*ds0-group-no*

Task	Command
Specify how incoming voice calls are to be handled.	For the Cisco 2600 and 3600: **isdn incoming-voice voice** For the Cisco AS5300: **isdn incoming-voice modem** [**56** | **64**]
Exit interface configuration mode.	**exit**
Configure the parameters of the T1 or E1 line that is connected to the PBX and enter controller configuration mode.	**controller** {**t1** | **e1**} *slot*/*port*
Select the frame type for the T1 or E1 data line.	For a T1 line: **framing** {**sf** | **esf**} For an E1 line: **framing** {**crc4** | **no-crc4**}
Configure the line coding for T1 lines.	**linecoding** { **b8zs** | **ami** }
Configure the ISDN PRI.	**pri-group timeslots** *range*
Exit controller configuration mode.	**exit**
Configure the VoIP dial-peers, which are used to handle outgoing calls from the gateway, and enter dial-peer configuration mode.	**dial-peer voice** *number* **voip**
Enable the session application. This is required for call-transfer.	**application session**
Specify the range of destination numbers that this dial peer will handle.	**destination-pattern** *string*
Specify that the dial-peer is to use SIP for all call signaling.	**session protocol sipv2**
Specify that all outbound calls are to be routed to the SIP proxy.	**session target sip-server**
Specify the codec to be used for outbound calls. This information is included in the SDP body of the INVITE.	**codec** {**g711alaw** | **g711ulaw** | **g723r63** | **g726r16** | **g728** | **g729r8**}
Exit VoIP dial-peer configuration mode.	**exit**
Configure the POTS dial-peers, which are used to handle incoming calls to the gateway, and enter dial-peer configuration mode.	**dial-peer voice** *number* **pots**
Enable the session application. This is required for call-transfer.	**application session**
Specify the range of destination numbers that this dial peer will handle.	**destination-pattern** *string*
Specify that direct inward dialing is to be used (there is no secondary dial tone).	**direct-inward-dial**
Specify that all calls that match the destination pattern should be routed to the specified voice port.	**port** *slot*/*port*:*ds0-group-no*

Task	Command
Specify how incoming voice calls are to be handled.	For the Cisco 2600 and 3600: **isdn incoming-voice voice** For the Cisco AS5300: **isdn incoming-voice modem** [**56**	**64**]
Exit interface configuration mode.	**exit**
Configure the parameters of the T1 or E1 line that is connected to the PBX and enter controller configuration mode.	**controller** {**t1**	**e1**} *slot*/*port*
Select the frame type for the T1 or E1 data line.	For a T1 line: **framing** {**sf**	**esf**} For an E1 line: **framing** {**crc4**	**no-crc4**}
Configure the line coding for T1 lines.	**linecoding** { **b8zs**	**ami** }
Configure the ISDN PRI.	**pri-group timeslots** *range*
Exit controller configuration mode.	**exit**
Configure the VoIP dial-peers, which are used to handle outgoing calls from the gateway, and enter dial-peer configuration mode.	**dial-peer voice** *number* **voip**
Enable the session application. This is required for call-transfer.	**application session**
Specify the range of destination numbers that this dial peer will handle.	**destination-pattern** *string*
Specify that the dial-peer is to use SIP for all call signaling.	**session protocol sipv2**
Specify that all outbound calls are to be routed to the SIP proxy.	**session target sip-server**
Specify the codec to be used for outbound calls. This information is included in the SDP body of the INVITE.	**codec** {**g711alaw**	**g711ulaw**	**g723r63**	**g726r16**	**g728**	**g729r8**}
Exit VoIP dial-peer configuration mode.	**exit**
Configure the POTS dial-peers, which are used to handle incoming calls to the gateway, and enter dial-peer configuration mode.	**dial-peer voice** *number* **pots**
Enable the session application. This is required for call-transfer.	**application session**
Specify the range of destination numbers that this dial peer will handle.	**destination-pattern** *string*
Specify that direct inward dialing is to be used (there is no secondary dial tone).	**direct-inward-dial**
Specify that all calls that match the destination pattern should be routed to the specified voice port.	**port** *slot*/*port*:*ds0-group-no*

Task	Command
Specify how incoming voice calls are to be handled.	For the Cisco 2600 and 3600: **isdn incoming-voice voice** For the Cisco AS5300: **isdn incoming-voice modem** [**56** | **64**]
Exit interface configuration mode.	**exit**
Configure the parameters of the T1 or E1 line that is connected to the PBX and enter controller configuration mode.	**controller** {**t1** | **e1**} *slot*/*port*
Select the frame type for the T1 or E1 data line.	For a T1 line: **framing** {**sf** | **esf**} For an E1 line: **framing** {**crc4** | **no-crc4**}
Configure the line coding for T1 lines.	**linecoding** { **b8zs** | **ami** }
Configure the ISDN PRI.	**pri-group timeslots** *range*
Exit controller configuration mode.	**exit**
Configure the VoIP dial-peers, which are used to handle outgoing calls from the gateway, and enter dial-peer configuration mode.	**dial-peer voice** *number* **voip**
Enable the session application. This is required for call-transfer.	**application session**
Specify the range of destination numbers that this dial peer will handle.	**destination-pattern** *string*
Specify that the dial-peer is to use SIP for all call signaling.	**session protocol sipv2**
Specify that all outbound calls are to be routed to the SIP proxy.	**session target sip-server**
Specify the codec to be used for outbound calls. This information is included in the SDP body of the INVITE.	**codec** {**g711alaw** | **g711ulaw** | **g723r63** | **g726r16** | **g728** | **g729r8**}
Exit VoIP dial-peer configuration mode.	**exit**
Configure the POTS dial-peers, which are used to handle incoming calls to the gateway, and enter dial-peer configuration mode.	**dial-peer voice** *number* **pots**
Enable the session application. This is required for call-transfer.	**application session**
Specify the range of destination numbers that this dial peer will handle.	**destination-pattern** *string*
Specify that direct inward dialing is to be used (there is no secondary dial tone).	**direct-inward-dial**
Specify that all calls that match the destination pattern should be routed to the specified voice port.	**port** *slot*/*port*:*ds0-group-no*

Task	Command
Specify the prefix of the dialed digits for this dial peer.	**prefix** *string*
Exit POTS dial-peer configuration mode.	**exit**
Specify the digits to use to expand an extension number into a destination pattern.	**num-exp** *extension-number expanded-number*
Enable SIP on the router and enter SIP user agent configuration mode.	**sip-ua**
Specify the retry values for SIP messages.	**retry** {**invite** *number* | **response** *number* | **bye** *number* | **cancel** *number*}
Specify the network address (IP address or host name) of the SIP proxy or redirect server.	**sip-server** { **dns**:[*host-name*] | **ipv4**:*ipaddr*[:*port-num*] }
Exit the SIP user-agent configuration mode.	**exit**

Example 4-1 shows the resulting configuration of a Cisco router as a SIP gateway for the Cisco VoIP Infrastructure Solution for SIP.

Example 4-1   Cisco SIP Gateway Running Configuration

```
router-sip-gw#show running
Building configuration...

Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rtp-sip-gw
!
enable secret 5 $1$JipI$QyBzbLd44Y4k6yXqND3iR.
!
!
!
!
!
voice-card 1
!
ip subnet-zero
ip domain-name cisco.com
ip name-server 161.44.11.21
!
isdn switch-type primary-5ess
isdn alert-end-to-end
!
!
!
!
!
!
!
controller T1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
```

```
!
controller T1 1/1
!
!
!
interface FastEthernet0/0
 ip address 172.17.207.91 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 no ip mroute-cache
 shutdown
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
!
interface Serial1/0:23
 no ip address
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 no cdp enable
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.17.207.1
no ip http server
ip pim ssm
!
!
voice-port 1/0:23
!
dial-peer voice 15690 voip
 application session
 destination-pattern 1569.
 session protocol sipv2
 session target sip-server
 codec g711ulaw
!
dial-peer voice 20000 pots
 application session
 destination-pattern 919392....
 direct-inward-dial
 port 1/0:23
 prefix 919392
!
dial-peer voice 30000 pots
 application session
 destination-pattern 408853....
 direct-inward-dial
 port 1/0:23
 prefix 408853
!
dial-peer voice 40000 pots
 application session
```

```
 destination-pattern 978244....
 direct-inward-dial
 port 1/0:23
 prefix 978244
!
dial-peer voice 50000 pots
 application session
 destination-pattern 408525....
 direct-inward-dial
 port 1/0:23
 prefix 408525
!
dial-peer voice 60000 pots
 application session
 destination-pattern 408526....
 direct-inward-dial
 port 1/0:23
 prefix 408526
!
dial-peer voice 70000 pots
 application session
 destination-pattern 408527....
 direct-inward-dial
 port 1/0:23
 prefix 408527
!
dial-peer voice 9 pots
 application session
 destination-pattern 9.......
 no digit-strip
 direct-inward-dial
 port 1/0:23
!
dial-peer voice 10 pots
 application session
 destination-pattern 91..........
 no digit-strip
 direct-inward-dial
 port 1/0:23
!
num-exp 991569. 1569.
num-exp 2.... 919392....
num-exp 3.... 408853....
num-exp 4.... 978244....
num-exp 5.... 408525....
num-exp 6.... 408526....
num-exp 7.... 408527....
sip-ua
retry invite 4
retry response 3
retry bye 2
retry cancel 2
sip-server ipv4:172.18.192.232
!
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password sip
 login
!
end
```

Example Cisco SIP IP Phone Configuration Files

To configure the Cisco SIP IP phone as shown in Figure 4-1, we created the default configuration file show in Example 4-2 and the phone-specific phone file shown in Example 4-3.

Example 4-2   Example Cisco SIP IP Phone Default Configuration File

```
# SIP Default Configuration File

# Proxy Server Address
proxy1_address : 172.18.192.232

# Image Version
image_version : P0S3Z313
```

Example 4-3   Example Cisco SIP IP Phone-Specific Configuration File

```
# SIP Configuration File - 003094C25D66

# Proxy Register (0-disable, 1-enable)
proxy_register : 1 ;

# Preferred Codec (g711ulaw, g711alaw, g729)
preferred_codec : g711ulaw ;

# Line 1 Name
line1_name :15691;

# Line 1 Authentication Name
line1_authname: ;

# Line 1 Password
line1_password: ;
```

CHAPTER

5

Managing and Troubleshooting the Cisco VoIP Infrastructure Solution for SIP

This chapter describes tools that you can use to manage and troubleshoot the Cisco VoIP Infrastructure Solution for SIP. It also includes tips for problem isolation and suggested actions for resolution. It includes the following sections:

- Using CVM 2.0 to Manage the Cisco VoIP Infrastructure Solution for SIP, page 5-1
- Troubleshooting the Cisco VoIP Infrastructure Solution for SIP, page 5-3

Using CVM 2.0 to Manage the Cisco VoIP Infrastructure Solution for SIP

Ciscoworks2000 Voice Manager (CVM) is a client-server, web-based voice management solution used by network administrators to configure and manage voice ports and create and modify dial plans on voice-enabled Cisco routers. Using CVM, network administrators can:

- Manage the configuration of FXO, FXS, E&M, and ISDN voice interfaces on voice-enabled routers
- Create and manage local (POTS) dial plans on voice-enabled routers
- Generate detailed reports using Telemate.net Quickview

> **Note** CVM is not a device configuration tool. Devices supported by CVM must first be configured through the CLI and have Simple Network Management Protocol (SNMP) enabled before they can be managed by CVM. You can then use CVM to modify the configuration of voice ports and create and manage local and network dial plans.

> **Note** For complete information about using CVM to manage your SIP VoIP infrastructure, see the *CiscoWorks2000 Voice Manager 2.0* documentation.

Prerequisites

The CVM Server requires the following:

Note   System requirements for the server are based on software requirements and a call volume of 96,000 calls per hour. The call volume is based on an estimated 20 calls per DS0 channel, 3 minutes holding time, and 60 busy minutes.

- 256 MB of memory
- CPU running at 450 MHz
- 8 GB of available hard disk space
- Windows NT 4.0 with Service Pack 5
- CiscoWorks2000 CD One

The CVM Client requires the following:

- 64 MB of memory
- CPU running at 300 MHz
- One of the following:
  - Windows 95 running Netscape 4.04 or Internet Explorer 4.01 and 64 MB of virtual memory
  - Windows NT running Netscape 4.04 or Internet Explorer 4.01 and 64 MB of virtual memory
  - Solaris running Netscape 4.04 with Telnet and Java enabled and 64 MB of virtual memory
- Display settings of:
  - 1024 x 768 resolution
  - 16-bit color palette

Before you can use CVM to manage your voice network, for each router that you are going to add to CVM:

- You must have network access to the router.
- You must know the IP address of the router.
- You must know all the passwords for the router.
- You must know the SNMP read community string for the router.
- Telnet must be enabled on the router. Because Telnet is used by CVM to communicate with a router, session timeout should be configured to a non-zero value for all tty lines.
- SNMP must be enabled on the router.

Note   For detailed information about using CVM to manage your SIP VoIP infrastructure, see the *CiscoWorks2000 Voice Manager 2.0* documentation.

Troubleshooting the Cisco VoIP Infrastructure Solution for SIP

This section provides procedural and reference information that you can use to determine and resolve problems you might experience while using the SIP components of the Cisco VoIP Infrastructure Solution for SIP.

This section contains the following information:

- Troubleshooting the Cisco SIP IP Phone 7960, page 5-3
- Troubleshooting the Cisco SIP Gateway, page 5-8
- Troubleshooting the Cisco SIP Proxy Server, page 5-21

Note For troubleshooting information on the other components of the Cisco VoIP Infrastructure Solution for SIP (Cisco uOne Messaging System, Cisco Secure PIX Firewall, and the SS7 Interconnect for VoIP Gateways Solution, see the documentation for those products.

Troubleshooting the Cisco SIP IP Phone 7960

This section describes troubleshooting features and tips for the Cisco SIP IP phone 7960.

Troubleshooting Features

The following is a list of features on the Cisco SIP IP phone that you can use to troubleshoot phone:

- Settings button to Network Configuration soft key—Use to view or modify the network configuration of the phone.
- Settings button to SIP Configuration soft key—Use to view or modify a phone's SIP settings.
- Settings button to Status—Display configuration or initialization errors.
- Call Messages on LED screen—Display basic SIP message flows.
- Pressing "i" key twice during a call—Displays real-time transferring and receiving call statistics. This option is recommended for trouble-shooting voice-quality issues.

In addition to the features listed above, the RS-232 port located on the back of the Cisco SIP IP phone 7960 is a console port and can be used to gather debug information.

The RS-232 port is password-protected and requires a custom RJ-11-to-RJ-45 cable.

Note For a PC connection, the RJ-45 connection needs a DB-9 female DTE adapter or an RJ-45 crossover cable for an octal async connection. The password "cisco" must be entered to enable any output to be seen via the RS-232 port. The connection baud rate, parity, start bits, and stop bits are 9600, N, 8, and 1.

To use the console port, use a RJ-11-to-RJ-45 custom cable to connect the RS-232 port to a PC.

Table 5-1 lists the RJ-11-to-RJ-45 cable pinouts.

Table 5-1   Pinouts

RJ-11 or RJ-12	RJ-45
2	6
3	4
4	3

To connect the console port, complete the following tasks:

Step 1   Insert the RJ-11 end of the rolled cable into the RS-232 port on the back of the phone.

Step 2   Use an RJ-45-to-DB-9 female DTE adapter (labeled "TERMINAL") to connect the console port to a PC running terminal emulation software.

Step 3   Insert the RJ-45 end of the rollover cable into the DTE adapter.

Step 4   From the console terminal, start the terminal emulation program.

Step 5   Type "cisco". A prompt will be displayed.

At the prompt, you can issue the following commands to assist you in troubleshooting and debugging the phone:

- **debug error**—Displays error messages that are occurring in the call flow process.
- **debug sip-message**—Enables you to view a text display of a call flow.

Troubleshooting Tips

This section provides tips for resolving the following Cisco SIP IP phone problems:

- Phone is Unprovisioned or is Unable to Obtain an IP Address, page 5-5
- Cisco SIP IP Phone will not Register with the SIP Proxy/Registrar Server, page 5-5
- Outbound Calls Cannot be Placed from a Cisco SIP IP Phone, page 5-6
- Inbound Calls Cannot be Received on a Cisco SIP IP Phone, page 5-6
- Poor Voice Quality on the Cisco SIP IP Phone, page 5-6
- DTMF Digits Do Not Function Properly, page 5-7
- Cisco SIP IP Phones do not Work When Plugged into a Line-Powered Switch, page 5-7
- Call Transfer Does Not Work Correctly, page 5-7
- Some SIP Messages are Retransmitted Too Often, page 5-7

Phone is Unprovisioned or is Unable to Obtain an IP Address

To determine why a phone is unprovisioned or unable to obtain an IP address, perform the following tasks as necessary:

- If using TFTP to download configuration files, verify that the SIPDefault.cnf and the phone-specific configuration (SIP*mac*.cnf where *mac* is the MAC address of the phone) files exist and are configured correctly.

- Verify that the TFTP server is working properly.

- Verify that the Cisco SIP IP phone Network Configuration parameters are properly configured and the phone is obtaining the proper IP addressing information (IP address, subnet mask, default gateway, TFTP server, etc.).

- Press the settings button, select **Status**, and then **Status Messages** to view messages for missing files or other errors.

- If the DHCP server is on a different IP subnet mask than the Cisco SIP IP phone, verify that "ip helper-address" address is enabled on the local router.

- Verify that the Cisco SIP IP phone software image (P0S3*xxyy*.bin where *xx* is the version number and *yy* is the subversion number) was downloaded from CCO using binary format.

Cisco SIP IP Phone will not Register with the SIP Proxy/Registrar Server

To determine why a phone will not register with a SIP proxy/registrar server, perform the following tasks as necessary:

Note   The character "x" displayed to the right of a line icon indicates that registration has failed.

- Verify that phone registration with a proxy server is enabled (via the **proxy_register** parameter in the configuration files). By default, registration during initialization is disabled.

- Verify that the IP address (**proxy1_address** parameter) of the primary SIP proxy server to be used by the phones is valid.

- If a Fully Qualified Domain Name (FQDN) is specified in the **proxy1_address** parameter, verify that the DNS server is configured to resolve the FQDN as a DNS A-record type.

- Verify whether the Cisco SIP Proxy Server has been configured to require authentication. If so, ensure that an authentication name and password has been defined in the Cisco SIP IP phone phone-specific configuration file (via the **linex_authname** and **linex_password** parameters).

- The Cisco SIP IP phone currently supports the HTTP Digest authentication method. Verify that the authentication method required by the Cisco SIP Proxy Server (via the **AuthScheme** directive in the sipd.conf file) is HTTP Digest.

- Verify that a registration request hasn't expired. By default, Cisco SIP IP phones will re-register every 3600 sections but this value can be modified via the **time_reqister_expires** parameter.

Outbound Calls Cannot be Placed from a Cisco SIP IP Phone

If a call cannot be placed from a Cisco SIP IP phone, perform the following tasks as necessary:

- Verify that the Cisco SIP IP phone Network Configuration IP address parameters have been correctly entered or received from a DHCP server.

- Verify that the Cisco SIP Proxy Server used by the phone is working properly.

- Verify that the remote SIP device is available.

- Verify that a dial plan has been defined via the dialplan.xml file and if so, that the configuration is correct. This file should have been downloaded from CCO to the root directory of your TFTP server.

- Determine the error tones that are being received and map those tones to the messages displayed on the phone's LCD (SIP 4xx messages, etc.)

- Verify that the Cisco SIP Proxy Server is correctly configured for routes or registrations to the remote destination.

Inbound Calls Cannot be Received on a Cisco SIP IP Phone

If inbound calls cannot be received on a Cisco SIP IP phone, perform the following tasks as necessary:

- Verify that the line (user portion) was defined in the Request-URI or the SIP INVITE request. The Cisco SIP IP phone requires this information to determine the proper line to ring.

- Verify that the Request-URI is sent to port 5060 of the phone's IP address. The phone listens on UDP port 5060.

- Verify that the Cisco SIP IP phone is registered with the local proxy server.

Poor Voice Quality on the Cisco SIP IP Phone

If a call's voice quality is compromised on the Cisco SIP IP phone, perform the following tasks as necessary:

- Check the network path for errors, packet drops, loss, loops, etc.

- Verify that the ToS level for the media stream being used have been correctly set (via the tos_media parameter in the configuration file).

- Verify that the Cisco SIP IP phone is plugged into a switch rather than a hub to avoid excessive collisions and packet loss.

- Ensure that there is enough bandwidth on the network for the selected codec (especially for calls over a WAN).

- Press the blue "i" button twice on the phone during the call to view realtime transferring and receiving call statistics

- Determine whether the problem just occurs with the handset, headset, or speaker phone, or with all of them.

DTMF Digits Do Not Function Properly

If DTMF digits are not functioning properly, perform the following tasks as necessary:

- If out-of-bound signaling via the AVT tone method has been enabled (via the **dtmf_outofband** configuration file parameter), verify that the remote device supports AVT tones (as defined in RFC 2833). If AVT tones have been enabled and the remote device does not support AVT tone, check for packet loss in the end-to-end path.

- Verify which codec is being used. Lower bandwidth codecs yield poorer result if AVT tones are not support because the DTMF digits are carried via audio.

- Verify the length of the tones being created. The tone must be a minimum signal duration of 40 ms with signaling velocity (tone and pause) of no less than 93 ms (as defined in RFC 2833).

Cisco SIP IP Phones do not Work When Plugged into a Line-Powered Switch

If the Cisco SIP IP phones do not work when plugged into a line-powered switch, perform the following task:

- Verify that the phone is running Version 2.0 of the Cisco SIP IP Phone software. (Line-powered support was not available in Version 1.0).

- Verify that the network media type Network Settings parameter is set to auto-negotiation (auto).

Call Transfer Does Not Work Correctly

If call transfer does not work, verify the remote SIP device that is sending the call is using the SIP BYE/Also: method (as defined in Internet draft sip-cc-01.txt.

Some SIP Messages are Retransmitted Too Often

The Cisco SIP IP phone has several timers (INVITE request retries, BYE request retries, etc.) that can be configured via the **sip_invite_retx** and **sip_retx** configuration file parameters. In most networks, the default values work fine, however, conditions such as network delay, slower-processing proxy servers, and packet loss might require that the timers be adjusted. If some SIP messages appear to be retransmitted too often, adjust these parameters.

Troubleshooting the Cisco SIP Gateway

This section describes troubleshooting features and tips for Cisco SIP Gateways running Cisco IOS Release 12 1(5)XM.

Troubleshooting Features

The following commands can be used to troubleshoot the Cisco SIP Gateway:

- **show sip ?**—Displays the different **show sip** commands.

```
router#show sip ?

retry      Display SIP Protocol Retry Counts
statistics Display SIP UA Statistics
status     Display SIP UA Listener Status
timers     Display SIP Protocol Timers
```

- **show sip status**—Displays the SIP user agent listener status.

```
sip-2600a#show sip status

SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP max-forwards : 6
```

- **show sip statistics**—Displays SIP user agent statistics

```
router#show sip statistics

SIP Response Statistics (Inbound/Outbound)
Informational:
Trying 3/0, Ringing 3/0,
Forwarded 0/0, Queued 0/0,
SessionProgress 0/0
Success:
OkInvite 3/0, OkBye 2/0,
OkCancel 0/0, OkOptions 0/0
Redirection (Inbound only):
MultipleChoice 0, MovedPermanently 0,
MovedTemporarily 0, SeeOther 0,
UseProxy 0, AlternateService 0
Client Error:
BadRequest 0/3, Unauthorized 0/0,
PaymentRequired 0/0, Forbidden 0/0,
NotFound 0/0, MethodNotAllowed 0/0,
NotAcceptable 0/0, ProxyAuthReqd 0/0,
ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
LengthRequired 0/0, ReqEntityTooLarge 0/0,
ReqURITooLarge 0/0, UnsupportedMediaType 0/0,
BadExtension 0/0, TempNotAvailable 0/0,
CallLegNonExistent 0/0, LoopDetected 0/0,
TooManyHops 0/0, AddrIncomplete 0/0,
Ambiguous 0/0, BusyHere 0/0
```

```
Server Error:
InternalError 0/0, NotImplemented 0/0,
BadGateway 0/0, ServiceUnavail 0/0,
GatewayTimeout 0/0, BadSipVer 0/0

Global Failure:
BusyEverywhere 0/0, Decline 0/0,
NotExistAnywhere 0/0, NotAcceptable 0/0

SIP Total Traffic Statistics (Inbound/Outbound)
Invite 3/7, Ack 2/1, Bye 0/2,
Cancel 0/0, Options 0/0
Retry Statistics
Invite 2, Bye 0, Cancel 0, Response 1
```

- **debug sip ?**—Displays the different **debug ccsip** commands.

```
router#debug ccsip ?

all      Enable all SIP debugging traces
calls    Enable CCSIP SPI calls debugging trace
error    Enable SIP error debugging trace
events   Enable SIP events debugging trace
messages Enable CCSIP SPI messages debugging trace
states   Enable CCSIP SPI states debugging trace
```

From one side of a call, the following is a sample of debug output:

```
Router1#debug ccsip all
All SIP call tracing enabled
Router1#
*Mar  6 14:10:42: 0x624CFEF8 : State change from (STATE_NONE, SUBSTATE_NONE)  to
(STATE_IDLE, SUBSTATE_NONE)
*Mar  6 14:10:42:  Queued event from SIP SPI : SIPSPI_EV_CC_CALL_SETUP
*Mar  6 14:10:42: CCSIP-SPI-CONTROL:  act_idle_call_setup
*Mar  6 14:10:42:  act_idle_call_setup:Not using Voice Class Codec

*Mar  6 14:10:42: act_idle_call_setup: preferred_codec set[0] type :g711ulaw bytes:
160
*Mar  6 14:10:42:  Queued event from SIP SPI : SIPSPI_EV_CREATE_CONNECTION
*Mar  6 14:10:42: 0x624CFEF8 : State change from (STATE_IDLE, SUBSTATE_NONE)  to
(STATE_IDLE, SUBSTATE_CONNECTING)
*Mar  6 14:10:42: REQUEST CONNECTION TO IP:166.34.245.231 PORT:5060

*Mar  6 14:10:42: 0x624CFEF8 : State change from (STATE_IDLE, SUBSTATE_CONNECTING)
to (STATE_IDLE, SUBSTATE_CONNECTING)
*Mar  6 14:10:42: CCSIP-SPI-CONTROL:  act_idle_connection_created
*Mar  6 14:10:42: CCSIP-SPI-CONTROL:  act_idle_connection_created: Connid(1) created
to 166.34.245.231:5060, local_port 54113
*Mar  6 14:10:42: sipSPIAddLocalContact
*Mar  6 14:10:42:  Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar  6 14:10:42: CCSIP-SPI-CONTROL:  sip_stats_method
*Mar  6 14:10:42: 0x624CFEF8 : State change from (STATE_IDLE, SUBSTATE_CONNECTING)
to (STATE_SENT_INVITE, SUBSTATE_NONE)
*Mar  6 14:10:42: Sent:
```

```
INVITE sip:3660210@166.34.245.231;user=phone;phone-context=unknown SIP/2.0
Via: SIP/2.0/UDP  166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Sat, 06 Mar 1993 19:10:42 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Cisco-Guid: 2881152943-2184249548-0-483039712
User-Agent: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Max-Forwards: 6
Timestamp: 731427042
Contact: <sip:3660110@166.34.245.230:5060;user=phone>
Expires: 180
Content-Type: application/sdp
Content-Length: 137

v=0
o=CiscoSystemsSIP-GW-UserAgent 1212 283 IN IP4 166.34.245.230
s=SIP Call
t=0 0
c=IN IP4 166.34.245.230
m=audio 20208 RTP/AVP 0

*Mar  6 14:10:42: Received:
SIP/2.0 100 Trying
Via: SIP/2.0/UDP  166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Mon, 08 Mar 1993 22:36:40 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Timestamp: 731427042
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Content-Length: 0


*Mar  6 14:10:42: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.231:5060
*Mar  6 14:10:42: CCSIP-SPI-CONTROL:  act_sentinvite_new_message
*Mar  6 14:10:42: CCSIP-SPI-CONTROL:  sipSPICheckResponse
*Mar  6 14:10:42: CCSIP-SPI-CONTROL:  sip_stats_status_code
*Mar  6 14:10:42:  Roundtrip delay 4 milliseconds for method INVITE

*Mar  6 14:10:42: 0x624CFEF8 : State change from (STATE_SENT_INVITE, SUBSTATE_NONE)
to (STATE_RECD_PROCEEDING, SUBSTATE_PROCEEDING_PROCEEDING)
*Mar  6 14:10:42: Received:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP  166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Mon, 08 Mar 1993 22:36:40 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Timestamp: 731427042
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Content-Type: application/sdp
Content-Length: 137
```

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 969 7889 IN IP4 166.34.245.231
s=SIP Call
t=0 0
c=IN IP4 166.34.245.231
m=audio 20038 RTP/AVP 0

*Mar  6 14:10:42: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.231:5060
*Mar  6 14:10:42: CCSIP-SPI-CONTROL:  act_recdproc_new_message
*Mar  6 14:10:42: CCSIP-SPI-CONTROL:  sipSPICheckResponse
*Mar  6 14:10:42: CCSIP-SPI-CONTROL:  sipSPICheckResponse : Updating session
description
*Mar  6 14:10:42: CCSIP-SPI-CONTROL:  sip_stats_status_code
*Mar  6 14:10:42:  Roundtrip delay 8 milliseconds for method INVITE

*Mar  6 14:10:42: HandleSIP1xxRinging: SDP MediaTypes negotiation successful!
Negotiated Codec     : g711ulaw , bytes :160
Inband Alerting      : 0

*Mar  6 14:10:42: 0x624CFEF8 : State change from (STATE_RECD_PROCEEDING,
SUBSTATE_PROCEEDING_PROCEEDING)  to (STATE_RECD_PROCEEDING,
SUBSTATE_PROCEEDING_ALERTING)
*Mar  6 14:10:46: Received:
SIP/2.0 200 OK
Via: SIP/2.0/UDP  166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27D3FCA8-C7F
Date: Mon, 08 Mar 1993 22:36:40 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Timestamp: 731427042
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Contact: <sip:3660210@166.34.245.231:5060;user=phone>
CSeq: 101 INVITE
Content-Type: application/sdp
Content-Length: 137

v=0
o=CiscoSystemsSIP-GW-UserAgent 969 7889 IN IP4 166.34.245.231
s=SIP Call
t=0 0
c=IN IP4 166.34.245.231
m=audio 20038 RTP/AVP 0

*Mar  6 14:10:46: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.231:5060
*Mar  6 14:10:46: CCSIP-SPI-CONTROL:  act_recdproc_new_message
*Mar  6 14:10:46: CCSIP-SPI-CONTROL:  sipSPICheckResponse
*Mar  6 14:10:46: CCSIP-SPI-CONTROL:  sipSPICheckResponse : Updating session
description
*Mar  6 14:10:46: CCSIP-SPI-CONTROL:  sip_stats_status_code
*Mar  6 14:10:46:  Roundtrip delay 3536 milliseconds for method INVITE

*Mar  6 14:10:46: CCSIP-SPI-CONTROL:  act_recdproc_new_message: SDP MediaTypes
negotiation successful!
Negotiated Codec     : g711ulaw , bytes :160

*Mar  6 14:10:46: CCSIP-SPI-CONTROL:  sipSPIReconnectConnection
*Mar  6 14:10:46:  Queued event from SIP SPI : SIPSPI_EV_RECONNECT_CONNECTION
*Mar  6 14:10:46: CCSIP-SPI-CONTROL:  recv_200_OK_for_invite
*Mar  6 14:10:46:  Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar  6 14:10:46: CCSIP-SPI-CONTROL:  sip_stats_method
*Mar  6 14:10:46: 0x624CFEF8 : State change from (STATE_RECD_PROCEEDING,
```

```
                    SUBSTATE_PROCEEDING_ALERTING)  to (STATE_ACTIVE, SUBSTATE_NONE)
                    *Mar  6 14:10:46: The Call Setup Information is :

                            Call Control Block (CCB) : 0x624CFEF8
                             State of The Call        : STATE_ACTIVE
                             TCP Sockets Used          : NO
                             Calling Number            : 3660110
                             Called Number             : 3660210
                             Negotiated Codec          : g711ulaw
                             Source IP Address (Media): 166.34.245.230
                             Source IP Port   (Media): 20208
                             Destn  IP Address (Media): 166.34.245.231
                             Destn  IP Port   (Media): 20038
                             Destn SIP Addr (Control) : 166.34.245.231
                             Destn SIP Port (Control) : 5060
                             Destination Name          : 166.34.245.231


                    *Mar  6 14:10:46: HandleUdpReconnection: Udp socket connected for fd: 1 with
                    166.34.245.231:5060
                    *Mar  6 14:10:46: Sent:
                    ACK sip:3660210@166.34.245.231:5060;user=phone SIP/2.0
                    Via: SIP/2.0/UDP  166.34.245.230:54113
                    From: "3660110" <sip:3660110@166.34.245.230>
                    To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27D3FCA8-C7F
                    Date: Sat, 06 Mar 1993 19:10:42 GMT
                    Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
                    Max-Forwards: 6
                    Content-Type: application/sdp
                    Content-Length: 137
                    CSeq: 101 ACK

                    v=0
                    o=CiscoSystemsSIP-GW-UserAgent 1212 283 IN IP4 166.34.245.230
                    s=SIP Call
                    t=0 0
                    c=IN IP4 166.34.245.230
                    m=audio 20208 RTP/AVP 0

                    *Mar  6 14:10:46: CCSIP-SPI-CONTROL:  ccsip_caps_ind
                    *Mar  6 14:10:46: ccsip_caps_ind: Load DSP with codec (5) g711ulaw, Bytes=160
                    *Mar  6 14:10:46: ccsip_caps_ind: set DSP for dtmf-relay =
                    CC_CAP_DTMF_RELAY_INBAND_VOICE
                    *Mar  6 14:10:46: CCSIP-SPI-CONTROL:  ccsip_caps_ack
                    *Mar  6 14:10:50: Received:
                    BYE sip:3660110@166.34.245.230:5060;user=phone SIP/2.0
                    Via: SIP/2.0/UDP  166.34.245.231:54835
                    From: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27D3FCA8-C7F
                    To: "3660110" <sip:3660110@166.34.245.230>
                    Date: Mon, 08 Mar 1993 22:36:44 GMT
                    Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
                    User-Agent: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
                    Max-Forwards: 6
                    Timestamp: 731612207
                    CSeq: 101 BYE
                    Content-Length: 0

                    *Mar  6 14:10:50: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
                    166.34.245.231:54835
                    *Mar  6 14:10:50: CCSIP-SPI-CONTROL:  act_active_new_message
                    *Mar  6 14:10:50: CCSIP-SPI-CONTROL:  sact_active_new_message_request
                    *Mar  6 14:10:50: CCSIP-SPI-CONTROL:  sip_stats_method
                    *Mar  6 14:10:50:  Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
                    *Mar  6 14:10:50: CCSIP-SPI-CONTROL:  sip_stats_status_code
                    *Mar  6 14:10:50: CCSIP-SPI-CONTROL:  sipSPIInitiateCallDisconnect : Initiate call
```

```
disconnect(16) for outgoing call
*Mar  6 14:10:50: 0x624CFEF8 : State change from (STATE_ACTIVE, SUBSTATE_NONE)  to
(STATE_DISCONNECTING, SUBSTATE_NONE)
*Mar  6 14:10:50: Sent:
SIP/2.0 200 OK
Via: SIP/2.0/UDP  166.34.245.231:54835
From: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27D3FCA8-C7F
To: "3660110" <sip:3660110@166.34.245.230>
Date: Sat, 06 Mar 1993 19:10:50 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Timestamp: 731612207
Content-Length: 0
CSeq: 101 BYE

*Mar  6 14:10:50:  Queued event From SIP SPI to CCAPI/DNS :
SIPSPI_EV_CC_CALL_DISCONNECT
*Mar  6 14:10:50: CCSIP-SPI-CONTROL:  act_disconnecting_disconnect
*Mar  6 14:10:50: CCSIP-SPI-CONTROL:  sipSPICallCleanup
*Mar  6 14:10:50:  Queued event from SIP SPI : SIPSPI_EV_CLOSE_CONNECTION
*Mar  6 14:10:50: CLOSE CONNECTION TO CONNID:1

*Mar  6 14:10:50: sipSPIIcpifUpdate :CallState: 4 Playout: 1755 DiscTime:48305031
ConnTime 48304651

*Mar  6 14:10:50: 0x624CFEF8 : State change from (STATE_DISCONNECTING, SUBSTATE_NONE)
to (STATE_DEAD, SUBSTATE_NONE)
*Mar  6 14:10:50: The Call Setup Information is :

        Call Control Block (CCB) : 0x624CFEF8
         State of The Call        : STATE_DEAD
         TCP Sockets Used         : NO
         Calling Number           : 3660110
         Called Number            : 3660210
         Negotiated Codec         : g711ulaw
         Source IP Address (Media): 166.34.245.230
         Source IP Port    (Media): 20208
         Destn  IP Address (Media): 166.34.245.231
         Destn  IP Port    (Media): 20038
         Destn SIP Addr (Control) : 166.34.245.231
         Destn SIP Port (Control) : 5060
         Destination Name         : 166.34.245.231

*Mar  6 14:10:50:

        Disconnect Cause (CC)    : 16
        Disconnect Cause (SIP)   : 200

*Mar  6 14:10:50: udpsock_close_connect: Socket fd: 1 closed for connid 1 with remote
port: 5060
Router1#
```

From the other side of the call, the debug output is as follows:

```
3660-2#debug ccsip all
All SIP call tracing enabled
3660-2#
*Mar  8 17:36:40: Received:
INVITE sip:3660210@166.34.245.231;user=phone;phone-context=unknown SIP/2.0
Via: SIP/2.0/UDP  166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Sat, 06 Mar 1993 19:10:42 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Cisco-Guid: 2881152943-2184249548-0-483039712
User-Agent: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Max-Forwards: 6
Timestamp: 731427042
Contact: <sip:3660110@166.34.245.230:5060;user=phone>
Expires: 180
Content-Type: application/sdp
Content-Length: 137

v=0
o=CiscoSystemsSIP-GW-UserAgent 1212 283 IN IP4 166.34.245.230
s=SIP Call
t=0 0
c=IN IP4 166.34.245.230
m=audio 20208 RTP/AVP 0

*Mar  8 17:36:40: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.230:54113
*Mar  8 17:36:40: CCSIP-SPI-CONTROL:  sipSPISipIncomingCall
*Mar  8 17:36:40: 0x624D8CCC : State change from (STATE_NONE, SUBSTATE_NONE)  to
(STATE_IDLE, SUBSTATE_NONE)
*Mar  8 17:36:40: CCSIP-SPI-CONTROL:  act_idle_new_message
*Mar  8 17:36:40: CCSIP-SPI-CONTROL:  sact_idle_new_message_invite
*Mar  8 17:36:40: CCSIP-SPI-CONTROL:  sip_stats_method
*Mar  8 17:36:40:  sact_idle_new_message_invite:Not Using Voice Class Codec

*Mar  8 17:36:40: sact_idle_new_message_invite: Preferred codec[0] type: g711ulaw
Bytes :160
*Mar  8 17:36:40: sact_idle_new_message_invite: Media Negotiation successful for an
incoming call

*Mar  8 17:36:40: sact_idle_new_message_invite: Negotiated Codec     : g711ulaw,
bytes :160
Preferred Codec       : g711ulaw, bytes :160
```

```
*Mar  8 17:36:40:  Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar  8 17:36:40: CCSIP-SPI-CONTROL:  sip_stats_status_code
*Mar  8 17:36:40: Num of Contact Locations 1 3660110 166.34.245.230 5060

*Mar  8 17:36:40: 0x624D8CCC : State change from (STATE_IDLE, SUBSTATE_NONE)  to
(STATE_RECD_INVITE, SUBSTATE_RECD_INVITE_CALL_SETUP)
*Mar  8 17:36:40: Sent:
SIP/2.0 100 Trying
Via: SIP/2.0/UDP  166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Mon, 08 Mar 1993 22:36:40 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Timestamp: 731427042
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Content-Length: 0

*Mar  8 17:36:40:  Queued event From SIP SPI to CCAPI/DNS :
SIPSPI_EV_CC_CALL_PROCEEDING
*Mar  8 17:36:40: CCSIP-SPI-CONTROL:  act_recdinvite_proceeding
*Mar  8 17:36:40:  Queued event From SIP SPI to CCAPI/DNS :
SIPSPI_EV_CC_CALL_ALERTING
*Mar  8 17:36:40: CCSIP-SPI-CONTROL:  ccsip_caps_ind
*Mar  8 17:36:40: ccsip_caps_ind: codec(negotiated) = 5(Bytes 160)
*Mar  8 17:36:40: ccsip_caps_ind: Load DSP with codec (5) g711ulaw, Bytes=160
*Mar  8 17:36:40: ccsip_caps_ind: set DSP for dtmf-relay =
CC_CAP_DTMF_RELAY_INBAND_VOICE
*Mar  8 17:36:40: CCSIP-SPI-CONTROL:  ccsip_caps_ack
*Mar  8 17:36:40: CCSIP-SPI-CONTROL:  act_recdinvite_alerting
*Mar  8 17:36:40:  180 Ringing with SDP - not likely

*Mar  8 17:36:40:  Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar  8 17:36:40: CCSIP-SPI-CONTROL:  sip_stats_status_code
*Mar  8 17:36:40: 0x624D8CCC : State change from (STATE_RECD_INVITE,
SUBSTATE_RECD_INVITE_CALL_SETUP)  to (STATE_SENT_ALERTING, SUBSTATE_NONE)
*Mar  8 17:36:40: Sent:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP  166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Mon, 08 Mar 1993 22:36:40 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Timestamp: 731427042
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Content-Type: application/sdp
Content-Length: 137

v=0
o=CiscoSystemsSIP-GW-UserAgent 969 7889 IN IP4 166.34.245.231
s=SIP Call
t=0 0
c=IN IP4 166.34.245.231
m=audio 20038 RTP/AVP 0

*Mar  8 17:36:44:  Queued event From SIP SPI to CCAPI/DNS : SIPSPI_EV_CC_CALL_CONNECT
*Mar  8 17:36:44: CCSIP-SPI-CONTROL:  act_sentalert_connect
*Mar  8 17:36:44: sipSPIAddLocalContact
*Mar  8 17:36:44:  Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar  8 17:36:44: CCSIP-SPI-CONTROL:  sip_stats_status_code
*Mar  8 17:36:44: 0x624D8CCC : State change from (STATE_SENT_ALERTING, SUBSTATE_NONE)
to (STATE_SENT_SUCCESS, SUBSTATE_NONE)
```

```
*Mar  8 17:36:44: Sent:
SIP/2.0 200 OK
Via: SIP/2.0/UDP  166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27D3FCA8-C7F
Date: Mon, 08 Mar 1993 22:36:40 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Timestamp: 731427042
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Contact: <sip:3660210@166.34.245.231:5060;user=phone>
CSeq: 101 INVITE
Content-Type: application/sdp
Content-Length: 137

v=0
o=CiscoSystemsSIP-GW-UserAgent 969 7889 IN IP4 166.34.245.231
s=SIP Call
t=0 0
c=IN IP4 166.34.245.231
m=audio 20038 RTP/AVP 0

*Mar  8 17:36:44: Received:
ACK sip:3660210@166.34.245.231:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP  166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27D3FCA8-C7F
Date: Sat, 06 Mar 1993 19:10:42 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Max-Forwards: 6
Content-Type: application/sdp
Content-Length: 137
CSeq: 101 ACK

v=0
o=CiscoSystemsSIP-GW-UserAgent 1212 283 IN IP4 166.34.245.230
s=SIP Call
t=0 0
c=IN IP4 166.34.245.230
m=audio 20208 RTP/AVP 0

*Mar  8 17:36:44: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.230:54113
*Mar  8 17:36:44: CCSIP-SPI-CONTROL:  act_sentsucc_new_message
*Mar  8 17:36:44: CCSIP-SPI-CONTROL:  sip_stats_method
*Mar  8 17:36:44: 0x624D8CCC : State change from (STATE_SENT_SUCCESS, SUBSTATE_NONE)
to (STATE_ACTIVE, SUBSTATE_NONE)
*Mar  8 17:36:44: The Call Setup Information is :

        Call Control Block (CCB) : 0x624D8CCC
         State of The Call        : STATE_ACTIVE
         TCP Sockets Used         : NO
         Calling Number           : 3660110
         Called Number            : 3660210
         Negotiated Codec         : g711ulaw
         Source IP Address (Media): 166.34.245.231
         Source IP Port    (Media): 20038
         Destn  IP Address (Media): 166.34.245.230
         Destn  IP Port    (Media): 20208
         Destn SIP Addr (Control) : 166.34.245.230
         Destn SIP Port (Control) : 5060
         Destination Name         : 166.34.245.230

*Mar  8 17:36:47:  Queued event From SIP SPI to CCAPI/DNS :
SIPSPI_EV_CC_CALL_DISCONNECT
```

```
*Mar  8 17:36:47: CCSIP-SPI-CONTROL:  act_active_disconnect
*Mar  8 17:36:47:  Queued event from SIP SPI : SIPSPI_EV_CREATE_CONNECTION
*Mar  8 17:36:47: 0x624D8CCC : State change from (STATE_ACTIVE, SUBSTATE_NONE)  to
(STATE_ACTIVE, SUBSTATE_CONNECTING)
*Mar  8 17:36:47: REQUEST CONNECTION TO IP:166.34.245.230 PORT:5060

*Mar  8 17:36:47: 0x624D8CCC : State change from (STATE_ACTIVE, SUBSTATE_CONNECTING)
to (STATE_ACTIVE, SUBSTATE_CONNECTING)
*Mar  8 17:36:47: CCSIP-SPI-CONTROL:  act_active_connection_created
*Mar  8 17:36:47: CCSIP-SPI-CONTROL:  sipSPICheckSocketConnection
*Mar  8 17:36:47: CCSIP-SPI-CONTROL:  sipSPICheckSocketConnection: Connid(1) created
to 166.34.245.230:5060, local_port 54835
*Mar  8 17:36:47:  Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar  8 17:36:47: CCSIP-SPI-CONTROL:  sip_stats_method
*Mar  8 17:36:47: 0x624D8CCC : State change from (STATE_ACTIVE, SUBSTATE_CONNECTING)
to (STATE_DISCONNECTING, SUBSTATE_NONE)
*Mar  8 17:36:47: Sent:
BYE sip:3660110@166.34.245.230:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP  166.34.245.231:54835
From: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27D3FCA8-C7F
To: "3660110" <sip:3660110@166.34.245.230>
Date: Mon, 08 Mar 1993 22:36:44 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
User-Agent: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Max-Forwards: 6
Timestamp: 731612207
CSeq: 101 BYE
Content-Length: 0

*Mar  8 17:36:47: Received:
SIP/2.0 200 OK
Via: SIP/2.0/UDP  166.34.245.231:54835
From: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27D3FCA8-C7F
To: "3660110" <sip:3660110@166.34.245.230>
Date: Sat, 06 Mar 1993 19:10:50 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Timestamp: 731612207
Content-Length: 0
CSeq: 101 BYE

*Mar  8 17:36:47: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.230:54113
*Mar  8 17:36:47: CCSIP-SPI-CONTROL:  act_disconnecting_new_message
*Mar  8 17:36:47: CCSIP-SPI-CONTROL:  sact_disconnecting_new_message_response
*Mar  8 17:36:47: CCSIP-SPI-CONTROL:  sipSPICheckResponse
*Mar  8 17:36:47: CCSIP-SPI-CONTROL:  sip_stats_status_code
*Mar  8 17:36:47:  Roundtrip delay 4 milliseconds for method BYE

*Mar  8 17:36:47: CCSIP-SPI-CONTROL:  sipSPICallCleanup
*Mar  8 17:36:47:  Queued event from SIP SPI : SIPSPI_EV_CLOSE_CONNECTION
*Mar  8 17:36:47: CLOSE CONNECTION TO CONNID:1

*Mar  8 17:36:47: sipSPIIcpifUpdate :CallState: 4 Playout: 1265 DiscTime:66820800
ConnTime 66820420

*Mar  8 17:36:47: 0x624D8CCC : State change from (STATE_DISCONNECTING, SUBSTATE_NONE)
to (STATE_DEAD, SUBSTATE_NONE)
*Mar  8 17:36:47: The Call Setup Information is :

        Call Control Block (CCB) : 0x624D8CCC
         State of The Call       : STATE_DEAD
         TCP Sockets Used        : NO
         Calling Number          : 3660110
```

```
                       Called Number          : 3660210
                       Negotiated Codec        : g711ulaw
                       Source IP Address (Media): 166.34.245.231
                       Source IP Port    (Media): 20038
                       Destn  IP Address (Media): 166.34.245.230
                       Destn  IP Port    (Media): 20208
                       Destn SIP Addr (Control) : 166.34.245.230
                       Destn SIP Port (Control) : 5060
                       Destination Name        : 166.34.245.230

       *Mar  8 17:36:47:

                       Disconnect Cause (CC)    : 16
                       Disconnect Cause (SIP)   : 200

       *Mar  8 17:36:47: udpsock_close_connect: Socket fd: 1 closed for connid 1 with remote
       port: 5060
```

Troubleshooting Tips

This section provides tips for resolving the following Cisco SIP gateway problems:

- Unable to Make Outbound Calls from the Cisco SIP Gateway to a SIP Endpoint, page 5-18
- Unable to Make Inbound Calls to a PSTN Through a Cisco SIP Gateway, page 5-19
- Calls to a PSTN via the Cisco SIP Gateway Fail with a "400 Bad Request" Response, page 5-19
- Voice Quality is Compromised on Calls Through or From the Cisco SIP Gateway, page 5-20
- Some SIP Messages are Retransmitted Too Often, page 5-21
- Some SIP Messages are Retransmitted Too Often, page 5-21
- Call Transfer Does Not Work Correctly, page 5-21

Unable to Make Outbound Calls from the Cisco SIP Gateway to a SIP Endpoint

If a call cannot be placed from the Cisco SIP gateway, perform the following tasks as necessary:

- Verify that the voice ports are properly configured and enabled for PSTN-side signaling protocol.
- Verify that there is a valid VoIP dial peer configured which meets the following requirements:
  - Matches the required destination pattern
  - Is SIP-enabled (via the **session protocol sipv2** command)
  - Has the correct dial peer session target defined (via the **session target** *sip-server* command
  - Has the codec correctly defined
- Using the **ping** command, verify that the SIP gateway can communicate via IP with the SIP proxy or remote SIP device.
- If the SIP proxy server is defined using a FQDN, verify that the DNS server is correctly configured to resolve that address using a DNS SRV record.
- Ensure that the timezone format configured on the SIP gateway is GMT.
- View the **debug ccsip all | calls | error | events | messages | states** command output for protocol errors.

Unable to Make Inbound Calls to a PSTN Through a Cisco SIP Gateway

If inbound calls to a PSTN cannot be made through the Cisco SIP gateway, perform the following tasks as necessary to determine the cause:

- Verify that the voice ports are correctly configured and enabled for the PSTN-side signaling protocol.
- Verify that a valid POTS dial peer is configured which matches the required destination pattern.
- Using the **ping** command, verify that the Cisco SIP gateway can communicate with the SIP proxy server or remote SIP device via IP.
- If the inbound call has any hostnames defined as a FQDN, ensure that the proper DNS configuration is enabled on the Cisco SIP gateway (to resolve the hosts).
- View the **debug ccsip all | calls | error | events | messages | states** command output for protocol errors.

Calls to a PSTN via the Cisco SIP Gateway Fail with a "400 Bad Request" Response

If the Cisco SIP gateway does not like part of a SIP message (header or SDP), the call attempt will fail with a "400 Bad Request" response.

To determine whether the call failed because of a SIP header errors, issue the **debug ccsip all | calls | error | events | messages | states** command that displays information on the error message or verify the required SIP header elements exist as defined in RFC 2543. Also, the "Cisco SIP Compliance Reference Information" in the *Session Initiation Protocol Gateway Call Flows* (http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121rel/sipcfs/index.htm) document lists the currently supported SIP headers.

Table 5-2 lists possible SDP-related errors and their related error codes. Table 5-3 lists the possible CheckRequest errors.

Table 5-2   SDP Errors and Related Error Codes

SIP SDP Parser Error Codes
SDP_ERR_INFO_UNAVAIL
SDP_ERR_VERSINFO_INVALID
SDP_ERR_CONNINFO_IN
SDP_ERR_CONNINFO_IP
SDP_ERR_CONNINFO_NULL
SDP_ERR_CONNINFO_INVALID
SDP_ERR_MEDIAINFO_TYPE
SDP_ERR_MEDIAINFO_INVALID
SDP_ERR_MEDIAINFO_NULL
SDP_ERR_OWNERINFO_NULL
SDP_ERR_OWNERINFO_SESSID_NULL
SDP_ERR_OWNERINFO_SESSID_INVALID
SDP_ERR_OWNERINFO_VERSID_NULL
SDP_ERR_OWNERINFO_VERSID_INVALID
SDP_ERR_OWNERINFO_IN

Table 5-2   SDP Errors and Related Error Codes

SIP SDP Parser Error Codes
SDP_ERR_OWNERINFO_IP
SDP_ERR_TIMEINFO_ST_NULL
SDP_ERR_TIMEINFO_ET_NULL
SDP_ERR_TIMEINFO_ST_INVALID
SDP_ERR_TIMEINFO_ET_INVALID
SDP_ERR_ATTRINFO_INVALID
SDP_ERR_ATTRINFO_NULL
SDP_ERR_AUDIO_MEDIA_UNAVAIL
SDP_ERR_MEDIAINFO_PORT_INVALID
SDP_ERR_MEDIAINFO_MALLOC_FAIL
SDP_ERR_ATTRINFO_MALLOC_FAIL

Table 5-3   Possible CheckRequest Errors

CheckRequest Errors
CHK_REQ_FAIL_MISMATCH_CSEQ
CHK_REQ_FAIL_INVALID_CSEQ
CHK_REQ_FAIL_FROM_TO
CHK_REQ_FAIL_VERSION
CHK_REQ_FAIL_METHOD_UNKNOWN
CHK_REQ_FAIL_REQUIRE_UNSUPPORTED
CHK_REQ_FAIL_CONTACT_MISSING
CHK_REQ_FAIL_MISMATCH_CALLID
CHK_REQ_FAIL_MALFORMED_CONTACT
CHK_REQ_FAIL_MALFORMED_RECORD_ROUTE

Voice Quality is Compromised on Calls Through or From the Cisco SIP Gateway

If the voice quality on calls through or from the Cisco SIP gateway is compromised, perform the following tasks as necessary to determine the cause:

- Check the network path for errors, packet drops, loss, loops, etc.

- Verify that the TOS bits have been correctly set in the VoIP dial peer using the **ip precedence** command.

- To minimize excessive collisions and packet loss, connect the Cisco SIP gateway to a switch rather than a hub.

- Verify that enough bandwidths exists on the network for the configured codec (especially for calls over a WAN).

- View the output of the show interface command for packet drops. View the output of the s**how voice dsp** command or DSP-related issues.

- Verify whether errors exists on the voice-ports that could be causing the echo, etc.

Some SIP Messages are Retransmitted Too Often

The Cisco SIP gateway has SIP timers (INVITE request retries, BYE request retries, etc) configured under the SIP UA via the **timers trying number**, **timers expires time**, and **retry invite number** commands. In most networks, the default values work fine, however, conditions such as network delay, slower-processing proxy servers, and packet loss might require that the timers be adjusted. If some SIP messages appear to be retransmitted too often, adjust these parameters.

Call Transfer Does Not Work Correctly

If call transfer does not function properly, perform the following tasks to determine the cause:

- Verify that the "application session" is defined on the VoIP and POTS dial peers.

- Verify that the remote SIP device that is sending the call is using the SIP BYE/Also: method (as defined in Internet draft sip-cc-01.txt.

- Verify that a dial peer that has "application session" defined is matched using the **debug voip ccapi inout** command. The application used after the BYE request is sent should be "session" instead of "SESSION."

Troubleshooting the Cisco SIP Proxy Server

This section describes troubleshooting features and tips for the Cisco SIP Proxy Server, Version 1.0.

Troubleshooting Features

When trying to troubleshoot problems with the Cisco SIP Proxy Server, remember the following:

- Each module with the Cisco SIP Proxy Server has debugging capabilities that can be set via a debug flag in the sipd.conf file. When these debug flags are set to On, and the server is running in multi-process mode, the debug output is written to the ./logs/error_log file. When the flags are set to On and single-process mode is enabled, the debug output is written to standard output.

- Changes to the sipd.conf file do not automatically take effect. To have any changes take effect, issue a graceful restart by issuing the following command:

  ./sipdctl graceful

Troubleshooting Tips

This section provides tips for resolving the following Cisco SIP Proxy Server problems:

- The Cisco SIP Proxy Server Does Not Start, page 5-22
- The Cisco SIP Proxy Server Does Not Allow Devices to Register, page 5-22
- The Cisco SIP Proxy Server Does Not Route Calls Properly, page 5-23
- The Cisco SIP Proxy Server Reports that SIP Messages are Bad, page 5-23
- Cisco SIP Proxy Server Farming Does Not Work Correctly, page 5-23
- Voice Quality Problems, page 5-23

The Cisco SIP Proxy Server Does Not Start

If the Cisco SIP Proxy Server does not start, perform the following tasks as necessary to determine the cause:

- Verify that the *usr/local/sip* directory (on Linux) or the *opt/local/sip/* directory (on Solaris) has the read and write permissions set that allow the user to start the Cisco SIP Proxy Server.
- Verify that the LD_LIBRARY_PATH environment variable has been enabled as defined in the *Cisco SIP Proxy Server Administrator Guide*.
- If using the Linux RPM version of the Cisco SIP Proxy Server, verify that the software has been correctly installed.
- Verify that an older version of the Cisco SIP Proxy Server is not still running by issuing the following command:

    ps -ef | grep -i sip

    If another version is running, disable these processes by issuing the following command:

    ./sipdctl stop

- Verify that the Cisco SIP Proxy Server can resolve its hostname via DNS.

The Cisco SIP Proxy Server Does Not Allow Devices to Register

If the Cisco SIP Proxy Server does not allow devices to register, perform the following tasks as necessary to determine the cause:

- Verify that registration services are enabled via the mod_sip_registry module in the sipd.conf file.
- If authentication is required, ensure that the SIP UA and password is defined in the MySQL database subscriber table and that the Cisco SIP Proxy Server can connect to the MySQL database.
- Verify the type the SIP UAs are using the HTTP Digest authentication method.

The Cisco SIP Proxy Server Does Not Route Calls Properly

If the Cisco SIP Proxy Server does not properly route calls, perform the following tasks as necessary to determine the cause:

- Verify that numbering plans statements are configured correctly in the mod_sip_numexpand module in the sipd.conf file.
- Verify that the translation modules (mod_sip_registry, mod_sip_enum, and mod_sip_gktmp are correctly configured and have the correct entries populated.
- Verify that the correct routes exist in the static routing table of the sipd.conf file.
- Verify that the DNS server is configured for DNS SRV and DNS A records of the devices to be routed.
- View the error_log file for error messages (bad SIP messages, process errors, etc.).

The Cisco SIP Proxy Server Reports that SIP Messages are Bad

If the Cisco SIP Proxy Server reports SIP messages as bad, enable the StateMachine debug flag in the sipd.conf file and view the SIP message in the error_log file. The error_log file should contain SIP messages that are received in ASCII format. Verify the SIP headers of those messages against the headers defined in RFC 2543 or verify the SDP information against the information defined in RFC 2327.

Cisco SIP Proxy Server Farming Does Not Work Correctly

If Cisco SIP Proxy Server farming does not work correctly, perform the following tasks as necessary to determine the cause:

- Verify that all members of the far have the same sipd.conf file configuration
- Verify that all members of the farm have an entry for the other farm members defined in the **Cisco_Registry_Farm_Members** directive in their sipd.conf file.
- Verify that all members of the farm are running the same version of the Cisco SIP Proxy Server.
- Verify that all members of the farm are sychronized to the same clock source via Network Time Protocol (NTP).

Voice Quality Problems

SIP using RTP to transmit media between two endpoints. The Cisco SIP Proxy server is only involved with the SIP signaling and not the media. Therefore, voice-quality issues should be determined in the endpoint devices not the Cisco SIP proxy server because the media does not pass through it.

SIP Messages and Compliance Information for the Cisco VoIP Infrastructure Solution for SIP

This chapter describes SIP messages and methods and describes how the SIP components of the Cisco VoIP Infrastructure Solution for SIP handle the messages. It includes the following sections:

- SIP Messages and Methods, page 6-1
- SIP Compliance Information, page 6-2
- PSTN Cause Code and SIP Event Mappings, page 6-11

SIP Messages and Methods

All SIP messages are either requests from a server or client, or responses to a request. The messages are formatted according to RFC 822, "Standard for the format of ARPA internet text messages". For all messages, the general format is:

- A start line
- One or more header fields
- An empty line
- A message body (optional)

Each line must end with a carriage return-line feed (CRLF).

Requests

SIP uses six types (methods) of requests:

- 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 currently in progress.
- OPTIONS—Queries the capabilities of servers.
- REGISTER—Registers the address listed in the To header field with a SIP server. Gateways do not support the REGISTER method.

Responses

In response to requests, SIP uses the following categories of responses:

- 1xx Informational Messages
- 2xx Successful Responses
- 3xx Redirection Responses
- 4xx Request Failure Responses
- 5xx Server Failure Responses
- 6xx General Failure Responses

The Registration Process

A registration occurs when a client needs to inform a proxy or redirect server of its location. During this process, the client sends a REGISTER request to the proxy or redirect server and includes the address (or addresses) at which it can be reached.

The Invitation Process

An invitation occurs when one SIP end point (user A) "invites" another SIP endpoint (user B) to join in a call. During this process, user A sends an INVITE message requesting that user B join a particular conference or establish a two-party conversation. If user B wants to join the call, it sends an affirmative response (SIP 2xx). Otherwise, it sends a failure response (SIP 4xx). Upon receiving the response, user A acknowledges the response with an ACK message. If user A no longer wants to establish this conference, it sends a BYE message instead of an ACK message.

SIP Compliance Information

Table 6-1 lists the SIP requests and describes the support provided by each component.

Table 6-1   Support for SIP Requests

Request	SIP IP Phone	SIP Gateway	SIP Proxy Server
INVITE	The SIP IP phone supports initial INVITEs as well as mid-call INVITEs, which are used for call hold and call transfer.	The gateway supports mid-call INVITEs with the same call ID but different SDP session parameters (to change the transport address).	The SIP proxy server proxies SIP INVITE requests.
ACK	Supported.	Supported.	The SIP proxy server proxies the SIP ACK method.[1]
OPTIONS	Not supported.	The gateway does not generate OPTIONS. However, it will respond to OPTIONS requests.	The SIP proxy server proxies OPTIONS.
BYE	Supported.	Supported.	Supported.

Request	SIP IP Phone	SIP Gateway	SIP Proxy Server
CANCEL	Supported.	Supported.	The SIP proxy server proxies the SIP CANCEL method.[2]
REGISTER	The SIP IP phone supports both user and device registration.	Not applicable.	The SIP proxy server supports both user and device registration.

1. The Cisco SIP Proxy Server can generate a local ACK for a non-200 OK final response to an INVITE request.

2. The Cisco SIP Proxy Server can generate a local CANCEL for a pending branch when it receives a 200 OK or 6*xx* response from the branch.

Table 6-2 lists the responses within each of the categories of SIP messages and describes how each is handled by the components in the solution.

Table 6-2   Handling of SIP Responses

Response	SIP IP Phone	SIP Gateway	SIP Proxy Server
1xx Informational Messages			
100 Trying This response indicates that action is being taken on behalf of the caller, but that the callee has not yet been located.	The SIP IP phone generates this response for an incoming INVITE. Upon receiving this response, the phone waits for a 180 Ringing or 200 OK response.	The SIP gateway generates this response for an incoming INVITE. Upon receiving this response, the gateway stops retransmitting INVITEs. It then waits for a 180 Ringing or 200 OK response.	The Cisco SIP proxy server generates and proxies this response for an incoming INVITE. Upon receiving this response, the server waits for a 180 Ringing, 183 Session progress, or 200 OK response.
180 Ringing This response indicates that the callee has been located and is being notified of the call.	The SIP IP phone generates this response when a request has been received and the phone is waiting for the user to "pick up". Upon receiving this response, the phone waits for a 200 OK response.	The SIP gateway generates a 180 Ringing response when the called party has been located and is being alerted. Upon receiving this response, the gateway waits for a 200 OK response.	The SIP proxy server proxies 180 Ringing responses.
181 Call is being forwarded This response indicates that the call is being rerouted to another destination.	The SIP IP phone does not generate this response. Upon receiving this response, the phone processes the response the same way that it processes a 100 Trying response.	The SIP gateway does not generate this response. Upon receiving this response, the gateway processes the response the same way that it processes a 100 Trying response.	The SIP proxy server proxies this response.
182 Queued This response indicates that the callee is not currently available but that they have elected to queue the call rather than reject it.	The SIP IP phone does not generate this message. Upon receiving this response, the phone processes the response the same way that it processes a 100 Trying response.	The SIP gateway does not generate this response. Upon receiving this response, the gateway processes the response the same way that it processes a 100 Trying response.	The SIP proxy server proxies this response.

Response	SIP IP Phone	SIP Gateway	SIP Proxy Server
183 Session progress This response is used to perform inband alerting for the caller.	The SIP IP phone does not generate this message. Upon receiving this response, the phone waits for a 200 OK response.	The SIP gateway generates a 183 Session progress response when it receives an ISDN SETUP message that contains a Progress element from a PSTN.	The SIP proxy server proxies 183 Session Progress responses.
2xx Successful Responses			
200 OK This response indicates that the request has been successfully processed. The action taken depends on the request made.	The SIP IP phone generates this response when the user has answered the phone. Upon receiving this response, the phone responds with an ACK.	The SIP gateway generates this response when the PBX indicates that the user has answered the phone. Upon receiving this response, the gateway forwards the response to the corresponding party and responds with an ACK.	The SIP proxy server can generate a 200 OK response to a REGISTER or CANCEL request. The SIP proxy server proxies 200 OK responses to other requests.
3xx Redirection Responses			
300 Multiple choices This response indicates that the address resolved to more than one location. All locations are provided and the user or UA is allowed to select which location to use.	The SIP IP phone does not generate this response. Upon receiving this response, the phone contacts the new address specified in the contact header.	The SIP gateway does not generate this response. Upon receiving this response, the gateway contacts the new address specified in the contact header.	When in Redirect mode, the SIP proxy server can only generate the 300 Multiple Choices response. When in Proxy mode, the SIP proxy server can generate or proxy this response.
301 Moved permanently This response indicates that the user is no longer available at the specified location. An alternate location is included in the header.	The SIP IP phone does not generate this response. Upon receiving this response, the phone contacts the new address specified in the contact header.	The SIP gateway does not generate this response. Upon receiving this response, the gateway contacts the new address specified in the contact header.	The SIP proxy server proxies this response.
302 Moved temporarily This response indicates that the user is temporarily unavailable at the specified location. An alternate location is included in the header.	The SIP IP phone does not generate this response at this time. Upon receiving this response, the phone contacts the new address specified in the contact header.	The SIP gateway does not generate this response. Upon receiving this response, the gateway contacts the new address specified in the contact header.	When in Redirect mode, the SIP proxy server can only generate the 302 Moved Temporarily response when a matching registration is located. When in Proxy mode, the SIP proxy server can generate or proxy this response.
305 Use proxy This response indicates that the caller must use a proxy to contact the callee.	The SIP IP phone does not generate this response. Upon receiving this response, the phone contacts the new address specified in the contact header field.	The SIP gateway does not generate this response. Upon receiving this response, the gateway contacts the new address specified in the contact header.	The SIP proxy server proxies this response.

Response	SIP IP Phone	SIP Gateway	SIP Proxy Server
380 Alternative service This response indicates that the call was unsuccessful, but that alternative services are available.	The SIP IP phone does not generate this response. Upon receiving this response, the phone contacts the new address specified in the contact header field.	The SIP gateway does not generate this response. Upon receiving this response, the gateway contacts the new address specified in the contact header.	The SIP proxy server does not proxy this response.
4xx Request Failure Responses			
400 Bad request This response indicates that the request could not be understood because of an illegal format.	The SIP IP phone generates a 400 Bad Request response for a badly formed request. Upon receiving this response, the phone initiates a graceful call disconnect [during which the caller will hear a fast busy tone] before clearing the call request.	The SIP gateway generates this response for a badly formed request. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server generates and proxies 400 Bad Request responses.
401 Unauthorized This response indicates that the request requires user authentication.	The SIP IP phone does not generate this response. Upon receiving this response during registration, the phone accepts the response and sends a new request that contains the user's authentication information.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The proxy server proxies this response.
402 Payment required This response indicates that payment is required to complete the call.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The proxy server proxies this response.
403 Forbidden This response indicates that the server has received and understood the request but will not provide the service.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The proxy server proxies this response.
404 Not found This response indicates that the server has definite information that the user does not exist in the specified domain.	The SIP IP phone generates this response if it is unable to locate the callee. Upon receiving this response, the phone notifies the user.	The SIP gateway generates this response if it is unable to locate the callee. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server generates and proxies this response.

Response	SIP IP Phone	SIP Gateway	SIP Proxy Server
405 Method not allowed This response indicates that the method specified in the request is not allowed. The response contains a list of allowed methods.	The SIP IP phone generates this response if an invalid method is specified in the request. Upon receiving this response, the phone notifies the user.	The SIP gateway generates this response if an invalid method is specified in the request. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The proxy server proxies this response.
406 Not acceptable This response indicates that the requested resource is capable of generating only responses that have content characteristics not acceptable as specified in the accept header of the request.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The proxy server proxies this response.
407 Proxy authentication required This response is similar to the 401 Unauthorized response. However, this response indicates that the client must first authenticate itself with the proxy.	The SIP IP phone does not generate this response. Upon receiving this response, the phone can repeat the request with a suitable Proxy-Authorization field. This field should contain the authentication information for the user agent for the next outbound proxy or gateway.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server generates and proxies this response.
408 Request timeout This response indicates that the server could not produce a response before the Expires time out.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server generates and proxies this response.
409 Conflict This response indicates that the request could not be processed because of a conflict with the current state of the resource.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server generates and proxies this response.
410 Gone This response indicates that a resource is no longer available at the server and no forwarding address is known.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user.	The SIP gateway generates this response if the PSTN returns a cause code of unallocated number. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server proxies this response. The 410 Gone response indicates that a resource is no longer available at the server and no forwarding address is known.

Response	SIP IP Phone	SIP Gateway	SIP Proxy Server
411 Length required This response indicates that the user refuses to accept the request without a defined content length.	The SIP IP phone does not generate this response. Upon receiving this response, the phone resends the request with a valid Content-Length header field.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server proxies this response. This response indicates that the user refuses to accept the request without a defined content length.
413 Request entity too large This response indicates that server refuses to process the request because it is larger than the server is willing or able to process.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user. If the response contains a Retry-after field, the user is informed that the call can be attempted in accordance with the retry time provided.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server proxies this response. 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.
414 Request-URI too long This response indicates that the server refuses to process the request because the Request-URI is too long for the server to interpret.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server generates and proxies this response. Upon receiving this response, the user is notified.
415 Unsupported media This response indicates that the server refuses to process the request because the format of the body is not supported by the destination endpoint.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server proxies this response. Upon receiving this response, the user is notified.
420 Bad extension This response indicates that the server could not understand the protocol extension indicated in the Require header.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user.	The SIP gateway generates this response if it does not understand the service requested in the Require header. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server generates and proxies this response.
480 Temporarily unavailable This response indicates that the callee was contacted but is temporarily unavailable.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user that the destination is temporarily unavailable and displays any retry information.	The SIP gateway generates this response if the callee is unavailable. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server proxies this response. 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.

Response	SIP IP Phone	SIP Gateway	SIP Proxy Server
481 Call leg/transaction does not exist This response indicates that the server is ignoring the request because it was either a BYE for which there was no matching leg ID or a CANCEL for which there was no matching transaction.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user.	The SIP gateway generates this response when an existing call leg cannot be identified. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server generates and proxies this response.
482 Loop detected This response indicates that the server received a request that included itself in the path.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server generates and proxies this response.
483 Too many hops This response indicates that the server received a request that required more hops than allowed by the Max-Forwards header.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server generates and proxies this response.
484 Address incomplete This response indicates that the server received a request containing an incomplete address.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server proxies this response.
485 Ambiguous This response indicates that the server received a request in which the callee address was ambiguous. It can provide possible alternate addresses.	The SIP IP phone does not generate this response. Upon receiving this response, the phone can reinitiate the call (if new contact information is received).	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server proxies this response.
486 Busy here This response indicates that the callee was contacted but that their system is unable to take additional calls.	The SIP IP phone generates this response if the called party is off hook. Upon receiving this response, the phone notifies the user and generates a busy tone.	The SIP gateway generates this response when the called party is busy. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server proxies this response.

Response	SIP IP Phone	SIP Gateway	SIP Proxy Server
5xx Server Failure Responses			
500 Server internal error This response indicates that the server or gateway encountered an unexpected error that prevented it from processing the request.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user with fast-busy signal and disconnects the call. If an additional contact is known, the phone can send a new request.	The SIP gateway generates this response if it encountered an unexpected error that prevented it from processing the request. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server generates and proxies this response.
501 Not implemented This response indicates that the server or gateway does not support the functions required to complete the request.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user with fast-busy signal and disconnects the call. If an additional contact is known, the phone can send a new request.	The SIP gateway generates this response if it does not support the functions required to complete the request. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server generates and proxies this response.
502 Bad gateway This response indicates that the server or gateway received an invalid response from a downstream server.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user with fast-busy signal and disconnects the call. If an additional contact is known, the phone can send a new request.	The SIP gateway generates this response if it received an invalid response from a downstream server. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server proxies this response.
503 Service unavailable This response indicates that the server or gateway is unable to process the request due to an overload or maintenance problem.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user with fast-busy signal and disconnects the call. If an additional contact is known, the phone can send a new request.	The SIP gateway generates this response if it is unable to process the request due to an overload or maintenance problem. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server proxies this response.
504 Gateway timeout This response indicates that the server or gateway did not receive a timely response from another server (such as a location server).	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user with fast-busy signal and disconnects the call. If an additional contact is known, the phone can send a new request.	The SIP gateway generates this response if it did not receive a timely response from another server (such as a location server). Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server proxies this response.

Response	SIP IP Phone	SIP Gateway	SIP Proxy Server
505 Version not supported This response indicates that the server or gateway does not support the version of the SIP protocol used in the request.	The SIP IP phone generates this response if it does not support the version indicated in the SIP request. Upon receiving this response, the phone notifies the user with fast-busy signal and disconnects the call. If an additional contact is known, the phone can send a new request.	The SIP gateway generates this response if it does not support the version indicated in the SIP request. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server proxies this response.
6xx Global Failure Responses			
600 Busy everywhere This response indicates that the callee was contacted but that the callee is busy and cannot take the call at this time.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user with fast-busy signal and disconnects the call.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server proxies this response.
603 Decline This response indicates that the callee was contacted but cannot or does not want to participate in the call.	The SIP IP phone can generate this response if the user is using call screening. Upon receiving this response, the phone notifies the user with fast-busy signal and disconnects the call.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server proxies this response.
604 Does not exist anywhere This response indicates that the server has authoritative information that the callee does not exist in the network.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user with fast-busy signal and disconnects the call.	The SIP gateway does not generate this response. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server proxies this response.
606 Not acceptable This response indicates that the callee was contacted, but that some aspect of the session description was unacceptable.	The SIP IP phone does not generate this response. Upon receiving this response, the phone notifies the user with fast-busy signal and disconnects the call. If an additional contact is known, the phone can send a new request.	The SIP gateway generates this response if some aspect of the session description is unacceptable to the callee. Upon receiving this response, the gateway initiates a graceful call disconnect and clears the call.	The SIP proxy server proxies this response.

PSTN Cause Code and SIP Event Mappings

Table 6-3 lists the PSTN cause codes that can be sent as an ISDN cause information element (IE) and the corresponding SIP event for each.

Table 6-3 PSTN Cause Code to SIP Event Mappings

PSTN Cause Code	Description	SIP Event
1	Unallocated number	410 Gone
3	No route to destination	404 Not found
16	Normal call clearing	BYE
17	User busy	486 Busy here
18	No user responding	480 Temporarily unavailable
19	No answer from the user	
21	Call rejected	603 Decline
22	Number changed	302 Moved temporarily
27	Destination out of order	404 Not found
28	Address incomplete	484 Address incomplete
29	Facility rejected	501 Not implemented
31	Normal unspecified	404 Not found
34	No circuit available	503 Service unavailable
38	Network out of order	
41	Temporary failure	
42	Switching equipment congestion	
44	Requested channel not available	
47	Resource unavailable	
55	Incoming class barred within CUG	603 Decline
57	Bearer capability not authorized	501 Not implemented
58	Bearer capability not presently available	
63	Service or option unavailable	503 Service unavailable
65	Bearer cap not implemented	501 Not implemented
79	Service or option not implemented	
87	User not member of CUG	603 Decline
88	Incompatible destination	400 Bad request
95	Invalid message	
102	Recover on timer expiry	408 Request timeout
111	Protocol error	400 Bad request
127	Interworking unspecified	500 Internal server error
Any code other than those listed above		500 Internal server error

Table 6-4 lists the SIP events and the corresponding PSTN cause codes for each.

Table 6-4 SIP Event to PSTN Cause Code Mapping

SIP Event	PSTN Cause Code	Description
400 Bad request	127	Interworking
401 Unauthorized	57	Bearer cap not authorized
402 Payment required	21	Call rejected
403 Forbidden	57	Bearer cap not authorized
404 Not found	1	Unallocated number
405 Method not allowed	127	Interworking
406 Not acceptable		
407 Proxy authentication required	21	Call rejected
408 Request timeout	102	Recover on timer expiry
409 Conflict	41	Temporary failure
410 Gone	1	Unallocated number
411 Length required	127	Interworking
413 Request entity too long		
414 Request URI too long		
415 Unsupported media type	79	Service or option not available
420 Bad extension	127	Interworking
480 Temporarily unavailable	18	No user response
481 Call leg does not exist	127	Interworking
482 Loop detected		
483 Too many hops		
484 Address incomplete	28	Address incomplete
485 Address ambiguous	1	Unallocated number
486 Busy here	17	User busy
500 Internal server error	41	Temporary failure
501 Not implemented	79	Service or option not implemented
502 Bad gateway	38	Network out of order
503 Service unavailable	63	Service or option not available
504 Gateway timeout	102	Recover on timer expiry
505 Version not implemented	127	Interworking
600 Busy everywhere	17	User busy
603 Decline	21	Call rejected
604 Does not exist anywhere	1	Unallocated number
606 Not acceptable	58	Bearer cap not presently available

SIP Call Flow Process for the Cisco VoIP Infrastructure Solution for SIP

This chapter describes the flow of these messages in the Cisco VoIP Infrastructure Solution for SIP. It includes the following sections:

Note For information about SIP-specific uOne Messaging System call flows, see the *SIP Compliance and Signaling Call Flows for uOne 4.2(2)s, SIP Edition* document at:

http://www.cisco.com/univercd/cc/td/doc/product/voice/uone/srvprov/r422ssip/callflow/index.htm

Call Flow Scenarios for Successful Calls

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

SIP Gateway-to-SIP Gateway—Call Setup and Disconnect

Figure 7-1 illustrates a successful gateway-to-gateway call setup and disconnect. In this call flow scenario, the two end users are User A and User B. User A is located at PBX A. PBX A is connected to SIP gateway 1 via a T1/E1. User B is located at PBX B. PBX B is connected to SIP gateway 2 via a T1/E1. User B's phone number is 555-0002. SIP gateway 1 is connected to SIP gateway 2 over 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 hangs up.

Figure 7-1   SIP Gateway-to-SIP Gateway—Call Setup and Disconnect

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.

Step	Action	Description
2	INVITE—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an INVITE request to SIP gateway 2. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as "INVITE sip:555-0002@companyb.com; user=phone." The "user=phone" parameter indicates that the Request-URI address is a telephone number rather than a user name.
		• PBX A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which SIP gateway 1 is prepared to receive the RTP data is specified.
3	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.
4	Setup—SIP gateway 2 to PBX B	SIP gateway 2 receives the INVITE request from SIP gateway 1 and initiates a Call Setup with User B via PBX B.
5	100 Trying—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 100 Trying response to the INVITE request sent by SIP gateway 1. The 100 Trying response indicates that the INVITE request has been received by SIP gateway 2 but that User B has not yet been located and that some unspecified action, such as a database consultation, is taking place.
6	Call Proceeding—PBX B to SIP gateway 2	PBX B sends a Call Proceeding message to SIP gateway 2 to acknowledge the Call Setup request.
7	Alerting—PBX B to SIP gateway 2	PBX B locates User B and sends an Alert message to SIP gateway 2. User B's phone begins ringing.
8	180 Ringing—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 180 Ringing response to SIP gateway 1. The 180 Ringing response indicates that SIP gateway 2 has located, and is trying to alert, User B.
9	Alerting—SIP gateway 1 to PBX A	SIP gateway 1 sends an Alert message to User A via PBX A. The Alert message indicates that SIP gateway 1 has received a 180 Ringing response from SIP gateway 2. User A hears the ringback tone that indicates that User B is being alerted.

At this point, a one-way voice path is established between SIP gateway 1 and PBX A and between SIP gateway 2 and PBX B. A two-way RTP channel is established between SIP gateway 1 and SIP gateway 2.

Step	Action	Description
10	Connect—PBX B to SIP gateway 2	User B answers phone. PBX B sends a Connect message to SIP gateway 2. The Connect message notifies SIP gateway 2 that the connection has been made.

Step	Action	Description
11	200 OK—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 200 OK response to SIP gateway 1. The 200 OK response notifies SIP gateway 1 that the connection has been made.
		If User B supports the media capability advertised in the INVITE message sent by SIP gateway 1, it advertises the intersection of its own and User A's media capability in the 200 OK response. If User B does not support the media capability advertised by User A, it sends back a 400 Bad Request response with a 304 Warning header field.
12	Connect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Connect message to PBX A. The Connect message notifies PBX A that the connection has been made.
13	Connect ACK—PBX A to SIP gateway 1	PBX A acknowledges SIP gateway 1's Connect message.
14	ACK—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an ACK to SIP gateway 2. The ACK confirms that SIP gateway 1 has received the 200 OK response from SIP gateway 2.
15	Connect ACK—SIP gateway 2 to PBX B	SIP gateway 2 acknowledges PBX B's Connect message.
		The call session is now active over a two-way voice path via Real-time Transport Protocol (RTP).

At this point, a two-way voice path is established between SIP gateway 1 and PBX A and between SIP gateway 2 and PBX B. A two-way RTP channel is established between SIP gateway 1 and SIP gateway 2.

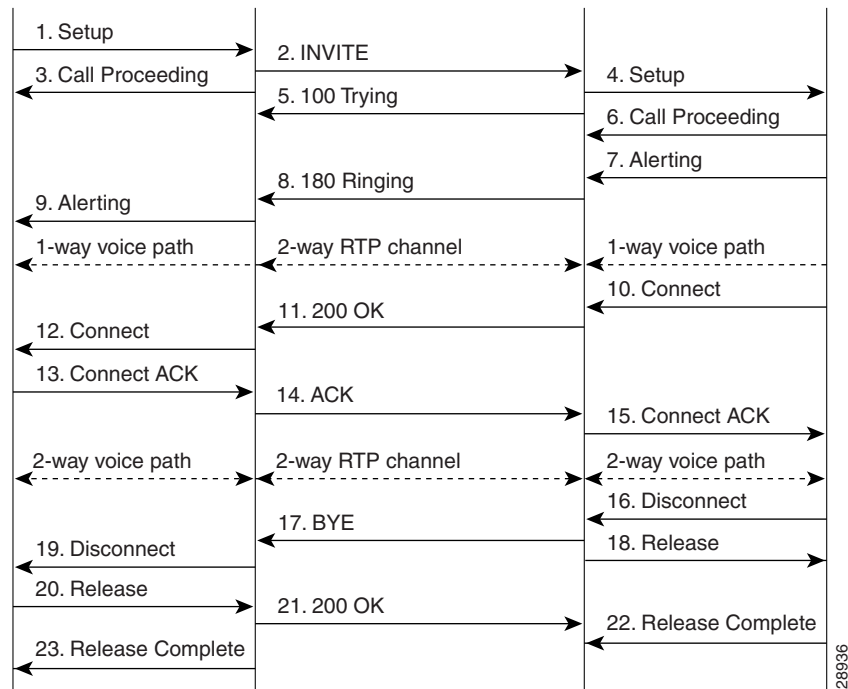| Step	Action	Description
16	Disconnect—PBX B to SIP gateway 2	Once User B hangs up, PBX B sends a Disconnect message to SIP gateway 2. The Disconnect message starts the call session termination process.
17	BYE—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a BYE request to SIP gateway 1. The BYE request indicates that User B wants to release the call. Because it is User B that wants to terminate the call, the Request-URI field is now replaced with PBX A's SIP URL and the From field contains User B's SIP URL. The cseq value is incremented by one.
18	Release—SIP gateway 2 to PBX B	SIP gateway 2 sends a Release message to PBX B.
19	Disconnect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Disconnect message to PBX A.
20	Release—PBX A to SIP gateway 1	PBX A sends a Disconnect message to SIP gateway 1.
21	200 OK—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends a 200 OK response to SIP gateway 2. The 200 OK response notifies SIP gateway 2 that SIP gateway 1 has received the BYE request.
22	Release Complete—PBX B to SIP gateway 2	PBX B sends a Release Complete message to SIP gateway 2.
23	Release Complete—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A and the session is terminated.

SIP Gateway-to-SIP Gateway—Call via SIP Redirect Server

Figure 7-2 illustrates a successful gateway-to-gateway call setup and disconnect via a SIP redirect server. In this scenario, the two end users are identified as User A and User B. User A is located at PBX A. PBX A is connected to SIP gateway 1 via a T1/E1. SIP gateway 1 is using a SIP redirect server. User B is located at PBX B. PBX B is connected to SIP gateway 2 via a T1/E1. User B's phone number is 555-0002. SIP gateway 1 is connected to SIP gateway 2 over an IP network.

The call flow scenario is as follows:

1. User A calls User B via SIP gateway 1 using a SIP redirect server.

2. User B answers the call.

3. User B hangs up.

Figure 7-2   SIP Gateway-to-SIP Gateway—Call via SIP Redirect Server

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.
2	INVITE—SIP gateway 1 to SIP redirect server	SIP gateway 1 sends an INVITE request to the SIP redirect server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: • The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as "INVITE sip:555-0002@companyb.com; user=phone." The "user=phone" parameter distinquishes that the Request-URI address is a telephone number rather than a user name. • PBX A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which SIP gateway 1 is prepared to receive the RTP data is specified.
3	300 Multiple Choice—SIP redirect server to SIP gateway 1	The SIP redirect server sends a 300 Multiple Choice response to SIP gateway 1. The 300 Multiple Choice response indicates that the SIP redirect server accepted the INVITE request, contacted a location server with all or part of User B's SIP URL, and the location server provided a list of alternative locations where User B might be located. The SIP redirect server returns these possible addresses to SIP gateway 1 in the 300 Multiple Choice response.
4	ACK—SIP gateway 1 to SIP redirect server	SIP gateway 1 acknowledges the 300 Multiple Choice response with an ACK.
5	INVITE—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends a new INVITE request to SIP gateway 2. The new INVITE request includes the first contact listed in the 300 Multiple Choice response as the new address for User B, a higher transaction number in the CSeq field, and the same Call-ID as the first INVITE request.
6	Setup—SIP gateway 2 to PBX B	SIP gateway 2 receives the INVITE request from SIP gateway 1 and initiates a Call Setup with User B via PBX B.
7	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.
8	100 Trying—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 100 Trying response to the INVITE request sent by SIP gateway 1. The 100 Trying response indicates that the INVITE request has been received by SIP gateway 2 but that User B has not yet been located.

Step	Action	Description
9	Call Proceeding—PBX B to SIP gateway 2	PBX B sends a Call Proceeding message to SIP gateway 2 to acknowledge the Call Setup request.
10	Alerting—PBX B to SIP gateway 2	PBX B locates User B and sends an Alert message to SIP gateway 2. User B's phone begins to ring.
11	180 Ringing—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 180 Ringing response to SIP gateway 1. The 180 Ringing response indicates that SIP gateway 2 has located, and is trying to alert, User B.
12	Alerting—SIP gateway 1 to PBX A	SIP gateway 1 sends an Alert message to PBX A. User A hears ringback tone.
At this point, a one-way voice path is established between SIP gateway 1 and PBXA and between SIP gateway 2 and PBX B. A two-way RTP channel is established between SIP gateway 1 and SIP gateway 2.		
13	Connect—PBX B to SIP gateway 2	User B answers phone. PBX B sends a Connect message to SIP gateway 2. The Connect message notifies SIP gateway 2 that the connection has been made.
14	200 OK—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 200 OK response to SIP gateway 1. The 200 OK response notifies SIP gateway 1 that the connection has been made.
		If User B supports the media capability advertised in the INVITE message sent by SIP gateway 1, it advertises the intersection of its own and User A's media capability in the 200 OK response. If User B does not support the media capability advertised by User A, it sends back a 400 Bad Request response with a 304 Warning header field.
15	Connect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Connect message to PBX A. The Connect message notifies PBX A that the connection has been made.
16	Connect ACK—PBX A to SIP gateway 1	PBX A acknowledges SIP gateway 1's Connect message.
17	ACK—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an ACK to SIP gateway 2. The ACK confirms that the 200 OK response has been received.
		The call is now in progress over a two-way voice path via RTP.
18	Connect ACK—SIP gateway 2 to PBX B	SIP gateway 2 acknowledges PBX B's Connect message.
At this point, a two-way voice path is established between SIP gateway 1 and PBX A and between SIP gateway 2 and PBX B. A two-way RTP channel is established between SIP gateway 1 and SIP gateway 2.		
19	Disconnect—PBX B to SIP gateway 2	Once User B hangs up, PBX B sends a Disconnect message to SIP gateway 2. The Disconnect message starts the call session termination process.
20	BYE—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a BYE request to SIP gateway 1. The BYE request indicates that User B wants to release the call. Because it is User B that wants to terminate the call, the Request-URI field is now replaced with PBX A's SIP URL and the From field contains User B's SIP URL.
21	Disconnect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Disconnect message to PBX A.
22	Release—SIP gateway 2 to PBX B	SIP gateway 2 sends a Release message to PBX B.

Step	Action	Description
23	Release—PBX A to SIP gateway 1	PBX A sends a Release message to SIP gateway 1.
24	200 OK—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends a 200 OK response to SIP gateway 2. The 200 OK response notifies SIP gateway 2 that SIP gateway 1 has received the BYE request.
25	Release Complete—PBX B to SIP gateway 2	PBX B sends a Release Complete message to SIP gateway 2.
26	Release Complete—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A and the session is terminated.

SIP Gateway-to-SIP Gateway—Call via SIP Proxy Server

Figure 7-3 and Figure 7-4 illustrate a successful gateway-to-gateway call setup and disconnect via a proxy server. In these scenarios, the two end users are User A and User B. User A is located at PBX A. PBX A is connected to SIP gateway 1 via a T1/E1. SIP gateway 1 is using a proxy server. SIP gateway 1 is connected to SIP gateway 2 over an IP network. User B is located at PBX B. PBX B is connected to SIP gateway 2 (a SIP gateway) via a T1/E1. User B's phone number is 555-0002.

In the scenario illustrated by Figure 7-3, the record route feature is enabled on the proxy server. In the scenario illustrated by Figure 7-4, record route is disabled on the proxy server.

When record route is enabled, the proxy server adds the Record-Route header to the SIP messages to ensure that it is in the path of subsequent SIP requests for the same call leg. The Record-Route field contains a globally reachable Request-URI that identifies the proxy server. When record route is enabled, each proxy server adds its Request-URI to the beginning of the list.

When record route is disabled, SIP messages flow directly through the SIP gateways once a call has been established.

The call flow is as follows:

1. User A calls User B via SIP gateway 1 using a proxy server.

2. User B answers the call.

3. User B hangs up.

Figure 7-3   SIP Gateway-to-SIP Gateway—Call via SIP Proxy Server with Record Route Enabled

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.

Step	Action	Description
2	INVITE—SIP gateway 1 to proxy server	SIP gateway 1 sends an INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as "INVITE sip:555-0002@companyb.com; user=phone." The "user=phone" parameter distinquishes that the Request-URI address is a telephone number rather than a user name.
		• PBX A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which SIP gateway 1 is prepared to receive the RTP data is specified.
3	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.
4	INVITE—SIP proxy server to SIP gateway 2	The SIP proxy server checks whether its own address is contained in the Via field (to prevent loops), directly copies the To, From, Call-ID, and Contact fields from the request it received from SIP gateway 1, changes the Request-URI to indicate the server to which it intends to send the INVITE request, and then sends a new INVITE request to SIP gateway 2.
5	100 Trying—SIP proxy server to SIP gateway 1	The SIP proxy server sends a 100 Trying response to SIP gateway 1.
6	Setup—SIP gateway 2 to PBX B	SIP gateway 2 receives the INVITE request from the SIP proxy server and initiates a Call Setup with User B via PBX B.
7	100 Trying—SIP gateway 2 to SIP proxy server	SIP gateway 2 sends a 100 Trying response to the SIP proxy server. The SIP proxy server might or might not forward the 100 Trying response to SIP gateway 1.
8	Call Proceeding—PBX B to SIP gateway 2	PBX B sends a Call Proceeding message to SIP gateway 2 to acknowledge the Call Setup request.
9	Alerting—PBX B to SIP gateway 2	PBX B locates User B and sends an Alert message to SIP gateway 2. User B's phone begins to ring.
10	180 Ringing—SIP gateway 2 to SIP proxy server	SIP gateway 2 sends a 180 Ringing response to the SIP proxy server.
11	180 Ringing—SIP proxy server to SIP gateway 1	The SIP proxy server forwards the 180 Ringing response to SIP gateway 1.

Step	Action	Description
12	Alerting—SIP gateway 1 to PBX A	SIP gateway 1 sends an Alert message to User A via PBX A. The Alert message indicates that SIP gateway 1 has received a 180 Ringing response. User A hears the ringback tone that indicates that User B is being alerted.
	At this point, a one-way voice path is established between SIP gateway 1 and PBX A and between SIP gateway 2 and PBX B. A two-way RTP channel is established between SIP gateway 1 and SIP gateway 2.	
13	Connect—PBX B to SIP gateway 2	User B answers the phone. PBX B sends a Connect message to SIP gateway 2. The connect message notifies SIP gateway 2 that the connection has been made.
14	200 OK—SIP gateway 2 to SIP proxy server	SIP gateway 2 sends a 200 OK response (including the Record-Route header received in the INVITE) to the SIP proxy server. The 200 OK response notifies the SIP proxy server that the connection has been made. If User B supports the media capability advertised in the INVITE message sent by the SIP proxy server, it advertises the intersection of its own and User A's media capability in the 200 OK response. If User B does not support the media capability advertised by User A, it sends back a 400 Bad Request response with a 304 Warning header field. The SIP proxy server must forward 200 OK responses upstream.
15	200 OK—SIP proxy server to SIP gateway 1	The SIP proxy server forwards the 200 OK response that it received from SIP gateway 2 to SIP gateway 1. In the 200 OK response, the SIP proxy server forwards the Record-Route header to ensure that it is in the path of subsequent SIP requests for the same call leg. In the Record-Route field, the SIP proxy server adds its Request-URI.
16	Connect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Connect message to PBX A. The Connect message notifies PBX A that the connection has been made.
17	Connect ACK—PBX A to SIP gateway 1	PBX A acknowledges SIP gateway 1's Connect message.
18	ACK—SIP gateway 1 to SIP proxy server	SIP gateway 1 sends an ACK to the SIP proxy server. The ACK confirms that SIP gateway 1 has received the 200 OK response from the SIP proxy server.
19	ACK—SIP proxy server to SIP gateway 2	Depending on the values in the To, From, CSeq, and Call-ID field, the SIP proxy server might process the ACK locally or proxy it. If the fields in the ACK match those in previous requests processed by the SIP proxy server, the server proxies the ACK. If there is no match, the ACK is proxied as if it were an INVITE request. The SIP proxy server forwards SIP gateway 1's ACK response to SIP gateway 2.
20	Connect ACK—SIP gateway 2 to PBX B	SIP gateway 2 acknowledges PBX B's Connect message. The call session is now active. The 2-way voice path is established directly between SIP gateway 1 and SIP gateway 2; not via the SIP proxy server.
	At this point, a two-way voice path is established between SIP gateway 1 and PBX A and between SIP gateway 2 and PBX B. A two-way RTP channel is established between SIP gateway 1 and SIP gateway 2.	
21	Disconnect—PBX B to SIP gateway 2	After the call is completed, PBX B sends a Disconnect message to SIP gateway 2. The Disconnect message starts the call session termination process.

Step	Action	Description
22	BYE—SIP gateway 2 to SIP proxy server	SIP gateway 2 sends a BYE request to the SIP proxy server. The BYE request indicates that User B wants to release the call. Because it is User B that wants to terminate the call, the Request-URI field is now replaced with PBX A's SIP URL and the From field contains User B's SIP URL.
23	BYE—SIP proxy server to SIP gateway 1	The SIP proxy server forwards the BYE request to SIP gateway 1.
24	Disconnect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Disconnect message to PBX A.
25	Release—SIP gateway 2 to PBX B	After the call is completed, SIP gateway 2 sends a Release message to PBX B.
26	Release—PBX A to SIP gateway 1	PBX A sends a Release message to SIP gateway 1.
27	200 OK—SIP gateway 1 to SIP proxy server	SIP gateway 1 sends a 200 OK response to the SIP proxy server. The 200 OK response notifies SIP gateway 2 that SIP gateway 1 has received the BYE request.
28	200 OK—SIP proxy server to SIP gateway 2	The SIP proxy server forwards the 200 OK response to SIP gateway 2.
29	Release Complete—PBX B to SIP gateway 2	PBX B sends a Release Complete message to SIP gateway 2.
30	Release Complete—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A and the call session is terminated.

Figure 7-4   SIP Gateway-to-SIP Gateway—Call via a Proxy Server with Record Route Disabled

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.

Step	Action	Description
2	INVITE—SIP gateway 1 to SIP proxy server	SIP gateway 1 sends an INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as "INVITE sip:555-0002@companyb.com; user=phone." The "user=phone" parameter distinquishes that the Request-URI address is a telephone number rather than a user name.
		• PBX A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which SIP gateway 1 is prepared to receive the RTP data is specified.
3	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.
4	INVITE—SIP proxy server to SIP gateway 2	The SIP proxy server checks whether its own address is contained in the Via field (to prevent loops), directly copies the To, From, Call-ID, and Contact fields from the request it received from SIP gateway 1, changes the Request-URI to indicate the server to which it intends to send the INVITE request, and then sends a new INVITE request to SIP gateway 2.
5	100 Trying—SIP proxy server to SIP gateway 1	The SIP proxy server sends a 100 Trying response to SIP gateway 1.
6	Setup—SIP gateway 2 to PBX B	SIP gateway 2 receives the INVITE request from the SIP proxy server and initiates a Call Setup with User B via PBX B.
7	100 Trying—SIP gateway 2 to SIP proxy server	SIP gateway 2 sends a 100 Trying response to the SIP proxy server. The SIP proxy server might or might not forward the 100 Trying response to SIP gateway 1.
8	Call Proceeding—PBX B to SIP gateway 2	PBX B sends a Call Proceeding message to SIP gateway 2 to acknowledge the Call Setup request.
9	Alerting—PBX B to SIP gateway 2	PBX B locates User B and sends an Alert message to SIP gateway 2. User B's phone begins to ring.
10	180 Ringing—SIP gateway 2 to SIP proxy server	SIP gateway 2 sends a 180 Ringing response to the SIP proxy server.
11	180 Ringing—SIP proxy server to SIP gateway 1	The SIP proxy server forwards the 180 Ringing response to SIP gateway 1.

Step	Action	Description
12	Alerting—SIP gateway 1 to PBX A	SIP gateway 1 sends an Alert message to User A via PBX A. The Alert message indicates that SIP gateway 1 has received a 180 Ringing response. User A hears the ringback tone that indicates that User B is being alerted.

At this point, a one-way voice path is established between SIP gateway 1 and PBX A and between SIP gateway 2 and PBX B. A two-way RTP channel is established between SIP gateway 1 and SIP gateway 2.

Step	Action	Description
13	Connect—PBX B to SIP gateway 2	User B answers the phone. PBX B sends a Connect message to SIP gateway 2. The connect message notifies SIP gateway 2 that the connection has been made.
14	200 OK—SIP gateway 2 to SIP proxy server	SIP gateway 2 sends a 200 OK response to the SIP proxy server. The 200 OK response notifies the SIP proxy server that the connection has been made.

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

The SIP proxy server must forward 200 OK responses upstream. |
15	200 OK—SIP proxy server to SIP gateway 1	The SIP proxy server forwards the 200 OK response that it received from SIP gateway 2 to SIP gateway 1.
16	Connect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Connect message to PBX A. The Connect message notifies PBX A that the connection has been made.
17	Connect ACK—PBX A to SIP gateway 1	PBX A acknowledges SIP gateway 1's Connect message.
18	ACK—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an ACK to SIP gateway 2. The ACK confirms that SIP gateway 1 has received the 200 OK response from the SIP proxy server.
19	Connect ACK—SIP gateway 2 to PBX B	SIP gateway 2 acknowledges PBX B's Connect message. The call session is now active.

The 2-way voice path is established directly between SIP gateway 1 and SIP gateway 2; not via the SIP proxy server. |

At this point, a two-way voice path is established between SIP gateway 1 and PBX A and between SIP gateway 2 and PBX B. A two-way RTP channel is established between SIP gateway 1 and SIP gateway 2.

Step	Action	Description
20	Disconnect—PBX B to SIP gateway 2	After the call is completed, PBX B sends a Disconnect message to SIP gateway 2. The Disconnect message starts the call session termination process.
21	BYE—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a BYE request to SIP gateway 1. The BYE request indicates that User B wants to release the call. Because it is User B that wants to terminate the call, the Request-URI field is now replaced with PBX A's SIP URL and the From field contains User B's SIP URL.
22	Disconnect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Disconnect message to PBX A.
23	Release—SIP gateway 2 to PBX B	After the call is completed, SIP gateway 2 sends a Release message to PBX B.
24	Release—PBX A to SIP gateway 1	PBX A sends a Release message to SIP gateway 1.

Step	Action	Description
25	200 OK—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends a 200 OK response to SIP gateway 2. The 200 OK response notifies SIP gateway 2 that SIP gateway 1 has received the BYE request.
26	Release Complete—PBX B to SIP gateway 2	PBX B sends a Release Complete message to SIP gateway 2.
27	Release Complete—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A and the call session is terminated.

SIP Gateway-to-SIP Gateway Call—Call Setup with Delayed Media via Third-Party Call Controller

Figure 7-5 illustrates a successful gateway-to-gateway call setup via a third-party call control agent.

The call flow scenario is as follows:

1. The call controller calls User B and then calls User A.

2. User A answers the call.

3. User B answers the call.

4. The call controller connects User A and User B.

Figure 7-5   SIP Gateway-to-SIP Gateway—Call Setup via Third-Party Call Controller

Step	Action	Description
1	INVITE—Call controller to SIP gateway 2	The third party call control agent sends an INVITE request to SIP gateway 2. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as "INVITE sip:555-0002@companyb.com; user=phone." The "user=phone" parameter indicates that the Request-URI address is a telephone number rather than a user name.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The SDP media line is omitted or the INVITE does not contain any SDP information.

Step	Action	Description
2	INVITE—Call controller to SIP gateway 1	The third party call control agent sends an INVITE request to SIP gateway 1. The INVITE request is an invitation to User A to participate in a call session. In the INVITE request: • The phone number of User A is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User A and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User A appears as "INVITE sip:555-0002@companyb.com; user=phone." The "user=phone" parameter indicates that the Request-URI address is a telephone number rather than a user name. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The SDP media line is omitted or the INVITE does not contain any SDP information.
3	Setup—SIP gateway 2 to PBX B	SIP gateway 2 receives the INVITE request from the call controller and initiates a Call Setup with User B via PBX B.
4	Setup—SIP gateway 1 to PBX A	SIP gateway 1 receives the INVITE request from the call controller and initiates a Call Setup with User A via PBX A.
5	100 Trying—SIP gateway 2 to call controller	SIP gateway 2 sends a 100 Trying response to the INVITE request sent by the call controller. The 100 Trying response indicates that the INVITE request has been received by SIP gateway 2 but that User B has not yet been located and that some unspecified action, such as a database consultation, is taking place.
6	Call Proceeding—PBX B to SIP gateway 2	PBX B sends a Call Proceeding message to SIP gateway 2 to acknowledge the Call Setup request.
7	100 Trying—SIP gateway 1 to call controller	SIP gateway 1 sends a 100 Trying response to the INVITE request sent by the call controller. The 100 Trying response indicates that the INVITE request has been received by SIP gateway 2 but that User A has not yet been located and that some unspecified action, such as a database consultation, is taking place.
8	Call Proceeding—PBX A to SIP gateway 1	PBX A sends a Call Proceeding message to SIP gateway 1 to acknowledge the Call Setup request.
9	183 Session Progress—SIP gateway 2 to call controller	SIP gateway 2 sends a 183 Session Progress message to the call controller.
10	183 Session Progress—SIP gateway 1 to call controller	SIP gateway 1 sends a 183 Session Progress message to the call controller.
11	Connect—PBX A to SIP gateway 1	User A answers phone. PBX A sends a Connect message to SIP gateway 1. The Connect message notifies SIP gateway 1 that the connection has been made.
12	200 OK—SIP gateway 1 to call controller	SIP gateway 1 sends a 200 OK response to the call controller. The 200 OK response notifies the call controller that the connection has been made. In the call 200 OK response, the SDP information of User A is specified.

Step	Action	Description
13	Connect ACK—SIP gateway 1 to PBX A	SIP gateway 1 acknowledges PBX A's Connect message.
14	Connect—PBX B to SIP gateway 2	PBX B sends a Connect message to SIP gateway 2. The Connect message notifies SIP gateway 2 that the connection has been made.
15	200 OK—SIP gateway 2 to call controller	SIP gateway 2 sends a 200 OK response to the call controller. The 200 OK response notifies the call controller that the connection has been made. In the call 200 OK response, the SDP information of User B is specified.
16	Connect ACK—SIP gateway 2 to PBX B	SIP gateway 2 acknowledges PBX B's Connect message.
17	ACK—Call controller to SIP gateway 1	The call controller sends an ACK response to SIP gateway 1. The ACK response confirms that the call controller has received the 200 OK response from SIP gateway 1. In the ACK response, the SDP information of User B is specified. Media negotiation takes place.
14	ACK—Call controller to SIP gateway 2	The call controller sends an ACK response to SIP gateway 2. The ACK response confirms that the call controller has received the 200 OK response from SIP gateway 2. In the ACK response, the SDP information of User A is specified. Media negotiation takes place.

At this point, a two-way voice path is established between SIP gateway 1 and PBX A and between SIP gateway 2 and PBX B. A two-way RTP channel is established between SIP gateway 1 and SIP gateway 2.

SIP Gateway-to-SIP Gateway—Call Setup using a FQDN and Delayed Media

Figure 7-6 illustrates a successful gateway-to-gateway call setup using delayed media and a FQDN in the SDP session connection parameter.

Figure 7-6   SIP Gateway-to-SIP Gateway—Call Setup using an FQDN in SDP

Step	Action	Description
1	INVITE—Call controller to SIP gateway 2	The third party call control agent sends an INVITE request to SIP gateway 2. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as "INVITE sip:555-0002@companyb.com; user=phone." The "user=phone" parameter indicates that the Request-URI address is a telephone number rather than a user name.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The SDP media line is omitted or the INVITE does not contain any SDP information.
2	INVITE—Call controller to SIP gateway 1	The third party call control agent sends an INVITE request to SIP gateway 1. The INVITE request is an invitation to User A to participate in a call session.
		In the INVITE request:
		• The phone number of User A is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User A and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User A appears as "INVITE sip:555-0002@companyb.com; user=phone." The "user=phone" parameter indicates that the Request-URI address is a telephone number rather than a user name.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The SDP media line is omitted or the INVITE does not contain any SDP information.
3	Setup—SIP gateway 2 to PBX B	SIP gateway 2 receives the INVITE request from the call controller and initiates a Call Setup with User B via PBX B.
4	Setup—SIP gateway 1 to PBX A	SIP gateway 1 receives the INVITE request from the call controller and initiates a Call Setup with User A via PBX A.
5	100 Trying—SIP gateway 2 to call controller	SIP gateway 2 sends a 100 Trying response to the INVITE request sent by the call controller. The 100 Trying response indicates that the INVITE request has been received by SIP gateway 2 but that User B has not yet been located and that some unspecified action, such as a database consultation, is taking place.
6	Call Proceeding—PBX B to SIP gateway 2	PBX B sends a Call Proceeding message to SIP gateway 2 to acknowledge the Call Setup request.

Step	Action	Description
7	100 Trying—SIP gateway 1 to call controller	SIP gateway 1 sends a 100 Trying response to the INVITE request sent by the call controller. The 100 Trying response indicates that the INVITE request has been received by SIP gateway 2 but that User A has not yet been located and that some unspecified action, such as a database consultation, is taking place.
8	Call Proceeding—PBX A to SIP gateway 1	PBX A sends a Call Proceeding message to SIP gateway 1 to acknowledge the Call Setup request.
9	183 Session Progress—SIP gateway 2 to call controller	SIP gateway 2 sends a 183 Session Progress message to the call controller.
10	183 Session Progress—SIP gateway 1 to call controller	SIP gateway 1 sends a 183 Session Progress message to the call controller.
11	Connect—PBX A to SIP gateway 1	User A answers phone. PBX A sends a Connect message to SIP gateway 1. The Connect message notifies SIP gateway 1 that the connection has been made.
12	200 OK—SIP gateway 1 to call controller	SIP gateway 1 sends a 200 OK response to the call controller. The 200 OK response notifies the call controller that the connection has been made. In the call 200 OK response, the SDP information of User A is specified.
13	Connect ACK—SIP gateway 1 to PBX A	SIP gateway 1 acknowledges PBX A's Connect message.
14	Connect—PBX B to SIP gateway 2	PBX B sends a Connect message to SIP gateway 2. The Connect message notifies SIP gateway 2 that the connection has been made.
15	200 OK—SIP gateway 2 to call controller	SIP gateway 2 sends a 200 OK response to the call controller. The 200 OK response notifies the call controller that the connection has been made. In the call 200 OK response, the SDP information of User B is specified.
16	Connect ACK—SIP gateway 2 to PBX B	SIP gateway 2 acknowledges PBX B's Connect message.
17	ACK—Call controller to SIP gateway 1	The call controller sends an ACK response to SIP gateway 1. The ACK response confirms that the call controller has received the 200 OK response from SIP gateway 1. In the ACK response the media capability of User B is specified and the domain name of gateway 2 is specified in the SDP sessions parameter (c=) field. Media negotiation takes place. At this point, a DNS query is performed by SIP gateway 1 to resolve c=IN IP4 gw2.com.
18	ACK—Call controller to SIP gateway 2	The call controller sends an ACK to SIP gateway 2. The ACK confirms that the call controller has received the ACK response from SIP gateway 2. In the 200 OK response the media capability of User A is specified and the domain name of gateway 1 is specified in the SDP sessions parameter (c=). Media negotiation takes place. At this point, a DNS query is performed by SIP gateway 2 to resolve c=IN IP4 gw1.com.

At this point, a two-way voice path is established between SIP gateway 1 and PBX A and between SIP gateway 2 and PBX B. A two-way RTP channel is established between SIP gateway 1 and SIP gateway 2.

SIP Gateway-to- SIP Gateway Call—Redirection with CC-Diversion

Figure 7-7 illustrates a successful gateway-to-gateway call setup with call redirection with CC-Diversion.

In this scenario, the three end users are identified as Alice at phone A, Bob at phone B, and Carol at phone C. Alice at phone A is located at PBX A. PBX A is connected to SIP gateway 1 via a T1/E1. SIP gateway 1 is using a SIP redirect server. Bob at phone B and Carol at phone C are located at PBX B. PBX B is connected to SIP gateway 2 via a T1/E1. SIP gateway 1 is connected to SIP gateway 2 over an IP network.

The call flow scenario is as follows:

1. Bob at phone B has delegated his calls to Carol at phone C.

1. Alice at phone A initiates a call with Bob via SIP gateway 1 that is using a SIP proxy server.

2. The proxy server returns Carol at SIP gateway 2 as a contact location for Bob.

3. Gateway 1 initiates call with Carol.

4. Carol answers the call.

Figure 7-7   SIP Gateway-to-SIP Gateway—Call Redirection with CC-Diversion

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as Alice at phone A attempts to call Bob at phone B.
2	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.
3	INVITE—SIP gateway 1 to SIP proxy server	SIP gateway 1 sends an INVITE request to the proxy server. The INVITE request is an invitation to Bob to participate in a call session. In the INVITE request: • Bob's phone number is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies Bob's address and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to Bob might appear 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. • Alice (via SIP gateway 1) is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability SIP gateway 1 is ready to receive is specified in the SDP. • The port on which SIP gateway 1 is prepared to receive the RTP data is specified in the SDP. • Alice at SIP gateway 1 is specified as a CC-Diversion header. In addition, the CC-Diversion header field contains a reason for the diversion and a counter. Possible values for the diversion reason include the following: unknown, user-busy, no-answer, unconditional, deflection, and follow-me.
4	302 Moved Temporarily—SIP proxy server to SIP gateway 1	The SIP proxy server determines that Bob's calls have been configured to be redirected to Carol at phone C via SIP gateway 2. The SIP proxy server sends a 302 Moved Temporarily message to SIP gateway 1. In the 302 Moved Temporarily message, Carol at SIP gateway 2 is added as the Contact and there are two CC-Diversion header fields included; one for Bob at GW2 (IP address or domain name) and one for Alice at SIP gateway 1 (IP address or domain name).
5	ACK—SIP gateway 1 to SIP proxy server	SIP gateway 1 sends an ACK to the SIP proxy server. The ACK confirms that the 302 Moved Temporarily response has been received.

Step	Action	Description
6	INVITE—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an INVITE request to Carol at phone C via SIP gateway 2. The INVITE request contains two CC-Diversion headers; one for Bob at SIP gateway 2 (IP address or domain name) and one for Alice at SIP gateway 1 (IP address or domain name).
7	Setup—SIP gateway 2 to PBX B	SIP gateway 2 receives the INVITE request from SIP gateway 1 and initiates a Call Setup with Carol via PBX B. In the Call Setup, the ISDN Redirecting Number IE is generated using the contents of the top CC-Diversion header field; in this case, Bob at SIP gateway 2.
8	Call Proceeding—PBX B to SIP gateway 2	PBX B sends a Call Proceeding message to SIP gateway 2 to acknowledge the Call Setup request.
9	Alerting—PBX B to SIP gateway 2	PBX B locates Carol at phone C and sends an Alert message to SIP gateway 2. Carol's phone begins to ring.
10	180 Ringing—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 180 Ringing response to SIP gateway 1. The 180 Ringing response indicates that SIP gateway 2 has located, and is trying to alert, Carol at phone C.
11	Alerting—SIP gateway 1 to PBX A	SIP gateway 1 sends an Alert message to PBX A. Alice hears ringback tone.

At this point, a one-way voice path is established between SIP gateway 1 and PBXA and between SIP gateway 2 and PBX B. A two-way RTP channel is established between SIP gateway 1 and SIP gateway 2.

Step	Action	Description
12	Connect—PBX B to SIP gateway 2	Carol answers phone. PBX B sends a Connect message to SIP gateway 2. The Connect message notifies SIP gateway 2 that the connection has been made.
13	200 OK—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 200 OK response to SIP gateway 1. The 200 OK response notifies SIP gateway 1 that the connection has been made. If Carol via SIP gateway 2 supports the media capability advertised in the INVITE message sent by SIP gateway 1, it advertises the intersection of its own and Alice's media capability in the 200 OK response. If Carol at SIP gateway 2 does not support the media capability advertised by Alice at SIP gateway 1, SIP gateway 2 sends back a 400 Bad Request response with a "Warning: 304 Codec negotiation failed" header field.
14	Connect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Connect message to PBX A. The Connect message notifies PBX A that the connection has been made.
15	Connect ACK—PBX A to SIP gateway 1	PBX A acknowledges SIP gateway 1's Connect message.
16	ACK—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an ACK to SIP gateway 2. The ACK confirms that the 200 OK response has been received. The call is now in progress over a two-way voice path via RTP.
17	Connect ACK—SIP gateway 2 to PBX B	SIP gateway 2 acknowledges PBX B's Connect message.

At this point, a two-way voice path is established between SIP gateway 1 and PBX A and between SIP gateway 2 and PBX B. A two-way RTP channel is established between SIP gateway 1 and SIP gateway 2.

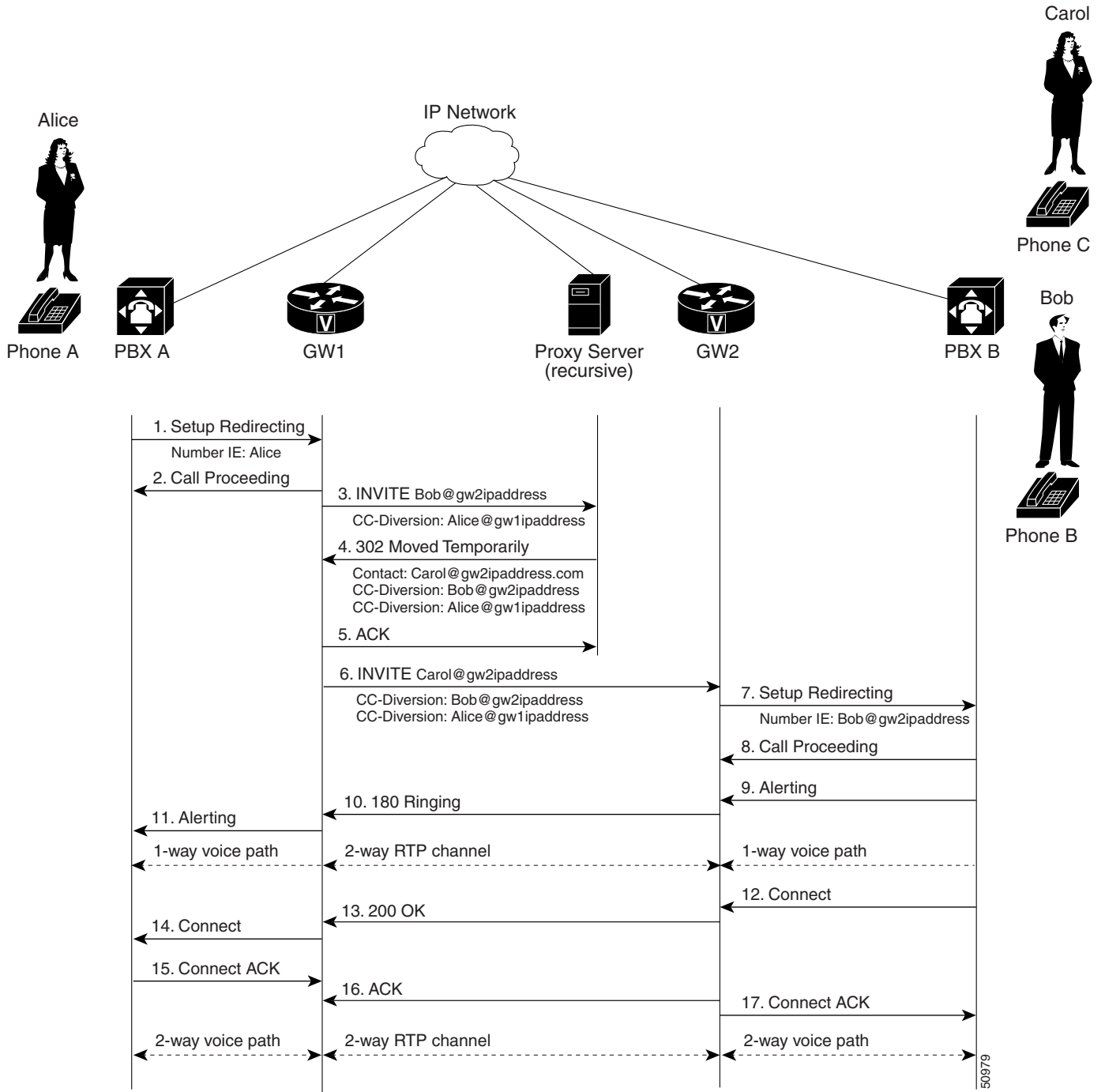# SIP Gateway-to-SIP Gateway Call—SIP 3*xx* Redirection Response

Figure 7-8 illustrates a successful gateway-to-gateway call setup in which a SIP 3xx Redirection response is processed after the receipt of a SIP 18*x* Information response.

In this scenario, the three end users are identified as Alice at phone A, Bob at phone B, and Carol at phone C. Alice at phone A is located at PBX A. PBX A is connected to SIP gateway 1 via a T1/E1. SIP gateway 1 is using a SIP redirect server. Bob at phone B and Carol at phone C are located at PBX B. PBX B is connected to SIP gateway 2 via a T1/E1. SIP gateway 1 is connected to SIP gateway 2 over an IP network.

The call flow scenario is as follows:

1. Bob at phone B has delegated his calls to Carol at phone C.

1. Alice at phone A initiates a call with Bob via SIP gateway 1that is using a SIP proxy server.

2. The proxy server returns Carol at SIP gateway 2 as a contact location for Bob.

3. Gateway 1 initiates call with Carol.

4. Carol answers the call.

Figure 7-8   Gateway-to-Gateway Call—Call Redirection
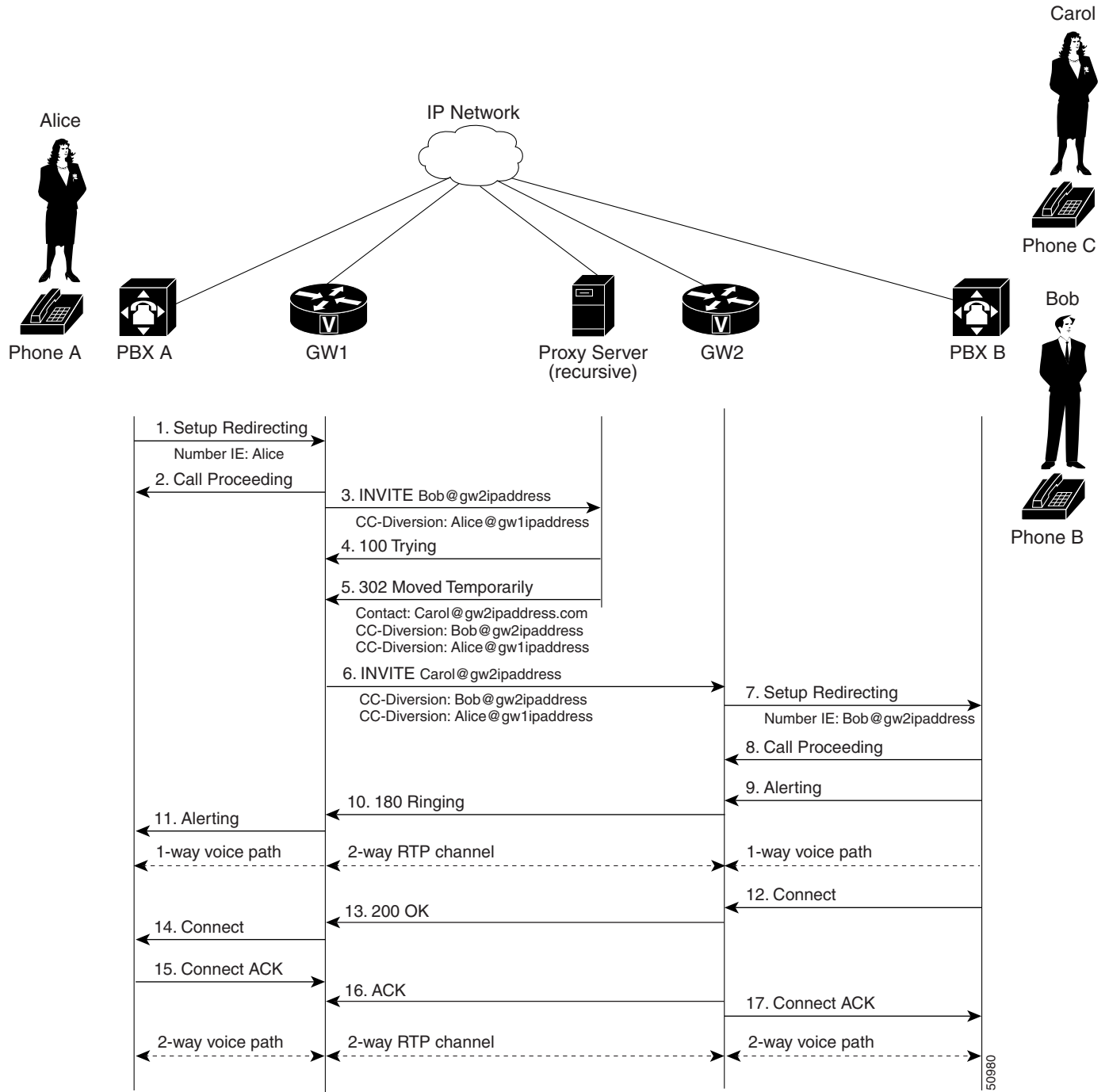
Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as Alice at phone A attempts to call Bob at phone B.

Step	Action	Description
2	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.
3	INVITE—SIP gateway 1 to SIP proxy server	SIP gateway 1 sends an INVITE request to the proxy server. The INVITE request is an invitation to Bob to participate in a call session.
		In the INVITE request:
		• Bob's phone number is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies Bob's address and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to Bob might appear 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.
		• Alice via SIP gateway 1 is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability SIP gateway 1 is ready to receive is specified in the SDP.
		• The port on which SIP gateway 1 is prepared to receive the RTP data is specified in the SDP.
		• Alice at SIP gateway 1 is specified as a CC-Diversion header. In addition, the CC-Diversion header field contains a reason for the diversion and a counter. Possible values for the diversion reason include the following: unknown, user-busy, no-answer, unconditional, deflection, and follow-me.
4	100 Trying—SIP proxy server to SIP gateway 1	The 100 Trying response indicates that the INVITE request has been received.
5	302 Moved Temporarily—SIP proxy server to SIP gateway 1	The SIP proxy server determines that Bob's calls have been configured to be redirected to Carol at phone C via SIP gateway 2. The SIP proxy server sends a 302 Moved Temporarily message to SIP gateway 1.
		In the 302 Moved Temporarily message, Carol at SIP gateway 2 is added as the Contact and there are two CC-Diversion header fields included; one for Alice at SIP gateway 1 (IP address or domain name) and Bob at SIP gateway 2 (IP address or domain name).
6	INVITE—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an INVITE request to Carol at phone C via SIP gateway 2. The INVITE request contains two CC-Diversion headers; one for Alice at SIP gateway 1 (IP address or domain name) and Bob at SIP gateway 2 (IP address or domain name).
7	Setup—SIP gateway 2 to PBX B	SIP gateway 2 receives the INVITE request from SIP gateway 1 and initiates a Call Setup with Carol via PBX B. In the Call Setup, the ISDN Redirecting Number IE is generated using the contents of the top CC-Diversion header field; in this case, Bob at SIP gateway 2.

Step	Action	Description
8	Call Proceeding—PBX B to SIP gateway 2	PBX B sends a Call Proceeding message to SIP gateway 2 to acknowledge the Call Setup request.
9	Alerting—PBX B to SIP gateway 2	PBX B locates Carol at phone C and sends an Alert message to SIP gateway 2. Carol's phone begins to ring.
10	180 Ringing—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 180 Ringing response to SIP gateway 1. The 180 Ringing response indicates that SIP gateway 2 has located, and is trying to alert, Carol at phone C.
11	Alerting—SIP gateway 1 to PBX A	SIP gateway 1 sends an Alert message to PBX A. Alice hears ringback tone.

At this point, a one-way voice path is established between SIP gateway 1 and PBXA and between SIP gateway 2 and PBX B. A two-way RTP channel is established between SIP gateway 1 and SIP gateway 2.

Step	Action	Description
12	Connect—PBX B to SIP gateway 2	Carol answers phone. PBX B sends a Connect message to SIP gateway 2. The Connect message notifies SIP gateway 2 that the connection has been made.
13	200 OK—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 200 OK response to SIP gateway 1. The 200 OK response notifies SIP gateway 1 that the connection has been made.
		If Carol via SIP gateway 2 supports the media capability advertised in the INVITE message sent by SIP gateway 1, it advertises the intersection of its own and Alice's media capability in the 200 OK response. If Carol at SIP gateway 2 does not support the media capability advertised by Alice at SIP gateway 1, SIP gateway 2 sends back a 400 Bad Request response with a "Warning: 304 Codec negotiation failed" header field.
14	Connect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Connect message to PBX A. The Connect message notifies PBX A that the connection has been made.
15	Connect ACK—PBX A to SIP gateway 1	PBX A acknowledges SIP gateway 1's Connect message.
16	ACK—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an ACK to SIP gateway 2. The ACK confirms that the 200 OK response has been received.
		The call is now in progress over a two-way voice path via RTP.
17	Connect ACK—SIP gateway 2 to PBX B	SIP gateway 2 acknowledges PBX B's Connect message.

At this point, a two-way voice path is established between SIP gateway 1 and PBX A and between SIP gateway 2 and PBX B. A two-way RTP channel is established between SIP gateway 1 and SIP gateway 2.

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

Figure 7-9 illustrates a successful gateway-to-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 SIP gateway 1 via a T1/E1. User B is located at a SIP IP phone. SIP gateway 1 is connected to the 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 7-9   SIP Gateway-to-SIP IP Phone—Successful Call Setup and Disconnect

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.

Step	Action	Description
2	INVITE—SIP gateway 1 to SIP IP phone	SIP 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. SIP gateway 1 sends an INVITE request to the address it receives in the dial peer which, in this scenario, is the SIP IP phone. In the INVITE request: • The IP address of the SIP IP phone is inserted in the Request-URI field. • PBX A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified. • The port on which the SIP gateway is prepared to receive the RTP data is specified.
3	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.
4	100 Trying—SIP IP phone to SIP gateway 1	The SIP IP phone sends a 100 Trying response to SIP gateway 1. The 100 Trying response indicates that the INVITE request has been received by the SIP IP phone.
5	180 Ringing—SIP IP phone to SIP gateway 1	The SIP IP phone sends a 180 Ringing response to SIP gateway 1. The 180 Ringing response indicates that the user is being alerted.
6	Alerting—SIP gateway 1 to PBX A	SIP gateway 1 sends an Alert message to User A. The Alert message indicates that SIP gateway 1 has received a 180 Ringing response from the SIP IP phone. User A hears the ringback tone that indicates that User B is being alerted.
7	200 OK—SIP IP phone to SIP gateway 1	The SIP IP phone sends a 200 OK response to SIP gateway 1. The 200 OK response notifies SIP gateway 1 that the connection has been made.
8	Connect—SIP gateway 1 to PBX A	SIP 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 SIP gateway 1	PBX A acknowledges SIP gateway 1's Connect message.
10	ACK—SIP gateway 1 to SIP IP phone	SIP gateway 1 sends an ACK to the SIP IP phone. The ACK confirms that SIP gateway 1 has received the 200 OK response. The call session is now active.
At this point, a two-way voice path is established between SIP gateway 1 and PBX A. A two-way RTP channel is established between SIP gateway 1 and SIP IP phone B.		
11	BYE—SIP IP phone to SIP gateway 1	User B terminates the call session at his SIP IP phone and the phone sends a BYE request to SIP gateway 1. The BYE request indicates that User B wants to release the call.
12	Disconnect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Disconnect message to PBX A.
13	Release—PBX A to SIP gateway 1	PBX A sends a Release message to SIP gateway 1.

Step	Action	Description
14	200 OK—SIP gateway 1 to SIP IP phone	SIP gateway 1 sends a 200 OK response to the SIP IP phone. The 200 OK response notifies the phone that SIP gateway 1 has received the BYE request.
15	Release Complete—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A and the call session is terminated.

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

Figure 7-10 illustrates a successful gateway-to-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 SIP gateway 1 via a T1/E1. User B is located at a SIP IP phone. SIP gateway 1 is connected to the 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 7-10   SIP Gateway-to-SIP IP Phone Call—Successful Call Setup and Call Hold

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.

Step	Action	Description
2	INVITE—SIP gateway 1 to SIP IP phone	SIP 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. SIP gateway 1 sends an INVITE request to the address it receives in the dial peer which, in this scenario, is the SIP IP phone.
		In the INVITE request:
		• The IP address of the SIP IP phone is inserted in the Request-URI field.
		• PBX A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which the SIP gateway is prepared to receive the RTP data is specified.
3	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.
4	100 Trying—SIP IP phone to SIP gateway 1	The SIP IP phone sends a 100 Trying response to SIP gateway 1. The 100 Trying response indicates that the INVITE request has been received by the SIP IP phone.
5	180 Ringing—SIP IP phone to SIP gateway 1	The SIP IP phone sends a 180 Ringing response to SIP gateway 1. The 180 Ringing response indicates that the user is being alerted.
6	Alerting—SIP gateway 1 to PBX A	SIP gateway 1 sends an Alert message to User A. The Alert message indicates that SIP gateway 1 has received a 180 Ringing response from the SIP IP phone. User A hears the ringback tone that indicates that User B is being alerted.
7	200 OK—SIP IP phone to SIP gateway 1	The SIP IP phone sends a 200 OK response to SIP gateway 1. The 200 OK response notifies SIP gateway 1 that the connection has been made.
8	Connect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Connect message to PBX A. The Connect message notifies PBX A that the connection has been made.
9	ACK—SIP gateway 1 to SIP IP phone	SIP gateway 1 sends an ACK to the 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 SIP gateway 1	PBX A acknowledges SIP gateway 1's Connect message.

At this point, a two-way voice path is established between SIP gateway 1 and PBX A. A two-way RTP channel is established between SIP gateway 1 and SIP IP phone B.

Step	Action	Description
11	INVITE—SIP IP phone to SIP gateway 1	SIP IP phone B sends a mid-call INVITE to the SIP gateway with new SDP session parameters (IP address), which are used to place the call on hold.
		The SIP INVITE contains an invalid IP address, which places the call in limbo.
		`SDP: c=IN IP4 0.0.0.0`
12	200 OK—SIP gateway 1 to SIP IP phone	SIP gateway 1 sends a 200 OK response to the SIP IP phone. The 200 OK response notifies the SIP IP phone that the INVITE was successfully processed.

Step	Action	Description
13	ACK—SIP IP phone to SIP gateway 1	The SIP IP phone sends an ACK to SIP gateway 1. The ACK confirms that the SIP IP phone has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.

The two-way RTP channel is torn down. The call is on hold.

Step	Action	Description
14	INVITE—SIP IP phone to SIP gateway 1	SIP IP phone B sends a mid-call INVITE to SIP gateway 1 with the same call ID as the previous INVITE and new SDP session parameters (IP address), which are used to re-establish the call. `SDP: c=IN IP4 IP-UserB`
15	200 OK—SIP gateway 1 to SIP IP phone	SIP gateway 1 sends a 200 OK response to the SIP IP phone. The 200 OK response notifies the SIP IP phone that the INVITE was successfully processed.
16	ACK—SIP IP phone to SIP gateway 1	The SIP IP phone sends an ACK to SIP gateway 1. The ACK confirms that the SIP IP phone has received the 200 OK response. The call session is now active.

At this point, a two-way voice path exists between SIP gateway 1 and PBX A and the two-way RTP channel is re-established between SIP gateway 1 and SIP IP phone B.

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

Figure 7-11 illustrates a successful gateway-to-SIP IP phone 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 SIP gateway 1 via a T1/E1. User B is located at a SIP IP phone and is directly connected to the IP network. User C is located at PBX B. PBX B is connected to SIP gateway 2 via a T1/E1. SIP gateway 1, SIP gateway 2, and the 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 7-11   SIP Gateway-to-SIP IP Phone Call—Successful Call Setup and Transfer without Consultation

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.

Step	Action	Description
2	INVITE—SIP gateway 1 to SIP IP phone	SIP 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. SIP gateway 1 sends an INVITE request to the address it receives in the dial peer which, in this scenario, is the SIP IP phone.
		In the INVITE request:
		• The IP address of the SIP IP phone is inserted in the Request-URI field.
		• PBX A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which the SIP gateway is prepared to receive the RTP data is specified.
3	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.
4	100 Trying—SIP IP phone to SIP gateway 1	The SIP IP phone sends a 100 Trying response to SIP gateway 1. The 100 Trying response indicates that the INVITE request has been received by the SIP IP phone.
5	180 Ringing—SIP IP phone to SIP gateway 1	The SIP IP phone sends a 180 Ringing response to SIP gateway 1. The 180 Ringing response indicates that the user is being alerted.
6	Alerting—SIP gateway 1 to PBX A	SIP gateway 1 sends an Alert message to User A. The Alert message indicates that SIP gateway 1 has received a 180 Ringing response from the SIP IP phone. User A hears the ringback tone that indicates that User B is being alerted.
7	200 OK—SIP IP phone to SIP gateway 1	The SIP IP phone sends a 200 OK response to SIP gateway 1. The 200 OK response notifies SIP gateway 1 that the connection has been made.
8	Connect—SIP gateway 1 to PBX A	SIP 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 SIP gateway 1	PBX A acknowledges SIP gateway 1's Connect message.
10	ACK—SIP gateway 1 to SIP IP phone	SIP gateway 1 sends an ACK to the SIP IP phone. The ACK confirms that SIP gateway 1 has received the 200 OK response. The call session is now active.

At this point, a two-way voice path is established between SIP gateway 1 and PBX A. A two-way RTP channel is established between SIP gateway 1 and SIP IP phone B.
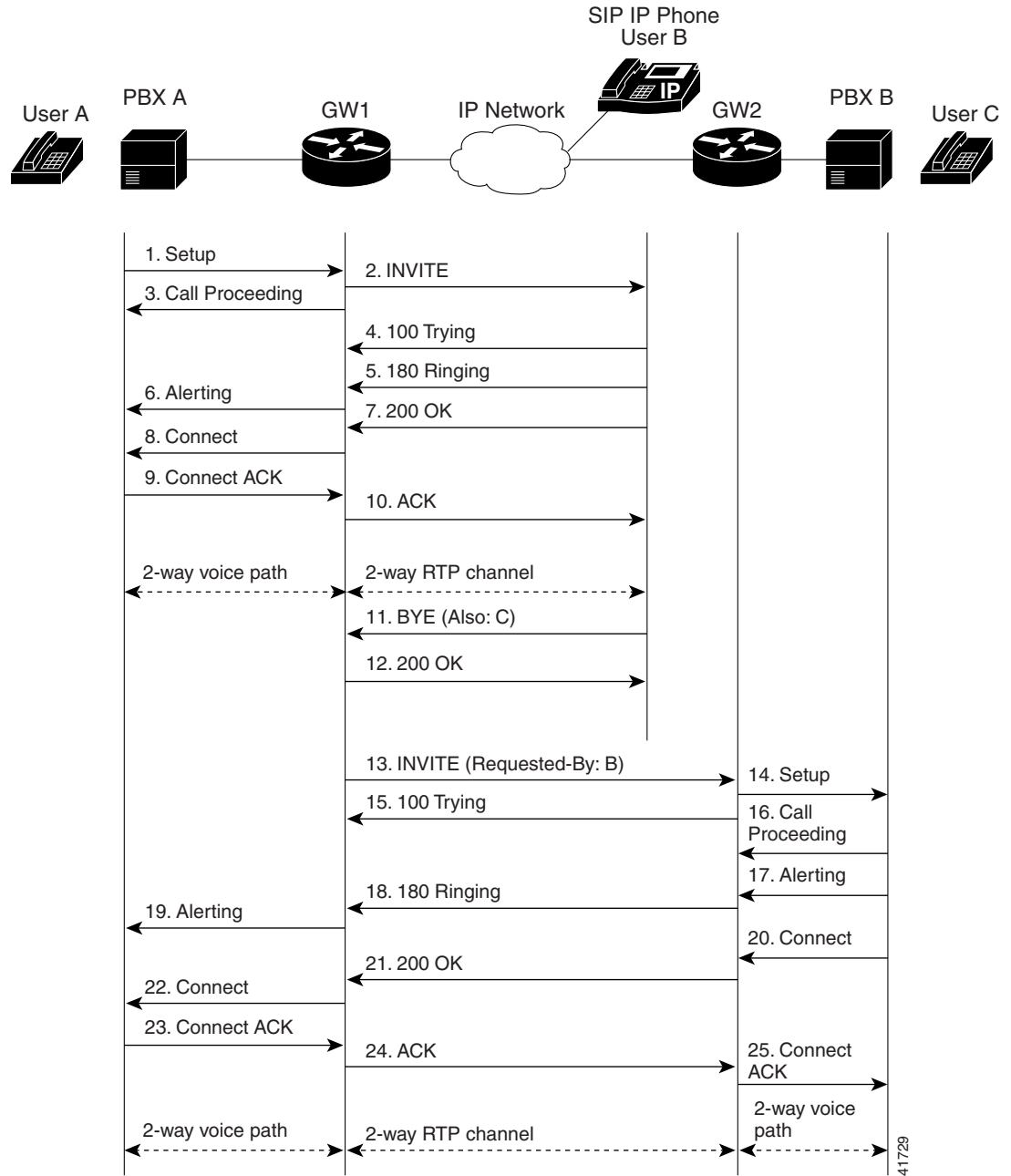
Step	Action	Description
11	BYE—SIP IP phone to SIP gateway 1	User B transfers User A's call to User C and then hangs up. The SIP IP phone sends a BYE request to SIP gateway 1. The BYE request includes the Also header. In this scenario, the Also header indicates that User C must be brought into the call while User B hangs up. This header distinguishes the call transfer BYE request from a normal disconnect BYE request.
		The Request-By header could be included in the BYE request, however, Cisco Systems' 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.
12	200 OK—SIP gateway 1 to SIP IP phone	SIP gateway 1 sends a 200 OK message to the SIP IP phone. The 200 OK response notifies the SIP IP phone that the BYE request has been received. The call session between User A and User B is now terminated.
13	INVITE—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an INVITE request to SIP 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—SIP gateway 2 to PBX B	SIP gateway 2 receives the INVITE request from SIP gateway 1 and initiates a Call Setup with User C via PBX B.
15	100 Trying—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 100 Trying response to the INVITE request sent by SIP gateway 1. The 100 Trying response indicates that SIP gateway 2 has received the INVITE request but that User C has not yet been located.
16	Call Proceeding—PBX B to SIP gateway 2	PBX B sends a Call Proceeding message to SIP gateway 2. User C's phone begins to ring.
17	Alerting—PBX B to SIP gateway 2	PBX B sends an Alert message to SIP gateway 2. The message indicates that the PBX is attempting to alert the user of the call (that is to say, the phone is ringing).
18	180 Ringing—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 180 Ringing response to SIP gateway 1. The 180 Ringing response indicates that SIP gateway 2 has located, and is trying to alert, User C.
19	Alerting—SIP gateway 1 to PBX A	SIP gateway 1 sends an Alert message to PBX A. The Alert message indicates that SIP gateway 1 has received a 180 Ringing response from the SIP IP phone. User A hears the ringback tone that indicates that User C is being alerted.
20	Connect—PBX B to SIP gateway 2	User C answers the phone. PBX B sends a Connect message to SIP gateway 2. The Connect message notifies SIP gateway 2 that the connection has been made.
21	200 OK—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 200 OK response to SIP gateway 1. The 200 OK response notifies SIP 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.
22	Connect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Connect message to PBX A. The Connect message notifies PBX A that the connection has been made.

Step	Action	Description
23	Connect ACK—PBX A to SIP gateway 1	PBX A acknowledges SIP gateway 1's Connect message.
24	ACK—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an ACK to SIP gateway 2. The ACK confirms that SIP gateway 1 has received the 200 OK message from SIP gateway 2.
25	Connect ACK—SIP gateway 2 to PBX B	SIP gateway 2 acknowledges PBX B's Connect message.

At this point, a two-way voice path is established between SIP gateway 1 and PBX A and between SIP gateway 2 and PBX B. A two-way RTP channel is established between SIP gateway 1 and SIP gateway 2.

SIP Gateway-to-uOne Call—Call Setup with Voice Mail

Figure 7-12 illustrates a successful SIP gateway-to-uOne system call setup.

Figure 7-12   SIP Gateway-to-SIP Gateway—Call Setup and Voice Mail
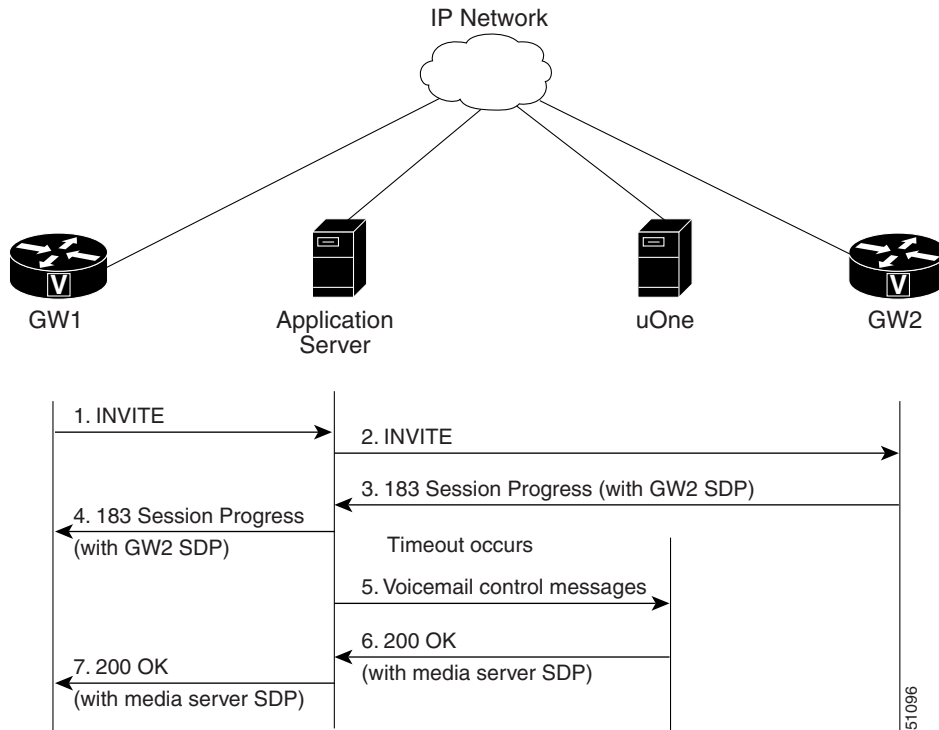
Step	Action	Description
1	INVITE—SIP gateway 1 to application server	SIP gateway 1 sends an INVITE request to the application server.
2	INVITE—Application server to SIP gateway 2	The application server sends the INVITE request to SIP gateway 2.

Step	Action	Description
3	183 Session Progress—SIP gateway 2 to application server	SIP gateway 2 sends a 183 Session Progress message to the application server.
4	183 Session Progress—Application server to SIP gateway 1	The application server proxies the 183 Session Progress message to SIP gateway 1.
At this point, a timeout occurs.		
5	Voice Mail control messages—Application server to uOne server	The application server forwards voice mail control messages to the uOne server (media server).
6	200 OK—uOne server to application server	The uOne server sends a 200 OK response to the application server. In the 200 OK response, the uOne server SDP is included.
7	200 OK response—Application server to SIP gateway 1	The application server proxies the 200 OK response to the SIP gateway. In the 200 OK response, the uOne server SDP is included.

SIP IP Phone-to-SIP Gateway—Automatic Route Selection

Figure 7-13, Figure 7-14, and Figure 7-15 illustrate scenarios in which the SIP Proxy has been configured to use different SIP gateways depending on the destination number.

In the first call flow scenario (Figure 7-13), User A first makes a local call. In the second (Figure 7-14), User A makes a long distance call within the United States. In the third (Figure 7-15), User A makes an international call to France.

Note This call flow requires the appropriate support on the SIP proxy server.

Figure 7-13   SIP IP Phone-to-SIP Gateway—Automatic Route Selection (Local)
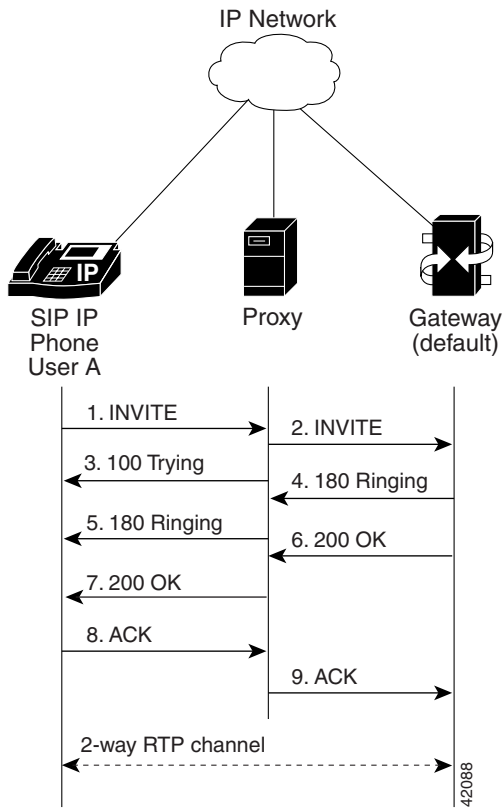
Figure 7-14   SIP IP Phone-to-SIP Gateway—Automatic Route Selection (Long Distance)
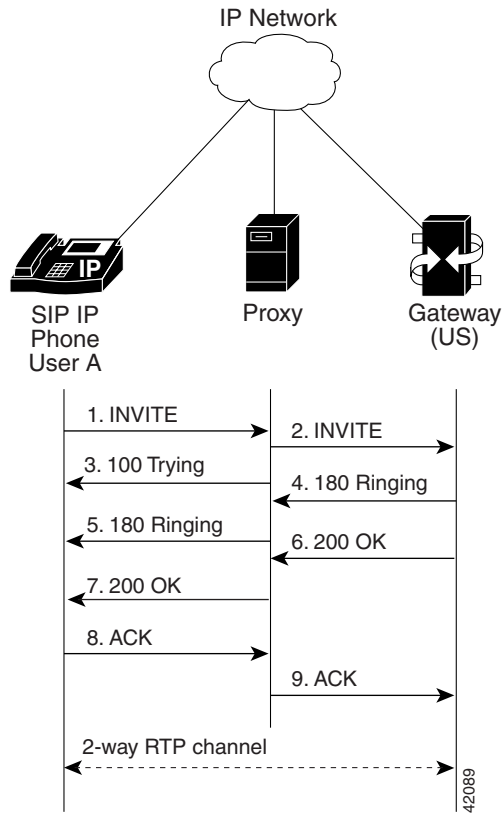
Figure 7-15   SIP IP Phone-to-SIP Gateway—Automatic Route Selection (International)

Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	SIP IP phone A sends an INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
2	INVITE—SIP proxy server to SIP gateway	SIP proxy server reads the invite and, based on the destination number, it sends the SIP INVITE request to the appropriate SIP gateway. For example, in the case of a 9... number, it sends the INVITE to the default SIP gateway. In the case of a 91... number, it sends the INVITE to the SIP gateway configured to handle all long-distance US calls. In the case of a 901133... number, it sends the INVITE to the SIP gateway configured to handle all international calls to France.
3	100 Trying—SIP proxy server to SIP IP phone A	SIP proxy server sends a 100 Trying message to SIP IP phone A.

Step	Action	Description
4	180 Ringing—SIP gateway to SIP proxy server	SIP gateway sends a 180 Ringing response to the SIP proxy server.
5	180 Ringing—SIP proxy server to SIP IP phone A	SIP proxy server sends a 180 Ringing message to SIP IP phone A.
6	200 OK—SIP gateway to SIP proxy server	SIP gateway sends a 200 OK response to the SIP proxy server.
7	200 OK—SIP proxy server to SIP IP phone A	SIP proxy server forwards the 200 OK response to SIP IP phone A.
8	ACK—SIP IP phone A to SIP proxy server	SIP IP phone A sends an ACK to the SIP proxy server. The ACK confirms that the SIP proxy server has received the 200 OK response from SIP IP phone C.
9	ACK—SIP proxy server to SIP gateway	SIP proxy server forwards the SIP ACK to the SIP gateway. The ACK confirms that SIP IP phone A has received the 200 OK response from the SIP gateway.

At this point, a two-way RTP channel is established between SIP IP phone A and the SIP gateway.

SIP IP Phone-to-SIP Gateway—Call Setup and Call Hold with Delayed Media

Figure 7-16 illustrates a successful SIP IP phone-to-SIP gateway call setup and call hold using delayed media.

The call flow scenario is as follows:

1. User A calls User B.
2. User A puts User B on hold.
3. User A takes User B off hold.

Figure 7-16   SIP IP Phone-to-SIP Gateway—Call Setup and Call Hold with Delayed Media
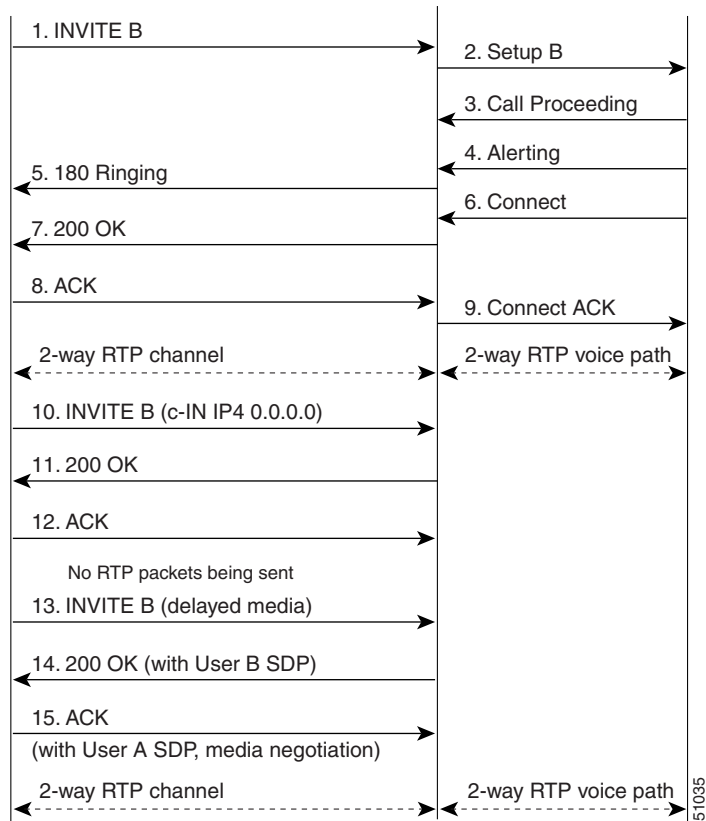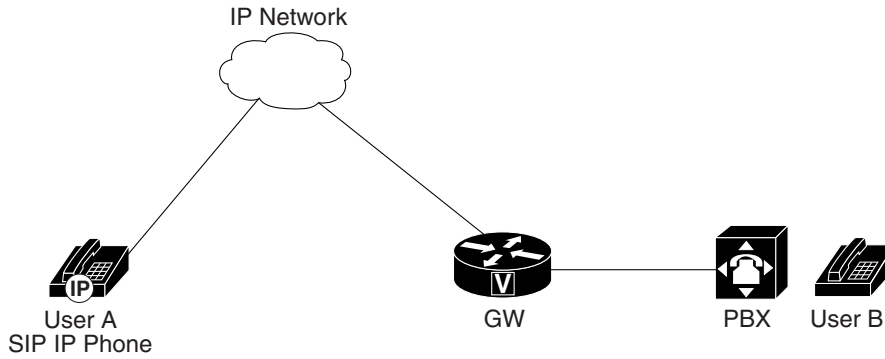
Step	Action	Description
1	INVITE—SIP IP phone to SIP gateway	SIP IP phone sends an INVITE request to the SIP gateway. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as "INVITE sip:555-0002@companyb.com; user=phone." The "user=phone" parameter indicates that the Request-URI address is a telephone number rather than a user name.
		• SIP IP phone is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
2	Setup B—SIP gateway to PBX	The SIP gateway receives the INVITE request from the call controller and initiates a Call Setup with User B via the PBX.
3	Call Proceeding—PBX to SIP gateway	The PBX sends a Call Proceeding message to the SIP gateway to acknowledge the Call Setup request.
4	Alerting—PBX to SIP gateway	The PBX sends an Alert message to the SIP gateway.
5	180 Ringing—SIP gateway to SIP IP phone	The SIP gateway sends a 180 Ringing response to the SIP IP phone. The 180 Ringing response indicates that the User B is being alerted.
6	Connect—PBX to SIP gateway	User B answers the phone. The PBX sends a Connect message to the SIP gateway. The Connect message notifies the SIP gateway that the connection has been made.
7	200 OK—SIP gateway to SIP IP phone	The SIP gateway sends a 200 OK response to the SIP IP phone. The 200 OK response notifies the SIP IP phone that the connection has been made.
8	ACK—SIP IP phone to SIP gateway	SIP IP phone sends an ACK to the SIP gateway. The ACK confirms that the SIP IP phone has received the 200 OK response from the SIP gateway.
9	Connect ACK—SIP gateway to PBX	The SIP gateway acknowledges the PBX's Connect message. The call between User A and User B session is now active.

A two-way RTP channel is established between the SIP IP phone and the SIP gateway. A two-way voice path is established between the SIP gateway and the PBX.

Step	Action	Description
10	INVITE—SIP IP phone to SIP gateway	SIP IP phone (User A) sends a mid-call INVITE request to the SIP gateway with a modified SDP session connection parameter (c=) that places the existing call between User A and User B on hold.
		The c= SDP field of the SIP INVITE contains an 0.0.0.0. This places the call in limbo.

Step	Action	Description
11	200 OK—SIP gateway to SIP IP phone	SIP gateway 1 sends a 200 OK response to the SIP IP phone. The 200 OK response notifies the SIP IP phone that the INVITE was successfully processed.
12	ACK—SIP IP phone to SIP gateway	The SIP IP phone sends an ACK to the SIP gateway. The ACK confirms that the SIP IP phone has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
13	INVITE—SIP IP phone to SIP gateway	SIP IP phone sends an INVITE with delayed media to the SIP gateway. No media is specified in the SDP media name and transport address (m=) parameter.
14	200 OK—SIP gateway to SIP IP phone	The SIP gateway sends a 200 OK response to User A. In the 200 OK response, the SDP information of User B is specified.
15	ACK—SIP IP phone to SIP gateway	SIP IP phone sends an ACK to the SIP gateway. The ACK confirms that the SIP IP phone has received the 200 OK response from the SIP gateway. In the ACK response, the SDP information of User A is specified. Media negotiation takes place.

A two-way RTP channel is re-established between the SIP IP phone and the SIP gateway. A two-way voice path (to User B) is established between the SIP gateway and the PBX.

SIP IP Phone-to-SIP IP Phone—Simple Call Hold

Figure 7-17 illustrates a successful call between 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 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.

Note To simplify the call flow, the intermediate SIP proxy server is not shown.

Figure 7-17   SIP IP Phone-to-SIP IP Phone—Simple Call Hold

Step	Action	Description
1	INVITE—SIP IP phone A to SIP IP phone B	SIP IP phone A sends an INVITE request to SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
2	180 Ringing—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a 180 Ringing response to SIP IP phone A.

Step	Action	Description
3	200 OK—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a 200 OK response to SIP IP phone A. The 200 OK response notifies SIP IP phone A that the connection has been made.
		If SIP IP phone B supports the media capability advertised in the INVITE message sent by SIP IP phone A, it advertises the intersection of its own and SIP IP phone A's media capability in the 200 OK response. If SIP IP phone B does not support the media capability advertised by SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field.
4	ACK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends an ACK to SIP IP phone B. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone B.
At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone B.		
5	INVITE—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a mid-call INVITE to SIP IP phone A with new SDP session parameters (IP address), which are used to place the call on hold.
		The SIP INVITE contains an invalid IP address, which places the call in limbo.
		SDP: c=IN IP4 0.0.0.0
6	200 OK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends a 200 OK response to SIP IP phone B.
7	ACK—SIP IP phone B to SIP IP phone A	SIP IP phone B sends an ACK to SIP IP phone A. The ACK confirms that SIP IP phone B has received the 200 OK response from SIP IP phone A.
The two-way RTP channel is torn down. The call is on hold.		
8	INVITE—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a mid-call INVITE to SIP IP phone A with the same call ID as the previous INVITE and new SDP session parameters (IP address), which are used to re-establish the call.
		SDP: c=IN IP4 181.23.250.2
9	200 OK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends a 200 OK response to SIP IP phone B.
10	ACK—SIP IP phone B to SIP IP phone A	SIP IP phone B sends an ACK to SIP IP phone A. The ACK confirms that SIP IP phone B has received the 200 OK response from SIP IP phone A.
At this point, the two-way RTP channel is re-established between IP phone A and IP phone B.		

SIP IP Phone-to-SIP IP Phone—Call Hold with Consultation

Figure 7-18 illustrates a successful call between 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 SIP IP phones, which are connected via an IP network.
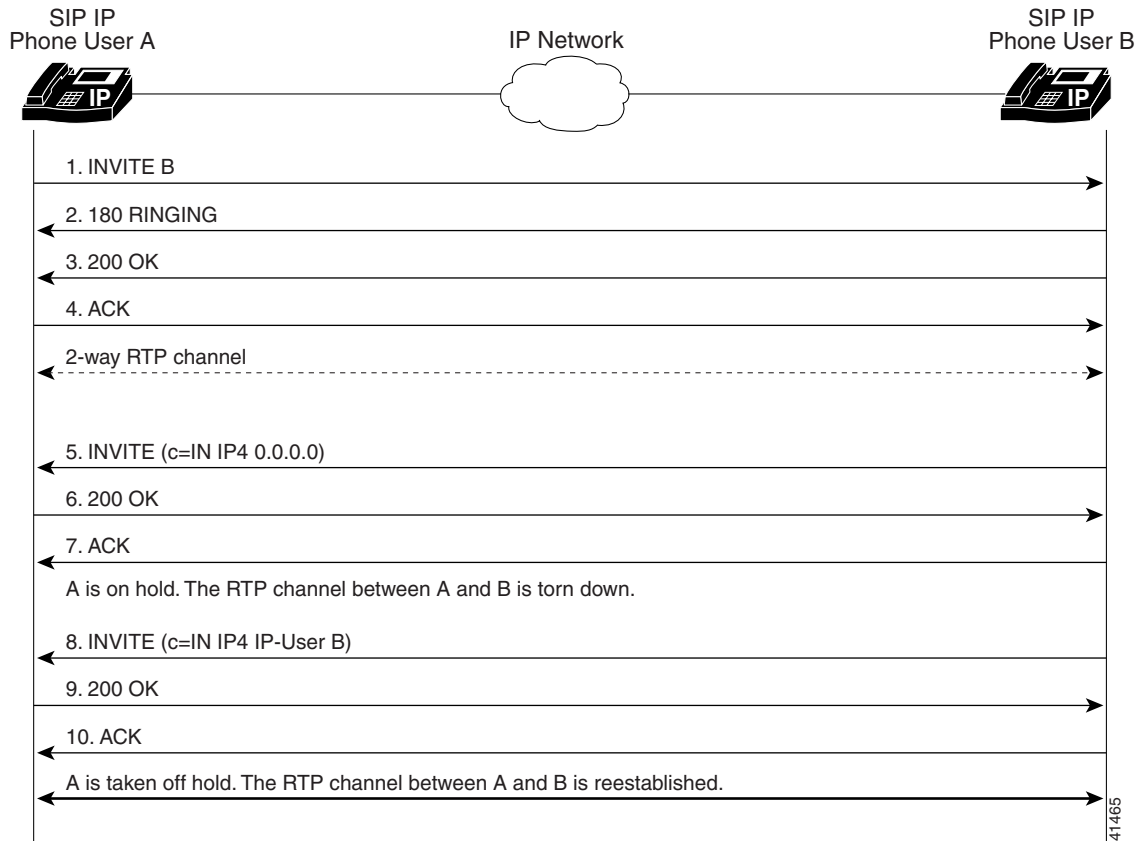
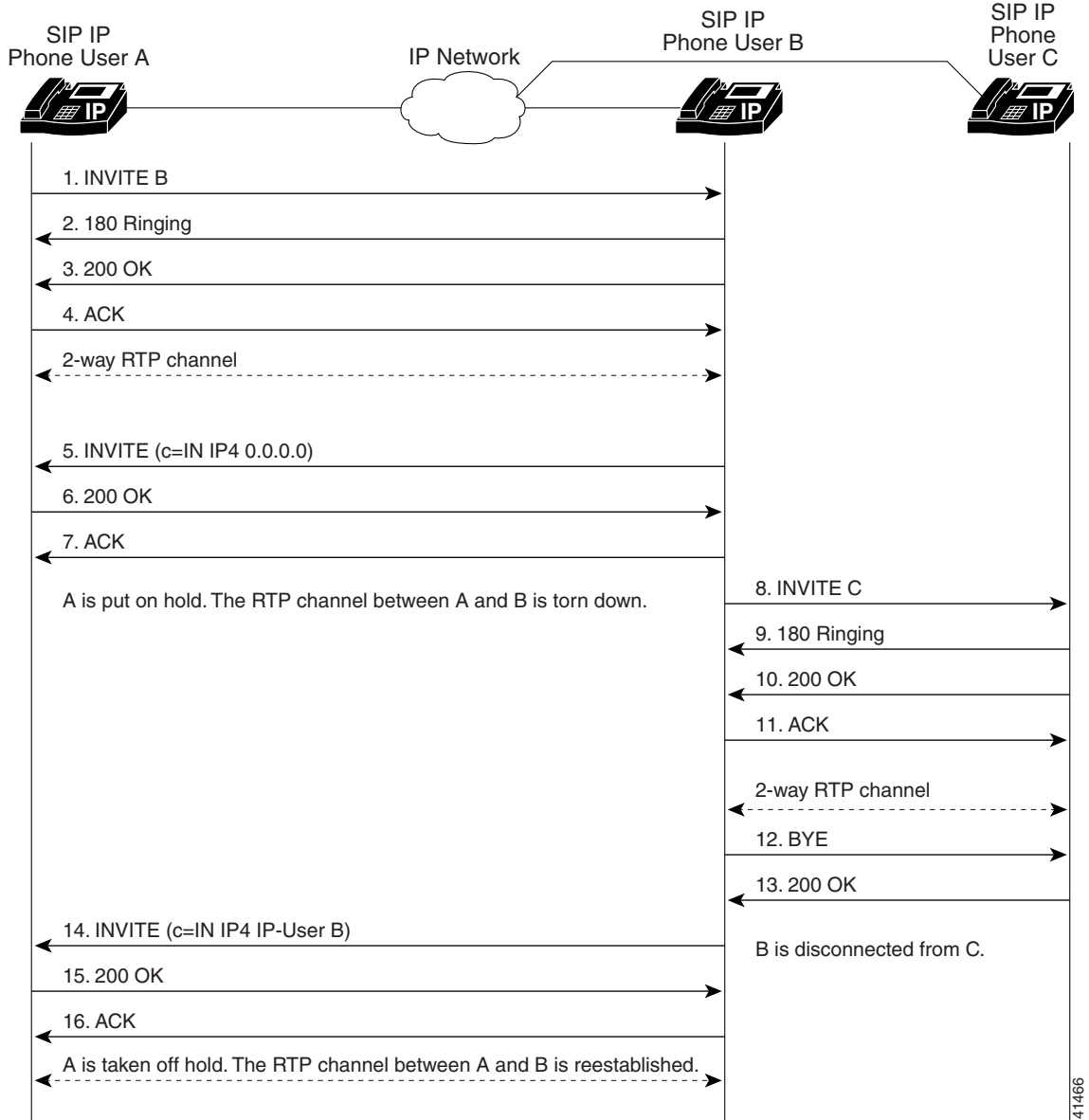The call flow scenario is as follows:

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.

Note   To simplify the call flow, the intermediate SIP proxy server is not shown.

Figure 7-18   SIP IP Phone-to-SIP IP Phone—Call Hold with Consultation

Step	Action	Description
1	INVITE—SIP IP phone A to SIP IP phone B	SIP IP phone A sends an INVITE request to SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
2	180 Ringing—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a 180 Ringing response to SIP IP phone A.
3	200 OK—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a 200 OK response to SIP IP phone A. The 200 OK response notifies SIP IP phone A that the connection has been made.
		If SIP IP phone B supports the media capability advertised in the INVITE message sent by SIP IP phone A, it advertises the intersection of its own and SIP IP phone A's media capability in the 200 OK response. If SIP IP phone B does not support the media capability advertised by SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field.
4	ACK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends an ACK to SIP IP phone B. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone B.
At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone B.		
5	INVITE—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a mid-call INVITE to SIP IP phone A with new SDP session parameters (IP address), which are used to place the call on hold.
		The SIP INVITE contains an invalid IP address, which places the call in limbo.
		`SDP: c=IN IP4 0.0.0.0`
6	200 OK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends a 200 OK response to SIP IP phone B.
7	ACK—SIP IP phone B to SIP IP phone A	SIP IP phone B sends an ACK to SIP IP phone A. The ACK confirms that SIP IP phone B has received the 200 OK response from SIP IP phone A.
The two-way RTP channel is torn down. The call is on hold.		
8	INVITE—SIP IP phone B to SIP IP phone C	SIP IP phone B sends an INVITE request to SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session.
9	180 Ringing—SIP IP phone C to SIP IP phone B	SIP IP phone C sends a 180 Ringing response to SIP IP phone B.

Step	Action	Description
10	200 OK—SIP IP phone C to SIP IP phone B	SIP IP phone C sends a 200 OK response to SIP IP phone B. The 200 OK response notifies SIP IP phone B that the connection has been made.
		If SIP IP phone B supports the media capability advertised in the INVITE message sent by SIP IP phone A, it advertises the intersection of its own and SIP IP phone A's media capability in the 200 OK response. If SIP IP phone B does not support the media capability advertised by SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field.
11	ACK—SIP IP phone B to SIP IP phone C	SIP IP phone B sends an ACK to SIP IP phone C. The ACK confirms that SIP IP phone B has received the 200 OK response from SIP IP phone C.
At this point, a two-way RTP channel is established between SIP IP phone B and SIP IP phone C.		
12	BYE—SIP IP phone B to SIP IP phone C	The call continues and then User B hangs up. SIP IP phone B sends a BYE request to SIP IP phone C. The BYE request indicates that User B wants to release the call.
13	200 OK—SIP IP phone C to SIP IP phone B	SIP IP phone C sends a 200 OK message to SIP IP phone B. The 200 OK response notifies SIP IP phone B that the BYE request has been received. The call session between User A and User B is now terminated.
At this point, the RTP channel between SIP IP phone C and SIP IP phone B is torn down.		
14	INVITE—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a mid-call INVITE to SIP IP phone A with the same call ID as the previous INVITE and new SDP session parameters (IP address), which are used to re-establish the call.
		SDP: c=IN IP4 181.23.250.2
15	200 OK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends a 200 OK response to SIP IP phone B.
16	ACK—SIP IP phone B to SIP IP phone A	SIP IP phone B sends an ACK to SIP IP phone A. The ACK confirms that SIP IP phone B has received the 200 OK response from SIP IP phone A.
At this point, the two-way RTP channel is re-established between SIP IP phone A and SIP IP phone B.		

SIP IP Phone-to-SIP IP Phone—Call Waiting

Figure 7-19 illustrates a successful call between 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 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.

Note   To simplify the call flow, the intermediate SIP proxy server is not shown.

Figure 7-19   SIP IP Phone-to-SIP IP Phone—Call Waiting

Step	Action	Description
1	INVITE—SIP IP phone A to SIP IP phone B	SIP IP phone A sends an INVITE request to SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
2	180 Ringing—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a 180 Ringing response to SIP IP phone A.
3	200 OK—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a 200 OK response to SIP IP phone A. The 200 OK response notifies SIP IP phone A that the connection has been made.
		If SIP IP phone B supports the media capability advertised in the INVITE message sent by SIP IP phone A, it advertises the intersection of its own and SIP IP phone A's media capability in the 200 OK response. If SIP IP phone B does not support the media capability advertised by SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field.
4	ACK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends an ACK to SIP IP phone B. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone B.
At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone B.		
5	INVITE—SIP IP phone C to SIP IP phone B	SIP IP phone C sends an INVITE request to SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.
6	180 Ringing—SIP IP phone B to SIP IP phone C	SIP IP phone B sends a 180 Ringing response to SIP IP phone C.
7	INVITE—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a mid-call INVITE to SIP IP phone A with new SDP session parameters (IP address), which are used to place the call on hold.
		The SIP INVITE contains an invalid IP address, which places the call in limbo.
		`SDP: c=IN IP4 0.0.0.0`
8	200 OK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends a 200 OK response to SIP IP phone B.
9	ACK—SIP IP phone B to SIP IP phone A	SIP IP phone B sends an ACK to SIP IP phone A. The ACK confirms that SIP IP phone B has received the 200 OK response from SIP IP phone A.
The two-way RTP channel is torn down. SIP IP phone A is on hold.		
10	200 OK—SIP IP phone B to SIP IP phone C	SIP IP phone B sends a 200 OK response to SIP IP phone C. The 200 OK response notifies SIP IP phone C that the connection has been made.

Step	Action	Description
11	ACK—SIP IP phone C to SIP IP phone B	SIP IP phone C sends an ACK to SIP IP phone B. The ACK confirms that SIP IP phone C has received the 200 OK response from SIP IP phone B.

At this point, a two-way RTP channel is established between SIP IP phone B and SIP IP phone C. SIP IP phone A remains on hold.

Step	Action	Description
12	INVITE—SIP IP phone B to SIP IP phone C	SIP IP phone B sends a mid-call INVITE to SIP IP phone C with new SDP session parameters (IP address), which are used to place the call on hold. The SIP INVITE contains an invalid IP address, which places the call in limbo. `SDP: c=IN IP4 0.0.0.0`
13	200 OK—SIP IP phone C to SIP IP phone B	SIP IP phone C sends a 200 OK response to SIP IP phone B.
14	ACK—SIP IP phone B to SIP IP phone C	SIP IP phone B sends an ACK to SIP IP phone C. The ACK confirms that SIP IP phone B has received the 200 OK response from SIP IP phone C.

The two-way RTP channel is torn down. SIP IP phone C is on hold.

Step	Action	Description
15	INVITE—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a mid-call INVITE to SIP IP phone A with the same call ID as the previous INVITE (sent to SIP IP phone A) and new SDP session parameters (IP address), which are used to re-establish the call. `SDP: c=IN IP4 181.23.250.2`
16	200 OK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends a 200 OK response to SIP IP phone B.
17	ACK—SIP IP phone B to SIP IP phone A	SIP IP phone B sends an ACK to SIP IP phone A. The ACK confirms that SIP IP phone B has received the 200 OK response from SIP IP phone A.

At this point, the two-way RTP channel is re-established between SIP IP phone A and SIP IP phone B.

Step	Action	Description
18	BYE—SIP IP phone B to SIP IP phone A	The call continues and then User B hangs up. SIP IP phone B sends a BYE request to SIP IP phone A. The BYE request indicates that User B wants to release the call.
19	200 OK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends a 200 OK message to SIP IP phone B. The 200 OK response notifies SIP IP phone B that the BYE request has been received. The call session between User A and User B is now terminated.

At this point, the RTP channel between SIP IP phone A and SIP IP phone B is torn down. SIP IP phone C remains on hold.

Step	Action	Description

20	INVITE—SIP IP phone B to SIP IP phone C	SIP IP phone B sends a mid-call INVITE to SIP IP phone C with the same call ID as the previous INVITE (sent to SIP IP phone C) and new SDP session parameters (IP address), which are used to re-establish the call.
		
		`Call_ID=2`
		`SDP: c=IN IP4 181.23.250.2`

21	200 OK—SIP IP phone C to SIP IP phone B	SIP IP phone C sends a 200 OK response to SIP IP phone B.

Step	Action	Description
22	ACK—SIP IP phone B to SIP IP phone C	SIP IP phone B sends an ACK to SIP IP phone C. The ACK confirms that SIP IP phone B has received the 200 OK response from SIP IP phone A.

At this point, the two-way RTP channel is re-established between SIP IP phone B and SIP IP phone C.

SIP IP Phone-to-SIP IP Phone—Call Transfer without Consultation

Figure 7-20 illustrates a successful call between 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 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.

Note To simplify the call flow, the intermediate SIP proxy server is not shown.

Figure 7-20   SIP IP Phone-to-SIP IP Phone—Call Transfer without Consultation

Step	Action	Description
1	INVITE—SIP IP phone A to SIP IP phone B	SIP IP phone A sends an INVITE request to SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
2	180 Ringing—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a 180 Ringing response to SIP IP phone A.

Step	Action	Description
3	200 OK—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a 200 OK response to SIP IP phone A. The 200 OK response notifies SIP IP phone A that the connection has been made.
		If SIP IP phone B supports the media capability advertised in the INVITE message sent by SIP IP phone A, it advertises the intersection of its own and SIP IP phone A's media capability in the 200 OK response. If SIP IP phone B does not support the media capability advertised by SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field.
4	ACK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends an ACK to SIP IP phone B. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone B.
At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone B. User B then selects the option to transfer the call to User C.	
5	BYE—SIP IP phone B to SIP IP phone A	The SIP BYE request includes the Also header. The Also header indicates that User C must be brought into the call while User B hangs up. This header distinguishes the call transfer BYE request from a normal disconnect BYE request.
6	200 OK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends a 200 OK message to SIP IP phone B. The 200 OK response notifies SIP IP phone B that the BYE request has been received. The call session between User A and User B is now terminated.
At this point, the RTP channel between SIP IP phone A and SIP IP phone B is torn down.	
7	INVITE—SIP IP phone A to SIP IP phone C (Requested by SIP IP phone B)	At the request of SIP IP phone B, SIP IP phone A sends an INVITE request to SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session.
8	180 Ringing—SIP IP phone C to SIP IP phone A	SIP IP phone C sends a 180 Ringing response to SIP IP phone A.
9	200 OK—SIP IP phone C to SIP IP phone A	SIP IP phone C sends a 200 OK response to SIP IP phone A. The 200 OK response notifies SIP IP phone A that the connection has been made.
10	ACK—SIP IP phone A to SIP IP phone C	SIP IP phone A sends an ACK to SIP IP phone C. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.
At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone C.	

SIP IP Phone-to-SIP IP Phone—Call Transfer with Consultation

Figure 7-21 illustrates a successful call between 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 SIP IP phones, which are connected via an IP network.
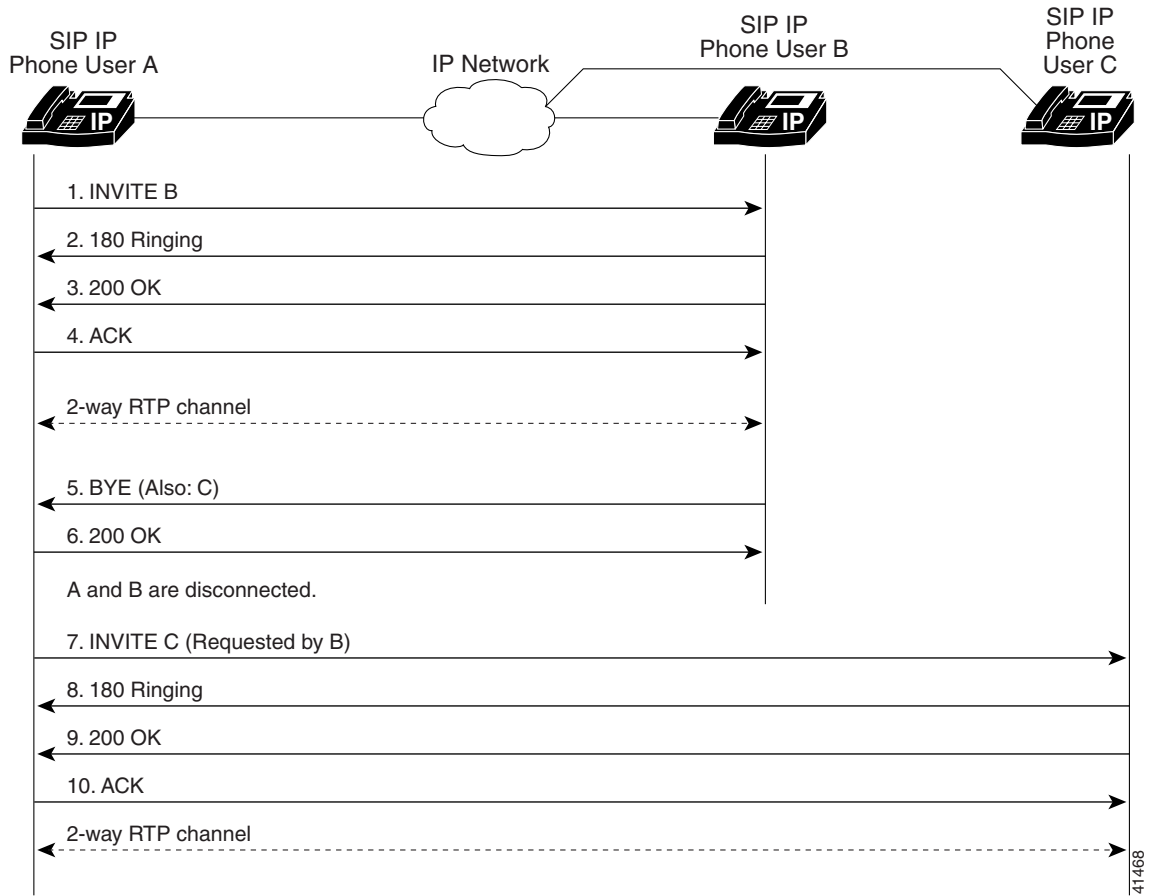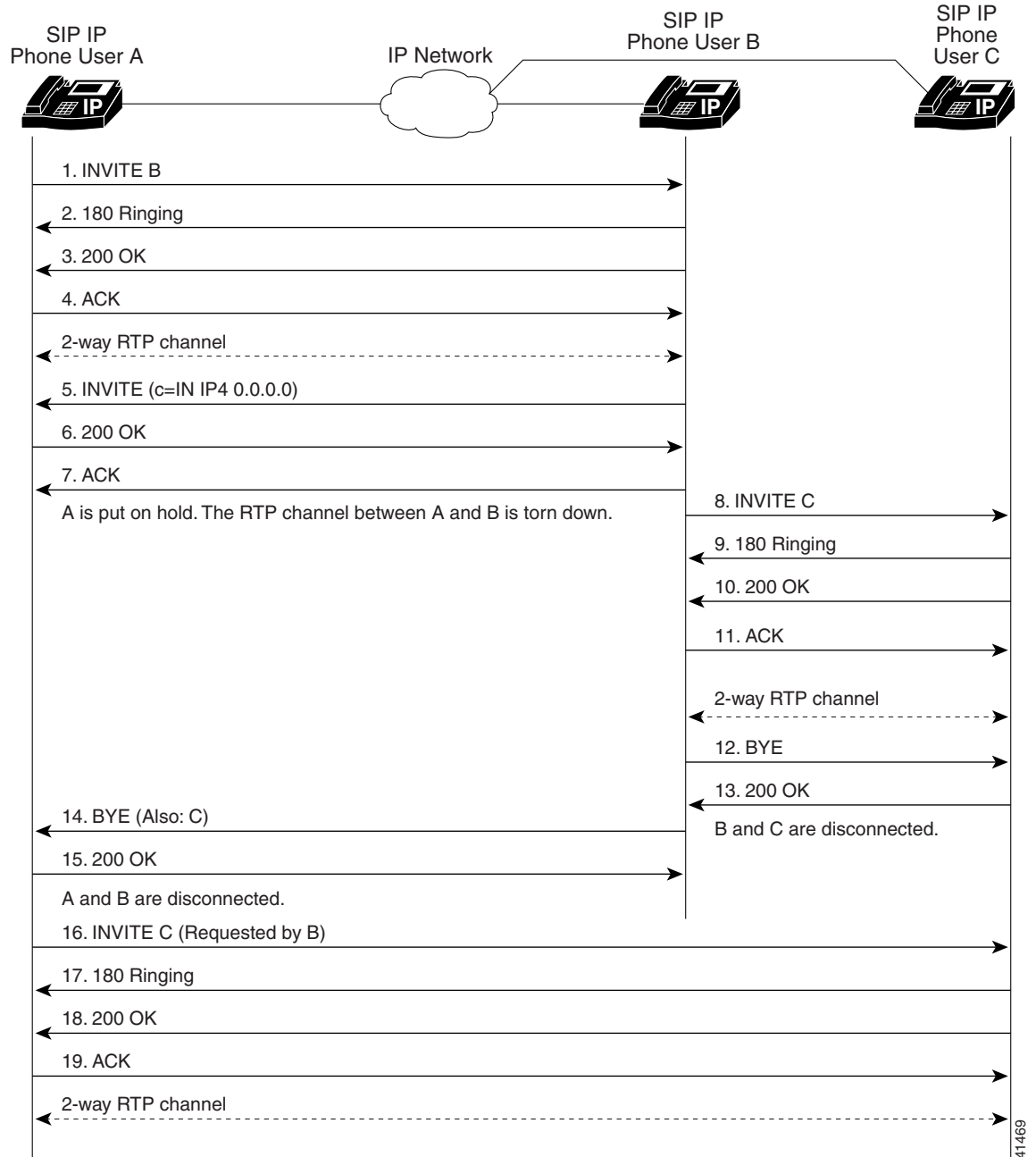
The call flow scenario is as follows:

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.

Note   To simplify the call flow, the intermediate SIP proxy server is not shown.

Figure 7-21   SIP IP Phone-to-SIP IP Phone—Call Transfer with Consultation

Step	Action	Description
1	INVITE—SIP IP phone A to SIP IP phone B	SIP IP phone A sends an INVITE request to SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
2	180 Ringing—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a 180 Ringing response to SIP IP phone A.
3	200 OK—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a 200 OK response to SIP IP phone A. The 200 OK response notifies SIP IP phone A that the connection has been made.
		If SIP IP phone B supports the media capability advertised in the INVITE message sent by SIP IP phone A, it advertises the intersection of its own and SIP IP phone A's media capability in the 200 OK response. If SIP IP phone B does not support the media capability advertised by SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field.
4	ACK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends an ACK to SIP IP phone B. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone B.
At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone B. User B then selects the option to transfer the call to User C.	
5	INVITE—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a mid-call INVITE to SIP IP phone A with new SDP session parameters (IP address), which are used to place the call on hold.
		The SIP INVITE contains an invalid IP address, which places the call in limbo.
		`SDP: c=IN IP4 0.0.0.0`
6	200 OK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends a 200 OK response to SIP IP phone B.
7	ACK—SIP IP phone B to SIP IP phone A	SIP IP phone B sends an ACK to SIP IP phone A. The ACK confirms that SIP IP phone B has received the 200 OK response from SIP IP phone A.
The two-way RTP channel is torn down. The call is on hold.	
8	INVITE—SIP IP phone B to SIP IP phone C	SIP IP phone B sends an INVITE request to SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session.
9	180 Ringing—SIP IP phone C to SIP IP phone B	SIP IP phone C sends a 180 Ringing response to SIP IP phone B.

Step	Action	Description
10	200 OK—SIP IP phone C to SIP IP phone B	SIP IP phone C sends a 200 OK response to SIP IP phone B. The 200 OK response notifies SIP IP phone B that the connection has been made.
		If SIP IP phone B supports the media capability advertised in the INVITE message sent by SIP IP phone A, it advertises the intersection of its own and SIP IP phone A's media capability in the 200 OK response. If SIP IP phone B does not support the media capability advertised by SIP IP phone A, it sends back a 400 Bad Request response with a 304 Warning header field.
11	ACK—SIP IP phone B to SIP IP phone C	SIP IP phone B sends an ACK to SIP IP phone C. The ACK confirms that SIP IP phone B has received the 200 OK response from SIP IP phone C.
At this point, a two-way RTP channel is established between SIP IP phone B and SIP IP phone C.		
12	BYE—SIP IP phone B to SIP IP phone C	The call continues and then User B hangs up. SIP IP phone B sends a BYE request to SIP IP phone C. The BYE request indicates that User B wants to release the call.
13	200 OK—SIP IP phone C to SIP IP phone B	SIP IP phone C sends a 200 OK message to SIP IP phone B. The 200 OK response notifies SIP IP phone B that the BYE request has been received. The call session between User A and User B is now terminated.
At this point, the RTP channel between SIP IP phone B and SIP IP phone C is torn down.		
14	BYE—SIP IP phone B to SIP IP phone A	The SIP BYE request includes the Also header. The Also header indicates that User C must be brought into the call while User B hangs up. This header distinguishes the call transfer BYE request from a normal disconnect BYE request.
15	200 OK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends a 200 OK message to SIP IP phone B. The 200 OK response notifies SIP IP phone B that the BYE request has been received. The call session between User A and User B is now terminated.
At this point, the RTP channel between SIP IP phone A and SIP IP phone B is torn down.		
16	INVITE—SIP IP phone A to SIP IP phone C (Requested by SIP IP phone B)	At the request of SIP IP phone B, SIP IP phone A sends an INVITE request to SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session.
17	180 Ringing—SIP IP phone C to SIP IP phone A	SIP IP phone C sends a 180 Ringing response to SIP IP phone A.
18	200 OK—SIP IP phone C to SIP IP phone A	SIP IP phone C sends a 200 OK response to SIP IP phone A. The 200 OK response notifies SIP IP phone A that the connection has been made.
19	ACK—SIP IP phone A to SIP IP phone C	SIP IP phone A sends an ACK to SIP IP phone C. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.
At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone C.		

SIP IP Phone-to-SIP IP Phone—Network Call Forwarding (Unconditional)

Figure 7-22 illustrates successful call forwarding between 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 SIP IP phone C. In this call flow scenario, the end users are User A, User B, and User C. They are all using SIP IP phones, which are connected via an IP network.

The call flow scenario is as follows:
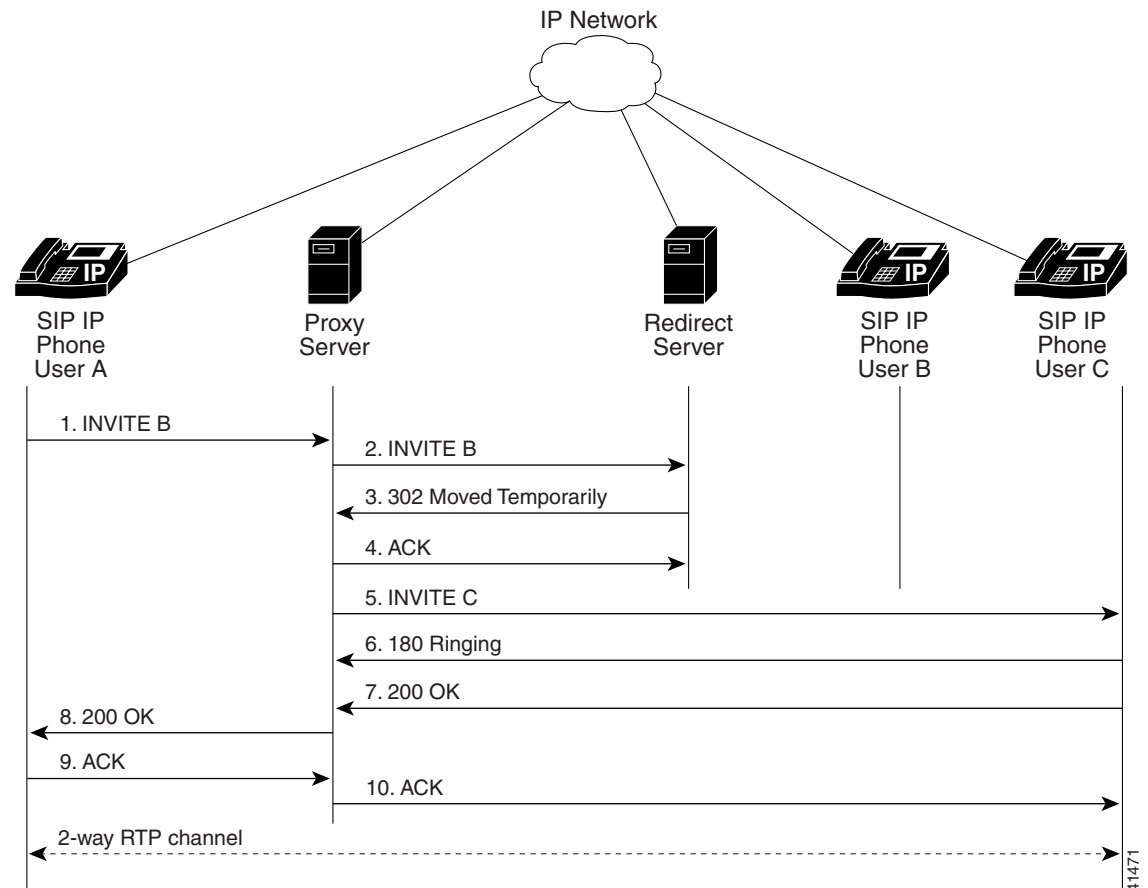
1. User B requests that the network forward all calls to SIP IP phone C.

2. User A calls User B.

3. The SIP proxy and redirect servers transfer the call to SIP IP phone C.

4. User C answers the call.

Note   To simplify the call flow, the intermediate SIP proxy server is not shown.

Figure 7-22   SIP IP Phone-to-SIP IP Phone—Network Call Forwarding (Unconditional)

Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	SIP IP phone A sends an INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: • The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. • SIP IP phone A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified.
2	INVITE—SIP proxy server to SIP redirect server	SIP proxy server sends the SIP INVITE request to the SIP redirect server.
3	302 Moved Temporarily—SIP redirect server to SIP proxy server	SIP redirect server sends a 302 Moved Temporarily message to the SIP proxy server. The message indicates that User B is not available at SIP IP phone B and includes instructions to locate User B at SIP IP phone C.
4	ACK—SIP proxy server to SIP redirect server	The SIP proxy server sends an ACK to the SIP redirect server. The ACK confirms that the 302 Moved Temporarily response has been received.
5	INVITE—SIP proxy server to SIP IP phone C	SIP proxy server sends an INVITE request to SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session.
6	180 Ringing—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 180 Ringing response to the SIP proxy server.
7	200 OK—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 200 OK response to the SIP proxy server.
8	200 OK—SIP proxy server to SIP IP phone A	SIP proxy server forwards the 200 OK response to SIP IP phone A.
9	ACK—SIP IP phone A to SIP proxy server	SIP IP phone A sends an ACK to the SIP proxy server. The ACK confirms that the SIP proxy server has received the 200 OK response from SIP IP phone C.
10	ACK—SIP proxy server to SIP IP phone C	SIP proxy server forwards the SIP ACK to SIP IP phone C. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.

At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone C.

SIP IP Phone-to-SIP IP Phone—Network Call Forwarding (Busy)

Figure 7-23 and Figure 7-24 illustrate successful call forwarding between 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 proxy server tries to place the call to SIP IP phone B and, if the line is busy, the call is transferred to SIP IP phone C. In this call flow scenario, the end users are User A, User B, and User C. They are all using 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 (SIP IP phone B) is busy the network should forward incoming calls to SIP IP phone C.

2. User A calls User B.

3. User B's phone is busy.

4. The SIP proxy and redirect servers transfer the call to SIP IP phone C.

5. User C answers the call.

This section contains two call flows. In the first (Figure 7-23), a SIP redirect server is supplying the alternative addresses. In the second (Figure 7-24), the proxy has been configured with the alternative addresses.

Figure 7-23   SIP IP Phone-to-SIP IP Phone—Network Call Forwarding (Busy) with SIP Redirect Server

Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	SIP IP phone A sends an INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: • The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. • SIP IP phone A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified.

Step	Action	Description
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 300 Multiple choices message to the SIP proxy server. The message indicates that User B can be reached either at SIP IP phone B or SIP IP phone C.
4	ACK—SIP proxy server to SIP redirect server	The SIP proxy server sends an ACK to the SIP redirect server. The ACK confirms that the 300 Multiple Choices response has been received.
5	INVITE—SIP proxy server to SIP IP phone B	SIP proxy server sends an INVITE request to SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.
6	486 Busy Here—SIP IP phone B to SIP proxy server	SIP IP phone B sends a 486 Busy here message to the SIP proxy server. The message indicates that SIP IP phone B is in use and the user is either unwilling or unable to take additional calls.
7	ACK—SIP proxy server to SIP IP phone B	SIP proxy server sends the SIP ACK to SIP IP phone B. The ACK confirms that the SIP Proxy server has received the 486 Busy here response from SIP IP phone B.
8	INVITE—SIP proxy server to SIP IP phone C	SIP proxy server sends an INVITE request to SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session.
9	180 Ringing—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 180 Ringing response to the SIP proxy server
10	200 OK—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 200 OK response to the SIP proxy server.
11	200 OK—SIP proxy server to SIP IP phone A	SIP proxy server forwards the 200 OK response to SIP IP phone A.
12	ACK—SIP IP phone A to SIP proxy server	SIP IP phone A sends an ACK to the SIP proxy server. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.
13	ACK—SIP proxy server to SIP IP phone C	SIP proxy server forwards the SIP ACK to SIP IP phone C. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.

At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone C.

Figure 7-24   SIP IP Phone-to-SIP IP Phone—Network Call Forwarding (Busy) without SIP Redirect Server

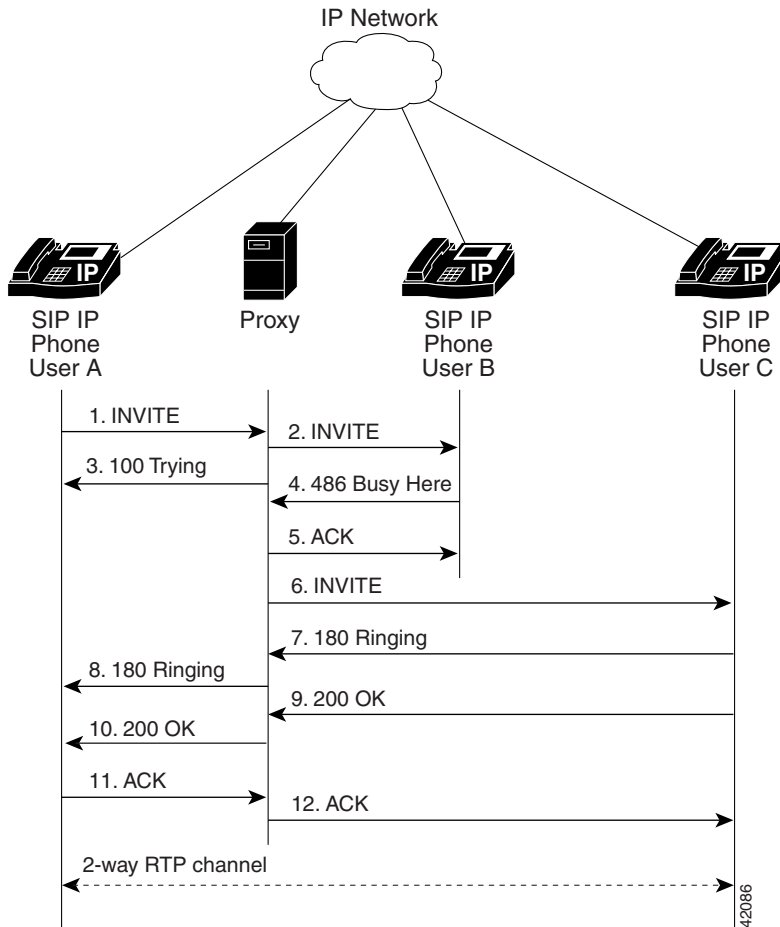| Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	SIP IP phone A sends an INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
2	INVITE—SIP proxy server to SIP IP phone B	SIP proxy server sends an INVITE request to SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.

Step	Action	Description
3	100 Trying—SIP Proxy to SIP IP phone A	SIP Proxy sends a 100 Trying message to SIP IP phone A.
4	486 Busy Here—SIP IP phone B to SIP proxy server	SIP IP phone B sends a 486 Busy here message to the SIP proxy server. The message indicates that SIP IP phone B is in use and the user is either unwilling or unable to take additional calls.
5	ACK—SIP proxy server to SIP IP phone B	SIP proxy server sends the SIP ACK to SIP IP phone B. The ACK confirms that the SIP Proxy server has received the 486 Busy here response from SIP IP phone B.
6	INVITE—SIP proxy server to SIP IP phone C	SIP proxy server sends an INVITE request to SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session.
7	180 Ringing—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 180 Ringing response to the SIP proxy server.
8	180 Ringing—SIP proxy server to SIP IP phone A	SIP proxy server sends a 180 Ringing response to SIP IP phone A.
9	200 OK—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 200 OK response to the SIP proxy server.
10	200 OK—SIP proxy server to SIP IP phone A	SIP proxy server forwards the 200 OK response to SIP IP phone A.
11	ACK—SIP IP phone A to SIP proxy server	SIP IP phone A sends an ACK to the SIP proxy server. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.
12	ACK—SIP proxy server to SIP IP phone C	SIP proxy server forwards the SIP ACK to SIP IP phone C. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.

At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone C.

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

Figure 7-25 and Figure 7-26 illustrate successful call forwarding between 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 SIP IP phone B and, if there is no answer, the call is transferred to SIP IP phone C. In this call flow scenario, the end users are User A, User B, and User C. They are all using 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 (SIP IP phone B) is not answered within a set amount of time the network should forward incoming calls to SIP IP phone C.

2. User A calls User B.

3. User B's phone is not answered.

4. The SIP proxy server transfers the call to SIP IP phone C.

5. User C answers the call.

This section contains two call flows. In the first (Figure 7-25), a SIP redirect server is supplying the alternative addresses. In the second (Figure 7-26), the proxy has been configured with the alternative addresses.

Figure 7-25   SIP IP Phone-to-SIP IP Phone—Network Call Forwarding (No Answer) with SIP Redirect Server

Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	SIP IP phone A sends an INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
2	INVITE—SIP proxy server to SIP redirect server	SIP proxy server sends the SIP INVITE request to the SIP redirect server.
3	300 Multiple Choices—SIP redirect server to SIP proxy server	SIP redirect server sends a 300 Multiple choices message to the SIP proxy server. The message indicates that User B can be reached either at SIP IP phone B or SIP IP phone C.
4	ACK—SIP proxy server to SIP redirect server	The SIP proxy server sends an ACK to the SIP redirect server. The ACK confirms that the 300 Multiple Choices response has been received.
5	INVITE—SIP proxy server to SIP IP phone B	SIP proxy server sends an INVITE request to SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.
6	180 Ringing—SIP IP phone B to SIP proxy server	SIP IP phone B sends a 180 Ringing response to the SIP proxy server.
7	180 Ringing—SIP proxy server to SIP IP phone A	SIP proxy server sends a 180 Ringing response to SIP IP phone A.
At this point, the timeout expires before the phone is answered.		
8	CANCEL (Ring Timeout)—SIP proxy server to SIP IP phone B	SIP proxy server sends a CANCEL request to SIP IP phone B to cancel the invitation.
9	200 OK—SIP IP phone B to SIP proxy server	SIP IP phone B sends a 200 OK response to the SIP proxy server. The response confirms receipt of the cancellation request.
10	INVITE—SIP proxy server to SIP IP phone C	SIP proxy server sends an INVITE request to SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session.
11	180 Ringing—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 180 Ringing response to the SIP proxy server.
12	200 OK—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 200 OK response to the SIP proxy server.
13	200 OK—SIP proxy server to SIP IP phone A	SIP proxy server forwards the 200 OK response to SIP IP phone A.
14	ACK—SIP IP phone A to SIP proxy server	SIP IP phone A sends an ACK to the SIP proxy server. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.

Step	Action	Description
15	ACK—SIP proxy server to SIP IP phone C	SIP proxy server forwards the SIP ACK to SIP IP phone C. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.

At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone C.

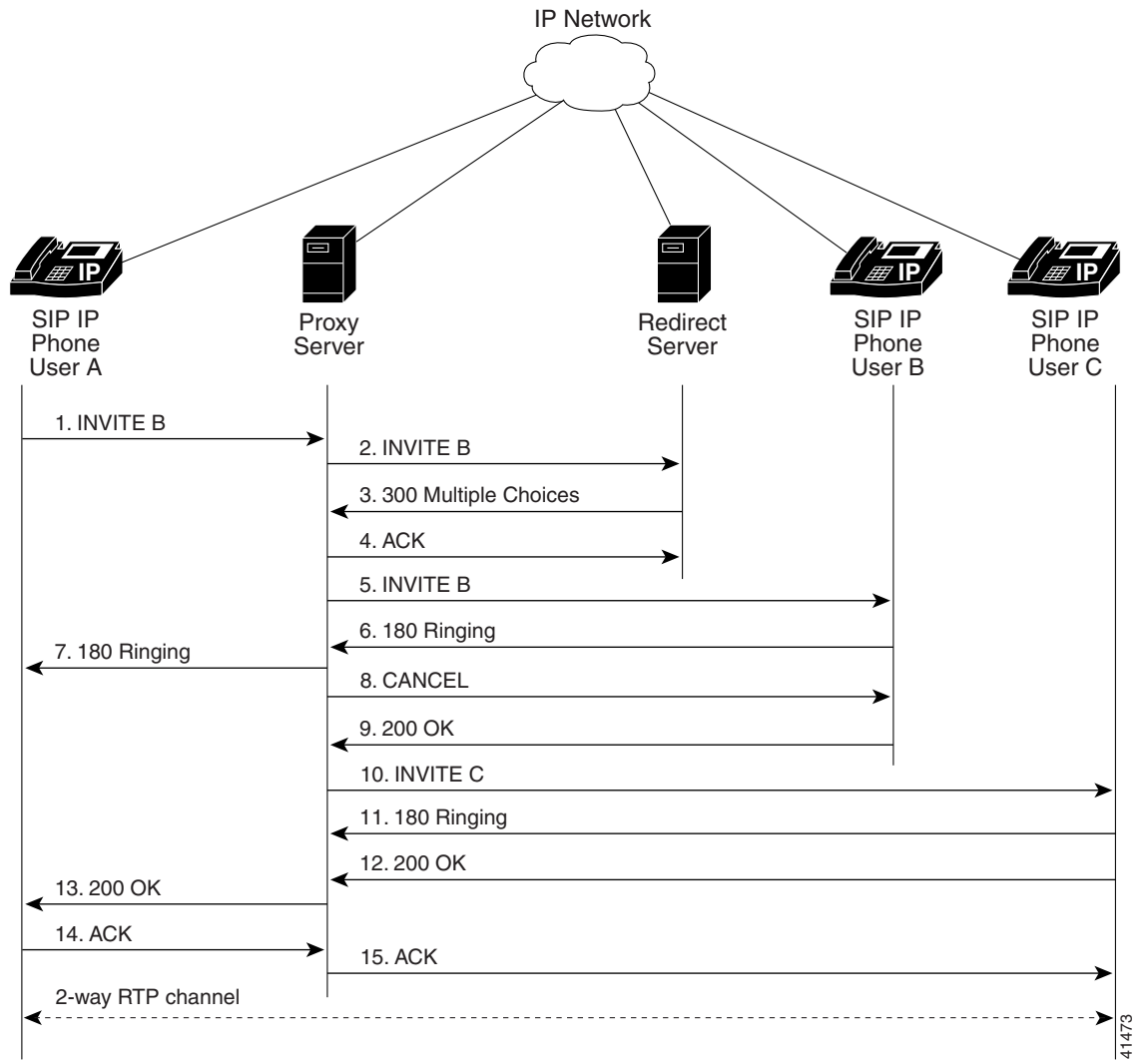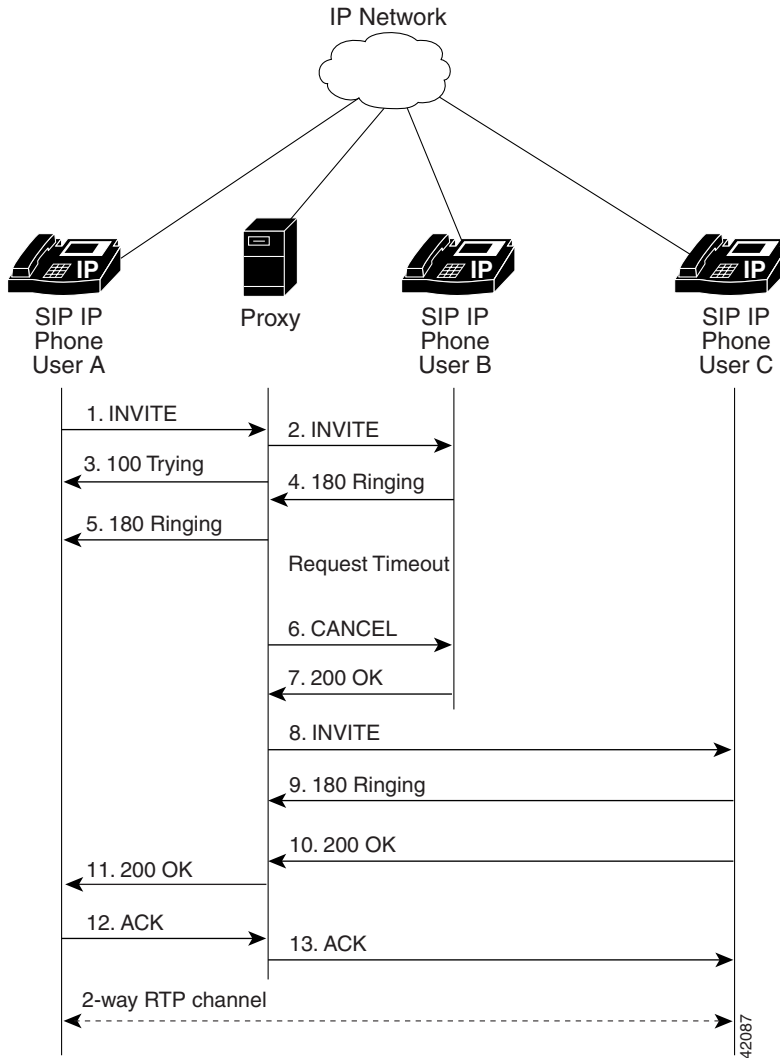*Figure 7-26   SIP IP Phone-to-SIP IP Phone—Network Call Forwarding (No Answer) without SIP Redirect Server*

Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	SIP IP phone A sends an INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.

Step	Action	Description
2	INVITE—SIP proxy server to SIP IP phone B	SIP proxy server sends an INVITE request to SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.
3	100 Trying—SIP Proxy to SIP IP phone A	SIP Proxy sends a 100 Trying message to SIP IP phone A.
4	180 Ringing—SIP IP phone B to SIP proxy server	SIP IP phone B sends a 180 Ringing response to the SIP proxy server.
5	180 Ringing—SIP proxy server to SIP IP phone A	SIP proxy server sends a 180 Ringing response to SIP IP phone A.
At this point, the timeout expires before the phone is answered.		
6	CANCEL (Ring Timeout)—SIP proxy server to SIP IP phone B	SIP proxy server sends a CANCEL request to SIP IP phone B to cancel the invitation.
7	200 OK—SIP IP phone B to SIP proxy server	SIP IP phone B sends a 200 OK response to the SIP proxy server. The response confirms receipt of the cancellation request.
8	INVITE—SIP proxy server to SIP IP phone C	SIP proxy server sends an INVITE request to SIP IP phone C. The INVITE request is an invitation to User C to participate in a call session.
9	180 Ringing—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 180 Ringing response to the SIP proxy server
10	200 OK—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 200 OK response to the SIP proxy server.
11	200 OK—SIP proxy server to SIP IP phone A	SIP proxy server forwards the 200 OK response to SIP IP phone A.
12	ACK—SIP IP phone A to SIP proxy server	SIP IP phone A sends an ACK to the SIP proxy server. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.
13	ACK—SIP proxy server to SIP IP phone C	SIP proxy server forwards the SIP ACK to SIP IP phone C. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.
At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone C.		

SIP IP Phone-to-SIP IP Phone Call Forward Unconditionally

Figure 7-27 and Figure 7-28 illustrate a successful SIP IP phone-to-SIP IP phone call forward unconditionally via a SIP proxy. In these scenarios, the three end users and end points are identified as Alice at SIP IP phone A, Bob at SIP IP phone B, and Carol at SIP IP phone C. Bob's calls are configured to forward to Carol unconditionally. Figure 7-27 illustrates the call as processed by a recursive proxy and Figure 7-28 illustrates the call as processed by a non-recursive proxy.

Figure 7-27 SIP IP Phone-to-SIP IP Phone Call Forward Unconditionally Call Setup via Recursive Proxy

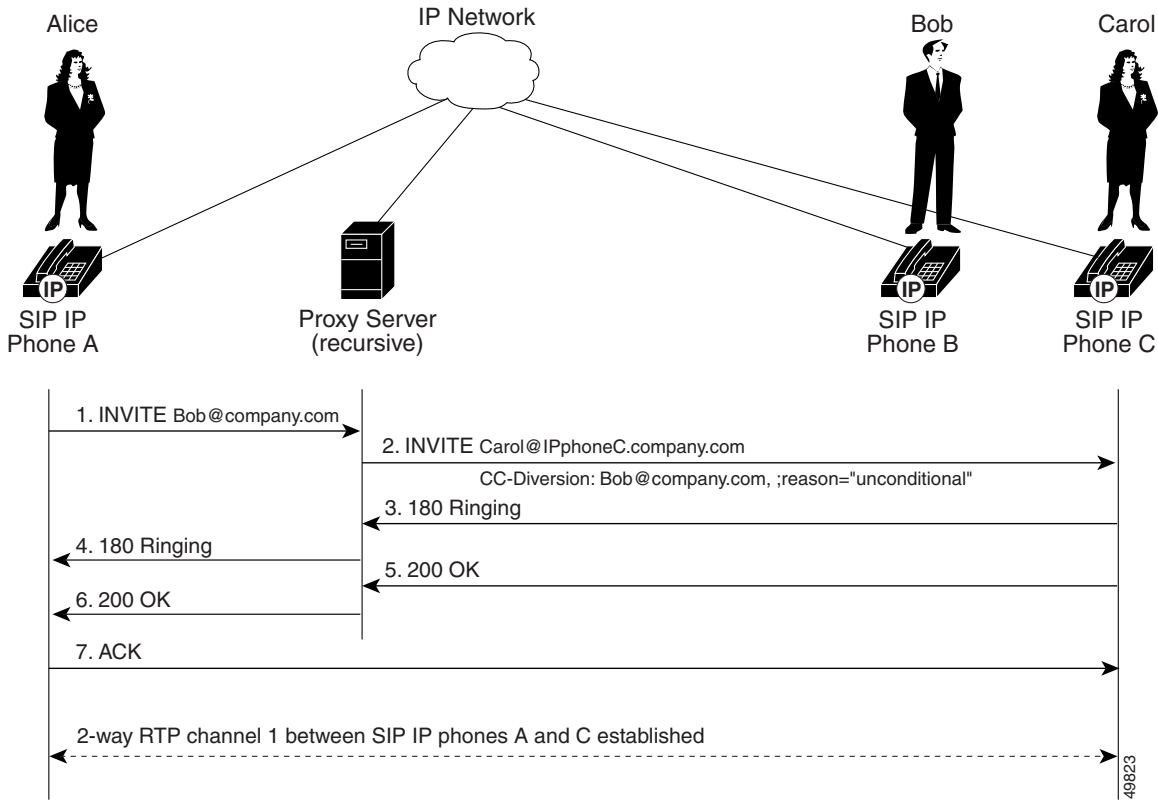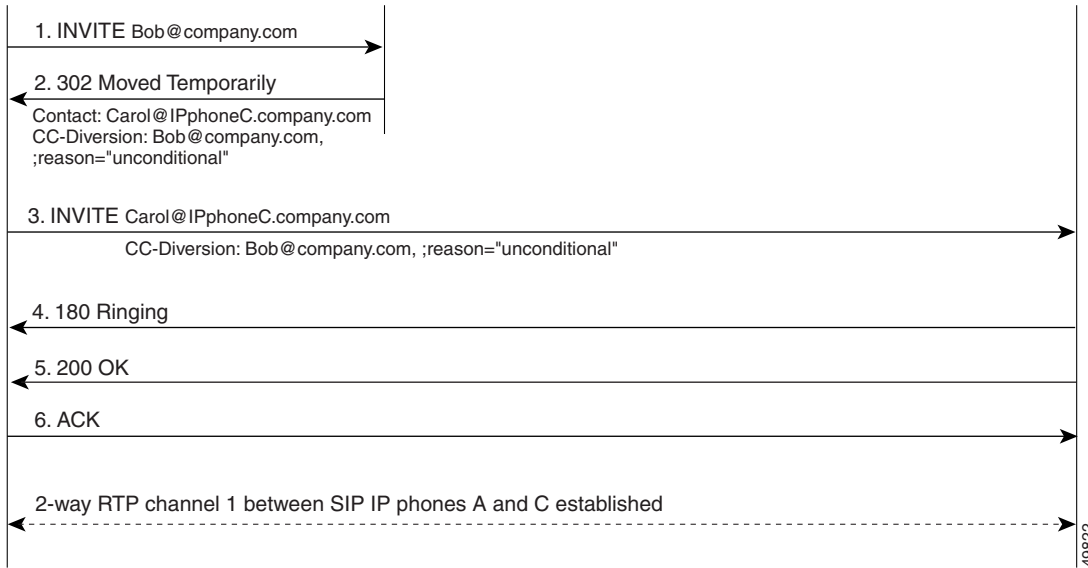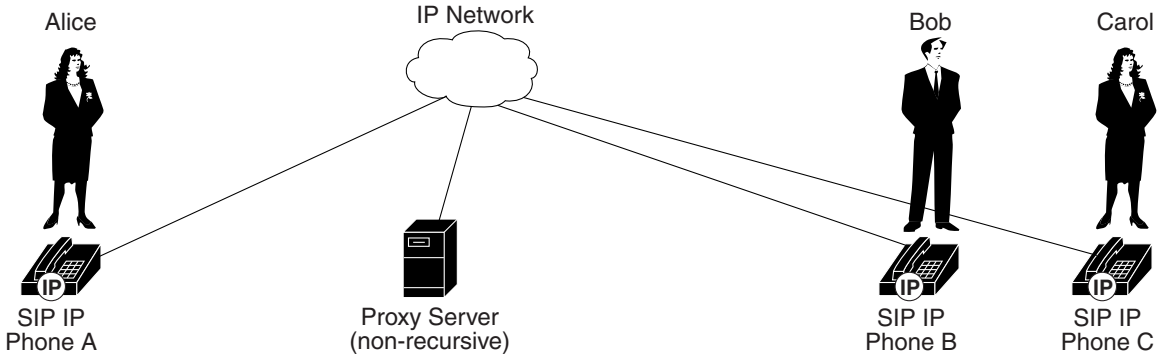| Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	Alice's SIP IP phone A sends an INVITE request to the proxy server. The INVITE request is an invitation to Bob to participate in a call session.
		In the INVITE request:
		• Bob's phone number is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies Bob's address and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to Bob might appear 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.
		• Alice at SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability SIP IP phone A is ready to receive is specified in the SDP.
		• The port on which SIP IP phone A is prepared to receive the RTP data is specified in the SDP.
2	INVITE—SIP proxy server to SIP IP phone C	The SIP proxy server determines that Bob's calls have been configured to forward unconditionally to Carol at SIP IP phone C. The SIP proxy server sends an INVITE request to Carol at SIP IP phone C. In the INVITE request, the proxy server changes the Request-URI to divert the request to Carol at SIP IP phone C and adds a CC-Diversion header containing the Request-URI from the initial INVITE request and the reason for the diversion.
3	180 Ringing—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 180 Ringing response to the SIP proxy server.
4	180 Ringing—SIP proxy server to SIP IP phone A	The SIP proxy server forwards the 180 Ringing response to SIP IP phone A.
5	200 OK—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 200 OK response to SIP IP phone A. The 200 OK response notifies the SIP IP phone A that Carol has answered the phone (for example, the handset of SIP IP phone C went off-hook).
		If SIP IP phone C supports the media capability advertised in the INVITE message sent by the SIP proxy server, it advertises the intersection of its own and SIP IP phone A's media capability in the 200 OK response. If SIP IP phone C does not support the media capability advertised by SIP IP phone A, it sends back a 400 Bad Request response with a "Warning: 304 Codec negotiation failed" header field.
6	ACK—SIP IP phone A to SIP IP phone C	SIP IP phone A sends an ACK to SIP IP phone C. The ACK confirms that User A's SIP IP phone has received the 200 OK response from User C's SIP IP phone.

At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP C phone.

Figure 7-28   SIP IP Phone-to-SIP IP Phone Call Forward Unconditionally via Non-recursive Proxy

Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	Alice's SIP IP phone A sends an INVITE request to the proxy server. The INVITE request is an invitation to Bob to participate in a call session.
		In the INVITE request:
		• Bob's phone number is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies Bob's address and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to Bob might appear 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.
		• Alice at SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability SIP IP phone A is ready to receive is specified in the SDP.
		• The port on which SIP IP phone A is prepared to receive the RTP data is specified in the SDP.
2	302 Moved Temporarily—SIP proxy server to SIP IP phone A	The SIP proxy server determines that Bob's calls have been configured to forward unconditionally to Carol at SIP IP phone C. The SIP proxy server sends a 302 Moved Temporarily message to SIP IP phone A.
		In the 302 Moved Temporarily message, Carol at SIP IP phone C is added as the Contact and a CC-Diversion header is added that contains the Request-URI from the initial INVITE and the reason for the diversion.
3	INVITE—SIP IP phone A to SIP IP phone C	SIP IP phone A sends an INVITE request to Carol at SIP IP phone C. The INVITE request contains a CC-Diversion header that contains the Request-URI from the initial INVITE request and the reason for the diversion.
4	180 Ringing—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 180 Ringing response to SIP IP phone A.
5	200 OK—SIP IP phone C to SIP IP phone A	SIP IP phone C sends a 200 OK response to SIP IP phone A. The 200 OK response notifies the SIP IP phone A that Carol has answered the phone (for example, the handset of SIP IP phone C went off-hook).
		If SIP IP phone C supports the media capability advertised in the INVITE message sent by the SIP proxy server, it advertises the intersection of its own and SIP IP phone A's media capability in the 200 OK response. If SIP IP phone C does not support the media capability advertised by SIP IP phone A, it sends back a 400 Bad Request response with a "Warning: 304 Codec negotiation failed" header field.

Step	Action	Description
6	ACK—SIP IP phone A to SIP IP phone C	SIP IP phone A sends an ACK to SIP IP phone C. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.

At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone C.

SIP IP Phone-to-SIP IP Phone Call Forward on Busy

Figure 7-29 and Figure 7-30 illustrate a successful SIP IP phone-to-SIP IP phone call forward on busy via a SIP proxy. In these scenarios, the three end users are identified as User A, User B, and User C. User B's calls are configured to forward to User C when User B's SIP IP phone sends a 486 Busy Here response. Figure 7-29 illustrates the call as processed by a recursive proxy and Figure 7-30 illustrates the call as processed by a non-recursive proxy.

Figure 7-29   SIP IP Phone-to-SIP IP Phone Call Forward on Busy Call Setup via Recursive Proxy

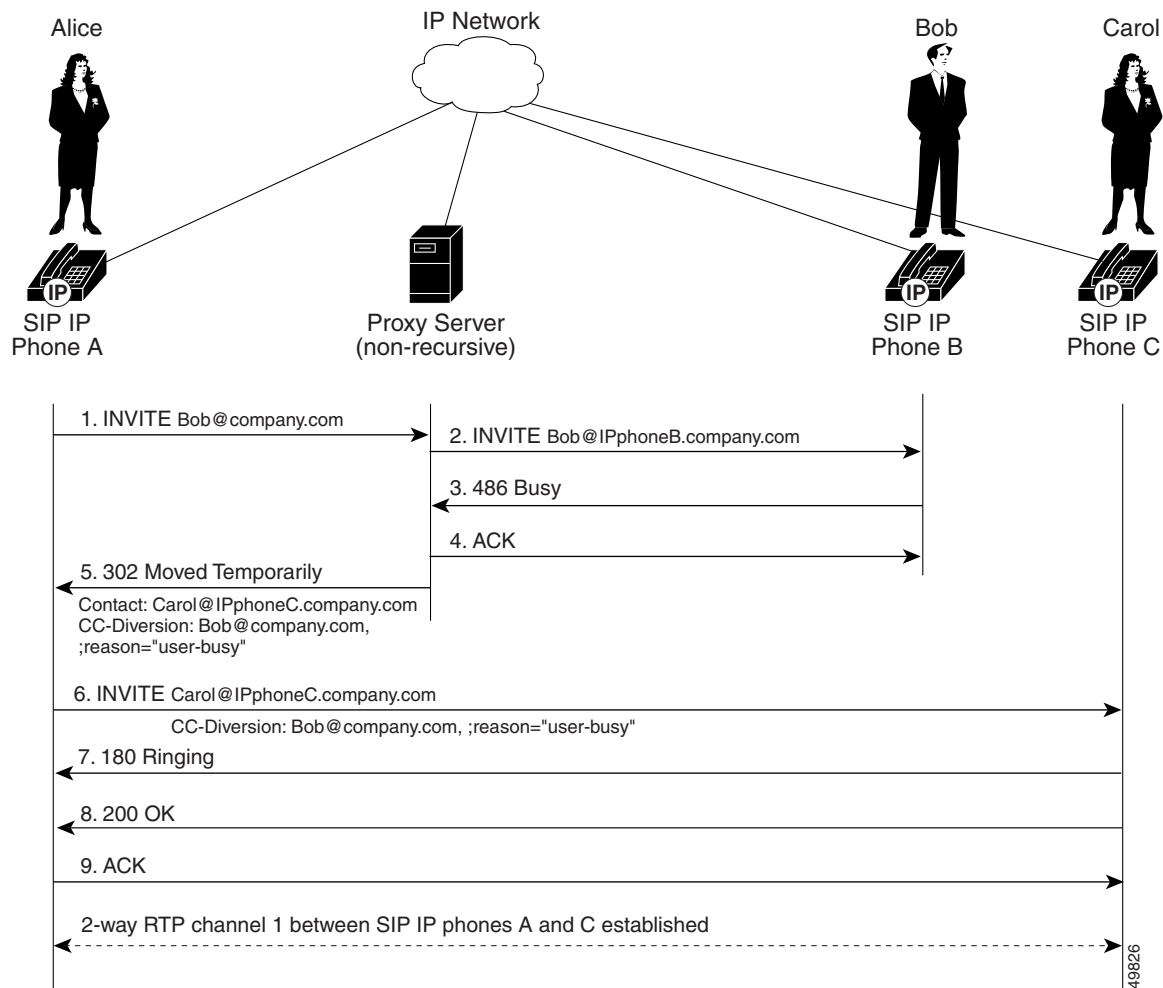| Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	Alice's SIP IP phone A sends an INVITE request to the proxy server. The INVITE request is an invitation to Bob to participate in a call session.
		In the INVITE request:
		• Bob's phone number is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies Bob's address and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to Bob might appear 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.
		• Alice at SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability SIP IP phone A is ready to receive is specified in the SDP.
		• The port on which SIP IP phone A is prepared to receive the RTP data is specified in the SDP.
2	INVITE—SIP proxy server to SIP IP phone B	The proxy server forwards the INVITE request to Bob at SIP IP phone B.
3	486 Busy Here—SIP IP phone B to the SIP proxy server	SIP IP phone B sends a 486 Busy response to the SIP proxy server. The 486 Busy Here response is a client error response that indicates that Bob at SIP IP phone B was successfully contacted but Bob was either unwilling or unable to take another call.
4	ACK—SIP proxy server to SIP IP phone B	The SIP proxy server sends an ACK to SIP IP phone B. The ACK confirms that the 486 Busy Here response has been received.
5	INVITE—SIP proxy server to SIP IP phone C	The SIP proxy server sends an INVITE request to Carol at SIP IP phone C to which Bob's calls have been configured to forward on busy. In the INVITE request, the proxy server changes the Request-URI to divert the request to Carol at SIP IP phone C and adds a CC-Diversion header containing the Request-URI from the initial INVITE request and the reason for the diversion.
6	180 Ringing—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 180 Ringing response to the SIP proxy server.
7	180 Ringing—SIP proxy server to SIP IP phone A	The SIP proxy server forwards the 180 Ringing response to SIP IP phone A.

Step	Action	Description
8	200 OK—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 200 OK response to SIP IP phone A.
		If SIP IP phone C supports the media capability advertised in the INVITE message sent by the SIP proxy server, it advertises the intersection of its own and SIP IP phone A's media capability in the 200 OK response. If SIP IP phone C does not support the media capability advertised by SIP IP phone A, it sends back a 400 Bad Request response with a "Warning: 304 Codec negotiation failed" header field.
9	200 OK—SIP proxy server to SIP IP phone A.	The SIP proxy server forwards the 200 OK response to SIP IP phone A. The 200 OK response notifies the SIP IP phone A that Carol has answered the phone (for example, the handset of SIP IP phone C went off-hook).
10	ACK—SIP IP phone A to SIP IP phone C	SIP IP phone A sends an ACK to SIP IP phone C. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.

At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone C.

Figure 7-30   SIP IP Phone-to-SIP IP Phone Call Forward on Busy Call Setup via Non-recursive Proxy

Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	Alice's SIP IP phone A sends an INVITE request to the proxy server. The INVITE request is an invitation to Bob to participate in a call session. In the INVITE request: • Bob's phone number is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies Bob's address and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to Bob might appear 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. • Alice at SIP IP phone A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability SIP IP phone A is ready to receive is specified in the SDP. • The port on which SIP IP phone A is prepared to receive the RTP data is specified in the SDP.
2	INVITE—SIP proxy server to SIP IP phone B	The SIP proxy server forwards the INVITE request to Bob at SIP IP phone B.
3	486 Busy Here—SIP IP phone B to the SIP proxy server	SIP IP phone B sends a 486 Busy response to the SIP proxy server. The 486 Busy Here response is a client error response that indicates that Bob at SIP IP phone B phone was successfully contacted but Bob was either unwilling or unable to take another call.
4	ACK—SIP proxy server to SIP IP phone B	The SIP proxy server sends an ACK to SIP IP phone B. The ACK confirms that the 486 Busy Here response has been received.
5	302 Moved Temporarily—SIP proxy server to SIP IP phone A	The SIP proxy server sends a 302 Moved Temporarily message to SIP IP phone A. In the 302 Moved Temporarily message, Carol at SIP IP phone C is added as the Contact and a CC-Diversion header is added that contains the Request-URI from the initial INVITE and the reason for the diversion.
6	INVITE—SIP proxy server to SIP IP phone C	The SIP proxy server sends an INVITE request to Carol at SIP IP phone C to which Bob's calls have been configured to forward on busy. In the INVITE request, the proxy server changes the Request-URI to divert the request to Carol at SIP IP phone C and adds a CC-Diversion header containing the Request-URI from the initial INVITE request and the reason for the diversion.
7	180 Ringing—SIP IP phone C to SIP IP phone A	SIP IP phone C sends a 180 Ringing response to SIP IP phone A.

Step	Action	Description
8	200 OK—SIP IP phone C to SIP IP phone A	SIP IP phone C sends a 200 OK response to SIP IP phone A. The 200 OK response notifies the SIP IP phone A that Carol has answered the phone (for example, the handset of SIP IP phone C went off-hook).
		If SIP IP phone C supports the media capability advertised in the INVITE message sent by the SIP proxy server, it advertises the intersection of its own and SIP IP phone A's media capability in the 200 OK response. If SIP IP phone C does not support the media capability advertised by SIP IP phone A, it sends back a 400 Bad Request response with a "Warning: 304 Codec negotiation failed" header field.
9	ACK—SIP IP phone A to SIP IP phone C	SIP IP phone A sends an ACK to SIP IP phone C. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.

At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone C.

SIP IP Phone-to-SIP IP Phone Call Forward No Answer

Figure 7-31 and Figure 7-32 illustrate a successful SIP IP phone-to-SIP IP phone call forward when there is no answer via a SIP proxy. In these scenarios, the three end users are identified as User A, User B, and User C. User B's calls are configured to forward to User C when a response timeout occurs. Figure 7-31 illustrates the call as processed by a recursive proxy and Figure 7-32 illustrates the call as processed by a non-recursive proxy.

Figure 7-31   SIP IP Phone-to-SIP IP Phone Call Forward No Answer Call Setup via Recursive Proxy
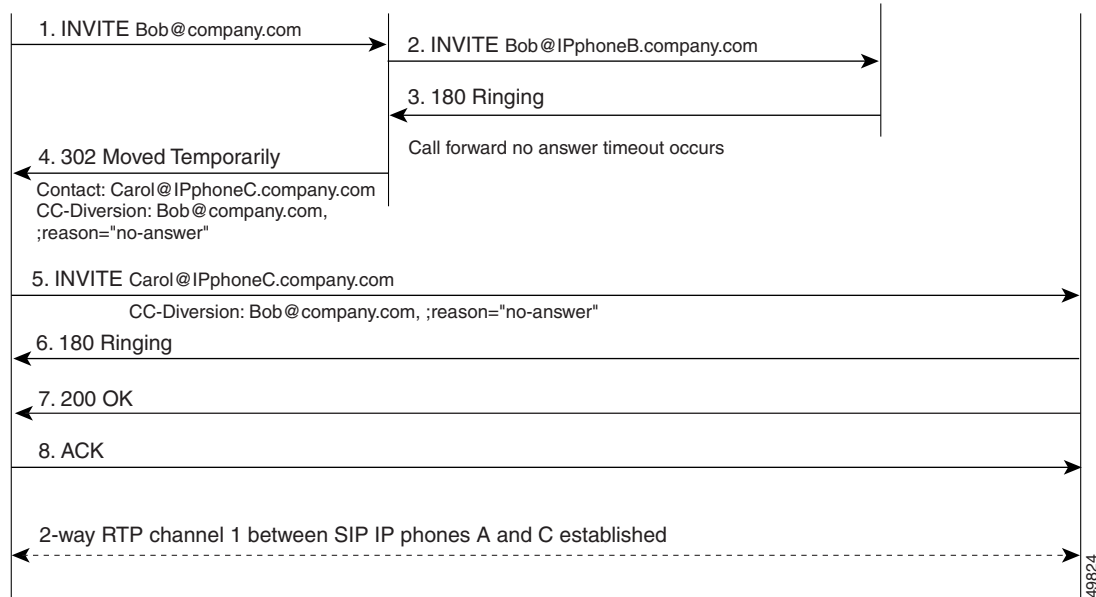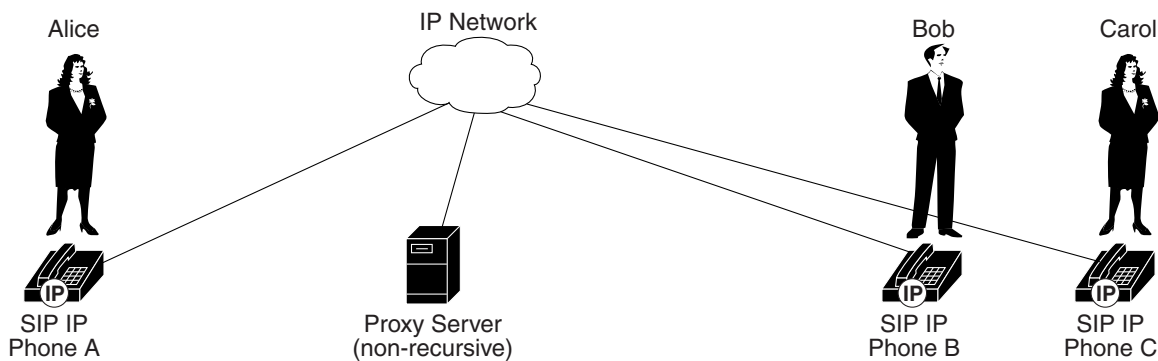
Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	Alice's SIP IP phone A sends an INVITE request to the proxy server. The INVITE request is an invitation to Bob to participate in a call session.
		In the INVITE request:
		• Bob's phone number is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies Bob's address and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to Bob might appear 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.
		• Alice at SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability SIP IP phone A is ready to receive is specified in the SDP.
		• The port on which SIP IP phone A is prepared to receive the RTP data is specified in the SDP.
2	INVITE—SIP proxy server to SIP IP phone B	The proxy server forwards the INVITE request to Bob at SIP IP phone B.
3	180 Ringing—SIP IP phone B to the SIP proxy server	SIP IP phone B sends a 180 Ringing response to the SIP proxy server.
Call forward no answer timer expires.		
4	INVITE—SIP proxy server phone to SIP IP phone C	The SIP proxy server sends an INVITE request to Carol at SIP IP phone C to which Bob's calls have been configured to forward when there is no answer. In the INVITE request, SIP IP phone A changes the Request-URI to divert the request to Carol at SIP IP phone C and adds a CC-Diversion header containing the Request-URI from the initial INVITE request and the reason for the diversion.
5	180 Ringing—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 180 Ringing response to the SIP proxy server.
6	200 OK—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 200 OK response to SIP IP phone A.
		If SIP IP phone C supports the media capability advertised in the INVITE message sent by the SIP proxy server, it advertises the intersection of its own and SIP IP phone A's media capability in the 200 OK response. If SIP IP phone C does not support the media capability advertised by SIP IP phone A, it sends back a 400 Bad Request response with a "Warning: 304 Codec negotiation failed" header field.

Step	Action	Description
7	200 OK—SIP proxy server to SIP IP phone A	The SIP proxy server forwards the 200 OK response to SIP IP phone A. The 200 OK response notifies the SIP IP phone A that Carol has answered the phone (for example, the handset of SIP IP phone C went off-hook).
8	ACK—SIP IP phone A to SIP IP phone C	SIP IP phone A sends an ACK to SIP IP phone C. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.

At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone C.

Figure 7-32   SIP IP Phone-to-SIP IP Phone Call Forward No Answer Setup via Non-recursive Proxy

Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	Alice's SIP IP phone A sends an INVITE request to the proxy server. The INVITE request is an invitation to Bob to participate in a call session.
		In the INVITE request:
		• Bob's phone number is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies Bob's address and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to Bob might appear 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.
		• Alice at SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability SIP IP phone A is ready to receive is specified in the SDP.
		• The port on which SIP IP phone A is prepared to receive the RTP data is specified in the SDP.
2	INVITE—SIP proxy server to SIP IP phone B	The SIP proxy server forwards the INVITE request to Bob at SIP IP phone B.
3	180 Ringing—SIP IP phone B to the SIP proxy server	SIP IP phone B sends a 180 Ringing response to the SIP proxy server.
At this point, a timeout to INVITE request occurs.		
4	302 Moved Temporarily—SIP proxy server to SIP IP phone A	The SIP proxy server sends a 302 Moved Temporarily message to SIP IP phone A. In the 302 Moved Temporarily message, Carol at SIP IP phone C is added as the Contact and a CC-Diversion header is added that contains the Request-URI from the initial INVITE and the reason for the diversion.
5	INVITE—SIP IP phone A to SIP IP phone C	SIP IP phone A sends an INVITE request to Carol at SIP IP phone C to which Bob's calls have been configured to forward when Bob is unavailable. In the INVITE request, the SIP proxy server changes the Request-URI to divert the request to Carol at SIP IP phone C and adds a CC-Diversion header containing the Request-URI from the initial INVITE request and the reason for the diversion.
6	180 Ringing—SIP IP phone C to SIP IP phone A	SIP IP phone C sends a 180 Ringing response to SIP IP phone A.

Step	Action	Description
7	200 OK—SIP IP phone C to SIP IP phone A	SIP IP phone C sends a 200 OK response to SIP IP phone A. The 200 OK response notifies the SIP IP phone A that Carol has answered the phone (for example, the handset of SIP IP phone C went off-hook).
		If SIP IP phone C supports the media capability advertised in the INVITE message sent by the SIP proxy server, it advertises the intersection of its own and SIP IP phone A's media capability in the 200 OK response. If SIP IP phone C does not support the media capability advertised by SIP IP phone A, it sends back a 400 Bad Request response with a "Warning: 304 Codec negotiation failed" header field.
8	ACK—SIP IP phone A to SIP IP phone C	SIP IP phone A sends an ACK to SIP IP phone C. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.

At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone C.

SIP IP Phone-to-SIP IP Phone Call Forward Unavailable

Figure 7-33 and Figure 7-34 illustrate a successful SIP IP phone-to-SIP IP phone call forward when the callee is unavailable via a SIP proxy. In these scenarios, the three end users are identified as User A, User B, and User C. User B's calls are configured to forward to User C when User B is unavailable. Figure 7-33 illustrates the call as processed by a recursive proxy and Figure 7-34 illustrates the call as processed by a non-recursive proxy.

Figure 7-33   SIP IP Phone-to-SIP IP Phone Call Forward Unavailable Call Setup via Recursive Proxy
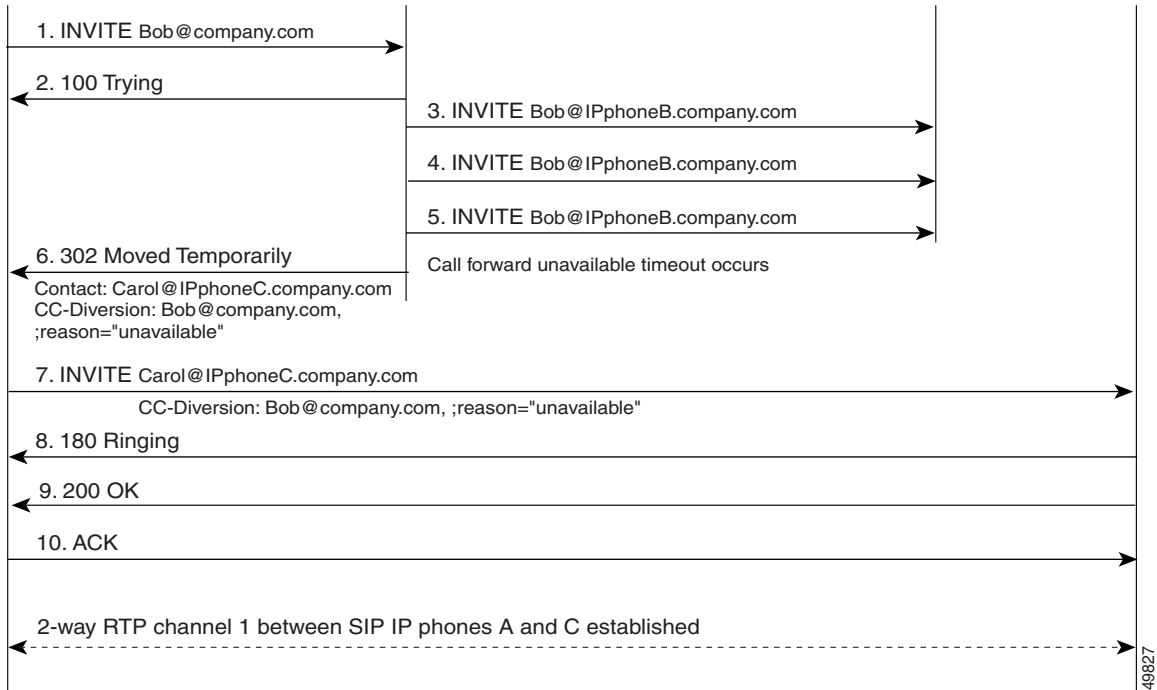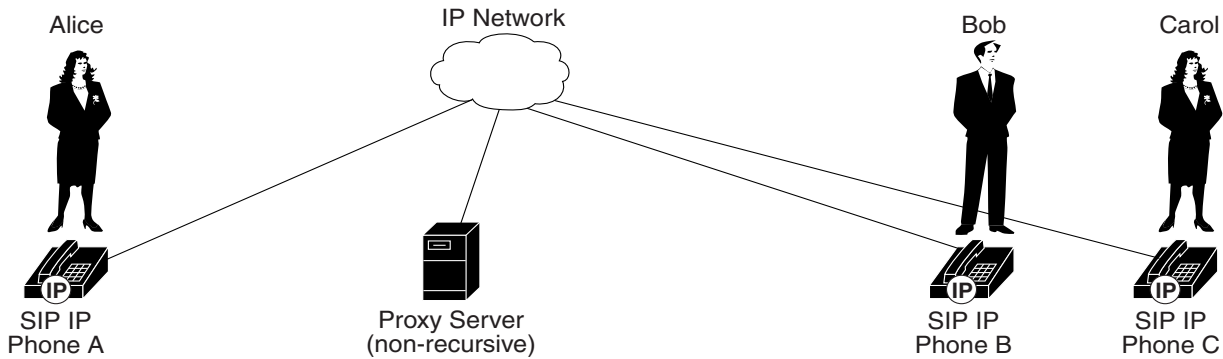
Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	Alice's SIP IP phone A sends an INVITE request to the proxy server. The INVITE request is an invitation to Bob to participate in a call session.
		In the INVITE request:
		• Bob's phone number is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies Bob's address and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to Bob might appear 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.
		• Alice at SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability SIP IP phone A is ready to receive is specified in the SDP.
		• The port on which SIP IP phone A is prepared to receive the RTP data is specified in the SDP.
2	100 Trying—SIP proxy server to SIP IP phone A	The SIP proxy server sends a 100 Trying response to the INVITE request sent by SIP IP phone A. The 100 Trying response indicates that the INVITE request has been received by the SIP proxy server but that Bob at SIP IP phone B has not yet been located and that some unspecified action, such as a database consultation, is taking place.
3 to 5	INVITE—proxy server to SIP IP phone B	The SIP proxy server forwards the INVITE request to Bob at SIP IP phone B.
Call forward unavailable timer expires.		
6	INVITE—SIP proxy server to SIP IP phone C	The SIP proxy server sends an INVITE request to Carol at SIP IP phone C to which Bob's calls have been configured to forward when there is no answer. In the INVITE request, SIP IP phone A changes the Request-URI to divert the request to Carol at SIP IP phone C, and adds a CC-Diversion header containing the Request-URI from the initial INVITE request and the reason for the diversion.
7	180 Ringing—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 180 Ringing response to the SIP proxy server.
8	200 OK—SIP IP phone C to SIP proxy server	SIP IP phone C sends a 200 OK response to SIP IP phone A.
		If SIP IP phone C supports the media capability advertised in the INVITE message sent by the SIP proxy server, it advertises the intersection of its own and SIP IP phone A's media capability in the 200 OK response. If SIP IP phone C does not support the media capability advertised by SIP IP phone A, it sends back a 400 Bad Request response with a "Warning: 304 Codec negotiation failed" header field.

Step	Action	Description
9	200 OK—SIP proxy server to SIP IP phone A	The SIP proxy server forwards the 200 OK response to SIP IP phone A. The 200 OK response notifies the SIP IP phone A that Carol has answered the phone (for example, the handset of SIP IP phone went off-hook).
10	ACK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends an ACK to SIP IP phone C. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.

At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone C.

Figure 7-34   SIP IP Phone-to-SIP IP Phone Call Forward Unavailable Call Setup via Non-recursive Proxy

Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	Alice's SIP IP phone A sends an INVITE request to the proxy server. The INVITE request is an invitation to Bob to participate in a call session.
		In the INVITE request:
		• Bob's phone number is inserted in the Request-URI field in the form of a SIP URL. The SIP URL identifies Bob's address and takes a form similar to an email address (*user@host* where *user* is the telephone number and *host* is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to Bob might appear 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.
		• Alice at SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability SIP IP phone A is ready to receive is specified in the SDP.
		• The port on which SIP IP phone A is prepared to receive the RTP data is specified in the SDP.
2	100 Trying—SIP proxy server to SIP IP phone A	The SIP proxy server sends a 100 Trying response to the INVITE request sent by SIP IP phone A. The 100 Trying response indicates that the INVITE request has been received by the SIP proxy server, but that Bob has not yet been located and that some unspecified action, such as a database consultation, is taking place.
3 to 5	INVITE—proxy server to SIP IP phone B	The SIP proxy server forwards the INVITE request to Bob at SIP IP phone B.
At this point, the call forward unavailable timer expires.		
6	302 Moved Temporarily—SIP proxy server to SIP IP phone A	The SIP proxy server sends a 302 Moved Temporarily message to SIP IP phone A. In the 302 Moved Temporarily message, Carol at SIP IP phone C is added as the Contact and a CC-Diversion header is added that contains the Request-URI from the initial INVITE and the reason for the diversion.
7	INVITE—SIP IP phone A to SIP IP phone C	SIP IP phone A sends an INVITE request to Carol at SIP IP phone C to which Bobs calls have been configured to forward when there is no answer. In the INVITE request, SIP IP phone A changes the Request-URI to divert the request to Carol at SIP IP phone C, and adds a CC-Diversion header containing the Request-URI from the initial INVITE request and the reason for the diversion.
8	180 Ringing—SIP IP phone C to SIP IP phone A	SIP IP phone C sends a 180 Ringing response to SIP IP phone A.

Step	Action	Description
9	200 OK—SIP IP phone C to SIP IP phone A	SIP IP phone C sends a 200 OK response to SIP IP phone A. The 200 OK response notifies the SIP IP phone A that Carol has answered the phone (for example, the handset of SIP IP phone C went off-hook).
		If SIP IP phone C supports the media capability advertised in the INVITE message sent by the SIP proxy server, it advertises the intersection of its own and SIP IP phone A's media capability in the 200 OK response. If SIP IP phone C does not support the media capability advertised by SIP IP phone A, it sends back a 400 Bad Request response with a "Warning: 304 Codec negotiation failed" header field.
10	ACK—SIP IP phone A to SIP IP phone C	SIP IP phone A sends an ACK to SIP IP phone C. The ACK confirms that SIP IP phone A has received the 200 OK response from SIP IP phone C.

At this point, a two-way RTP channel is established between SIP IP phone A and SIP IP phone C.

Call Flow Scenarios for Failed Calls

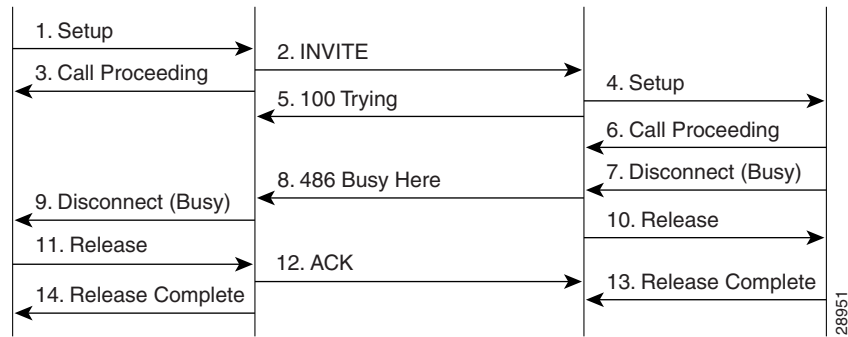This section describes call flows for the following scenarios, which illustrate successful calls:

SIP Gateway-to-SIP Gateway—Called User is Busy

Figure 7-35 illustrates an unsuccessful call in which User A initiates a call to User B but User B is on the phone and is either unable or unwilling to accept another call.

Figure 7-35   SIP Gateway-to-SIP Gateway Call—Called User is Busy

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.
2	INVITE—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an INVITE request to SIP gateway 2. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• PBX A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which SIP gateway 1 is prepared to receive the RTP data is specified.
3	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.
4	Setup—SIP gateway 2 to PBX B	SIP gateway 2 receives the INVITE request from SIP gateway 1 and initiates a Call Setup with User B via PBX B.

Step	Action	Description
5	100 Trying—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 100 Trying response to the INVITE request sent by SIP gateway 1. The 100 Trying message indicates that the INVITE request has been received by SIP gateway 2 but that User B has not yet been located and that some unspecified action, such as a database consultation, is taking place.
6	Call Proceeding—PBX B to SIP gateway 2	PBX B sends a Call Proceeding message to SIP gateway 2 to acknowledge the Call Setup request.
7	Disconnect (Busy)—PBX B to SIP gateway 2	PBX B sends a Disconnect message to SIP gateway 2. In the Disconnect message, the cause code indicates that User B is busy. The Disconnect message starts the call session termination process.
8	486 Busy Here—SIP gateway 2 to SIP gateway 1	SIP gateway 2 maps the Release message cause code (Busy) to the 486 Busy Here response and sends the response to SIP gateway 1. The 486 Busy Here response is a client error response that indicates that User B's phone was successfully contacted but User B was either unwilling or unable to take another call.
9	Disconnect (Busy)—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release message to PBX A. User A hears a busy tone.
10	Release—SIP gateway 2 to PBX B	SIP gateway 2 sends a Release message to PBX B.
11	Release—PBX A to SIP gateway 1	PBX A sends a Release message to SIP gateway 1.
12	ACK—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an ACK to SIP gateway 2. The ACK confirms that the 486 Busy Here response has been received.
13	Release Complete—PBX B to SIP gateway 2	PBX B sends a Release Complete message to SIP gateway 2.
14	Release Complete—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A and the call session attempt is terminated.

SIP Gateway-to-SIP Gateway—Called User Does Not Answer

Figure 7-36 illustrates an unsuccessful call in which User A initiates a call to User B but User B does not answer.

Figure 7-36   SIP Gateway-to-SIP Gateway Call—Called User Does Not Answer
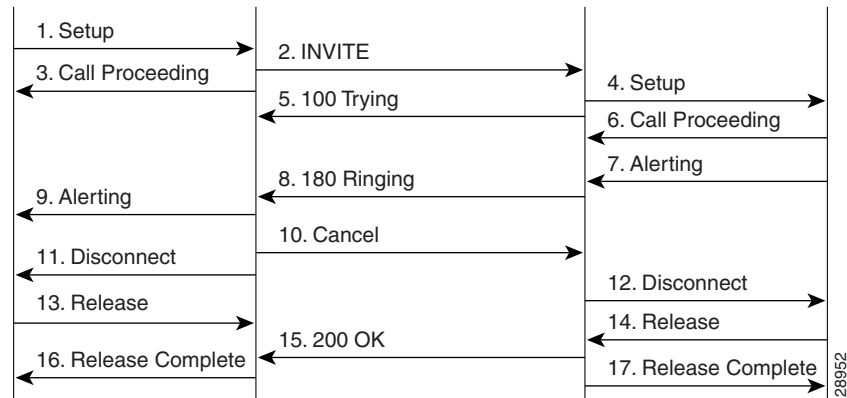

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.
2	INVITE—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an INVITE request to SIP gateway 2. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• PBX A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which SIP gateway 1 is prepared to receive the RTP data is specified.
3	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.

Step	Action	Description
4	Setup—SIP gateway 2 to PBX B	SIP gateway 2 receives the INVITE request from SIP gateway 1 and initiates a Call Setup with User B via PBX B.
5	100 Trying—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 100 Trying response to the INVITE request sent by SIP gateway 1. The 100 Trying response indicates that the INVITE request has been received by SIP gateway 2 but that User B has not yet been located and that some unspecified action, such as a database consultation, is taking place.
6	Call Proceeding—PBX B to SIP gateway 2	PBX B sends a Call Proceeding message to SIP gateway 2 to acknowledge the Call Setup request.
7	Alerting—PBX B to SIP gateway 2	PBX B sends an Alert message to SIP gateway 2. The message indicates that the PBX is attempting to alert the user of the call (that is to say, the phone is ringing).
8	180 Ringing—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 180 Ringing response to SIP gateway 1. The 180 Ringing response indicates that SIP gateway 2 has located, and is trying to alert, User B.
9	Alerting—SIP gateway 1 to PBX A	SIP gateway 1 sends an Alert message to PBX A. The Alert message indicates that SIP gateway 1 has received a 180 Ringing response from SIP gateway 2. User A hears the ringback tone that indicates that User B is being alerted.
10	Cancel (Ring Timeout)—SIP gateway 1 to SIP gateway 2	Because SIP gateway 2 did not return an appropriate response within the time specified by the Expires header in the INVITE request, SIP gateway 1 sends a SIP CANCEL request to SIP gateway 2. A CANCEL request cancels a pending request with the same Call-ID, To, From, and CSeq header field values.
11	Disconnect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Disconnect message to PBX A.
12	Disconnect—SIP gateway 2 to PBX B	SIP gateway 2 sends a Disconnect message to PBX B.
13	Release—PBX A to SIP gateway 1	PBX A sends a Release message to SIP gateway 1.
14	Release—PBX B to SIP gateway 2	PBX B sends a Release message to SIP gateway 2.
15	200 OK—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 200 OK response to SIP gateway 2. The 200 OK response confirms that the Cancel request has been received.
16	Release Complete—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A.
17	Release Complete—SIP gateway 2 to PBX B	SIP gateway 2 sends a Release Complete message to PBX B and the call session attempt is terminated.

SIP Gateway-to SIP Gateway—Client, Server, or Global Error

Figure 7-37 illustrates an unsuccessful call in which User A initiates a call to User B but there are no more channels available on the gateway. Therefore, SIP gateway 2 refuses the connection.

Figure 7-37   SIP Gateway-to-SIP Gateway Call—Client, Server, or Global Error

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.
2	INVITE—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an INVITE request to SIP gateway 2. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• PBX A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which SIP gateway 1 is prepared to receive the RTP data is specified.
3	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.

Step	Action	Description
4	100 Trying—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 100 Trying response to the INVITE request sent by SIP gateway 1. The 100 Trying message indicates that the INVITE request has been received by SIP gateway 2 but that User B has not yet been located and that some unspecified action, such as a database consultation, is taking place.
5	Class 4*xx*/5*xx*/6*xx* Failure—SIP gateway 2 to SIP gateway 1	SIP gateway 2 determines that it does not have any more channels available, refuses the connection, and sends a SIP 503 Service Unavailable response to SIP gateway 1.
		The 503 Service Unavailable response is a class 4*xx*, 5*xx*, or class 6*xx* failure response. Depending on which class the failure response is, the call actions differ.
		If SIP gateway 2 sends a class 4*xx* failure response (a definite failure response that is a client error), the request will not be retried without modification.
		If SIP gateway 2 sends a class 5*xx* failure response (an indefinite failure that is a server error), the request is not terminated but rather other possible locations are tried.
		If SIP gateway 2 sends a class 6*xx* failure response (a global error), the search for User B is terminated because the 6*xx* 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.
		The call failure on SIP gateway 2 might occur before a proceeding indication from PBX B. In that case a SIP failure response is sent before the 100 Trying response.
6	Disconnect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Disconnect message to PBX A.
7	Release—PBX A to SIP gateway 1	PBX A sends a Release message to SIP gateway 1.
8	ACK—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an ACK to SIP gateway 2. The ACK confirms that the 503 Service Unavailable response has been received.
9	Release Complete—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A and the call session attempt is terminated.

SIP Gateway-to-SIP Gateway via SIP Redirect Server—Called User is Busy

Figure 7-38 illustrates an unsuccessful call in which User A initiates a call to User B but User B is on the phone and is either unable or unwilling to accept another call.

Figure 7-38   SIP Gateway-to-SIP Gateway Call via a SIP Redirect Server—Called User is Busy

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.
2	INVITE—SIP gateway 1 to SIP redirect server	SIP gateway 1 sends an INVITE request to the SIP redirect server. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• PBX A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which SIP gateway 1 is prepared to receive the RTP data is specified.

Step	Action	Description
3	302 Moved Temporarily—SIP redirect server to SIP gateway 1	SIP redirect server sends a 302 Moved Temporarily message to SIP gateway 1. The message indicates that User B is not available and includes instructions to locate User B.
4	ACK—SIP gateway 1 to SIP redirect server	SIP gateway 1 acknowledges the 302 Moved Temporarily response with an ACK.
5	INVITE—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends a new INVITE request to User B. The new INVITE request includes the first contact listed in the 300 Multiple Choice response as the new address for User B, a higher transaction number in the CSeq field, and the same Call-ID as the first INVITE request.
6	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.
7	Setup—SIP gateway 2 to PBX B	SIP gateway 2 receives the INVITE request from SIP gateway 1 and initiates a Call Setup with User B via PBX B.
8	100 Trying—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 100 Trying response to the INVITE request sent by SIP gateway 1. The 100 Trying response indicates that the INVITE request has been received by SIP gateway 2 but that User B has not yet been located and that some unspecified action, such as a database consultation, is taking place.
9	Call Proceeding—PBX B to SIP gateway 2	PBX B sends a Call Proceeding message to SIP gateway 2 to acknowledge the Call Setup request.
10	Disconnect (Busy)—PBX B to SIP gateway 2	PBX B sends a Disconnect message to SIP gateway 2. In the Disconnect message, the cause code indicates that User B is busy. The Disconnect message starts the call session termination process.
11	486 Busy Here—SIP gateway 2 to SIP gateway 1	SIP gateway 2 maps the Release message cause code (Busy) to the 486 Busy response and sends the response to SIP gateway 1. The 486 Busy Here response is a client error response that indicates that User B's phone was successfully contacted but User B was either unwilling or unable to take another call.
12	Disconnect (Busy) —SIP gateway 1 to PBX A	SIP gateway 1 sends a Disconnect message to PBX A. User A hears a busy tone.
13	Release—PBX A to SIP gateway 1	PBX A sends a Release message to SIP gateway 1.
14	Release—SIP gateway 2 to PBX B	SIP gateway 1 sends a Release message to PBX B.
15	ACK—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an ACK to SIP gateway 2. The ACK confirms that the 486 Busy Here response has been received.
16	Release Complete—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A and the call session attempt is terminated.
17	Release Complete—PBX B to SIP gateway 2	PBX B sends a Release Complete message to SIP gateway 2.

SIP Gateway-to-SIP Gateway via SIP Redirect Server—Called User Does Not Answer

Figure 7-39 illustrates an unsuccessful call in which User A initiates a call to User B but User B does not answer.

Figure 7-39   SIP Gateway-to-SIP Gateway Call via a SIP Redirect Server—Called User Does Not Answer

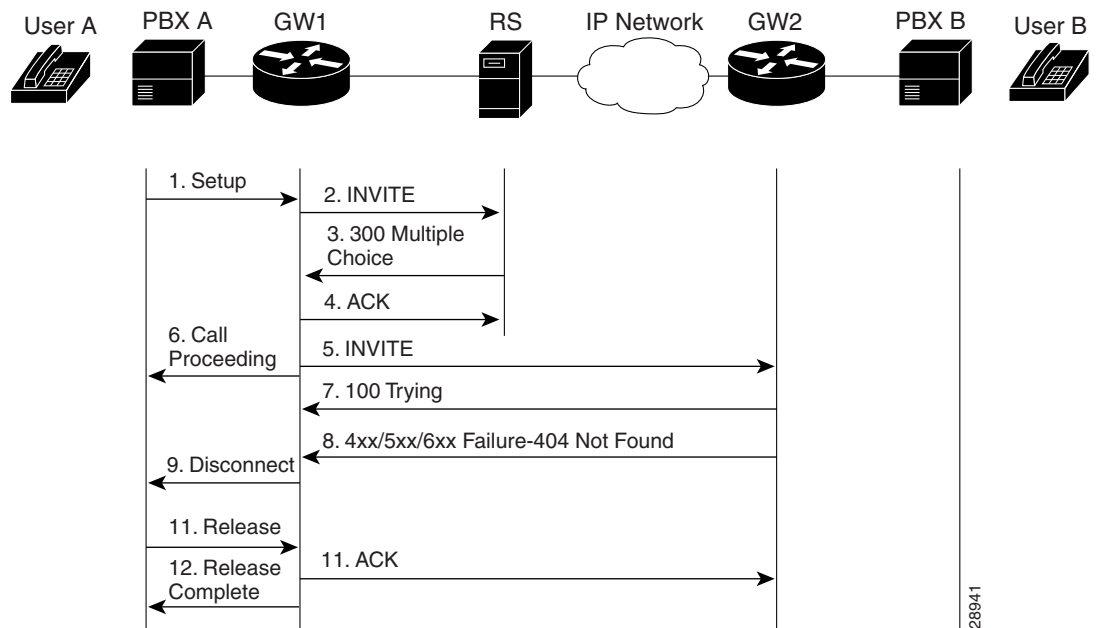| Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.

Step	Action	Description
2	INVITE—SIP gateway 1 to SIP redirect server	SIP gateway 1 sends an INVITE request to the SIP redirect server. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• PBX A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which SIP gateway 1 is prepared to receive the RTP data is specified.
3	302 Moved Temporarily— SIP redirect server to SIP gateway 1	SIP redirect server sends a 302 Moved Temporarily message to SIP gateway 1. The message indicates that User B is not available and includes instructions to locate User B.
4	ACK—SIP gateway 1 to SIP redirect server	SIP gateway 1 acknowledges the 302 Moved Temporarily response with an ACK.
5	INVITE—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends a new INVITE request to User B. The new INVITE request includes a new address for User B, a higher transaction number in the CSeq field, but the same Call-ID as the first INVITE request.
6	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.
7	Setup—SIP gateway 2 to PBX B	SIP gateway 2 receives the INVITE request from SIP gateway 1 and initiates a Call Setup with User B via PBX B.
8	100 Trying—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 100 Trying response to the INVITE request sent by SIP gateway 1. The 100 Trying message indicates that the INVITE request has been received by SIP gateway 2 but that User B has not yet been located and that some unspecified action, such as a database consultation, is taking place.
9	Call Proceeding—PBX B to SIP gateway 2	PBX B sends a Call Proceeding message to SIP gateway 2 to acknowledge the Call Setup request.
10	Alerting—PBX B to SIP gateway 2	PBX B sends an Alert message to SIP gateway 2. User B's phone begins to ring.
11	180 Ringing—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 180 Ringing response to SIP gateway 1. The 180 Ringing response indicates that SIP gateway 2 has located, and is trying to alert, User B.
12	Alerting—SIP gateway 1 to PBX A	SIP gateway 1 sends an Alert message to PBX A.
13	CANCEL (Ring Timeout)—SIP gateway 1 to SIP gateway 2	Because SIP gateway 2 did not return an appropriate response within the time specified by the Expires header in the INVITE request, SIP gateway 1 sends a SIP CANCEL request to SIP gateway 2. A CANCEL request cancels a pending request with the same Call-ID, To, From, and CSeq header field values.

Step	Action	Description
14	Disconnect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Disconnect message to PBX A.
15	Release—PBX A to SIP gateway 1	PBX A sends a Release message to SIP gateway 1.
16	Disconnect—SIP gateway 2 to PBX B	SIP gateway 2 sends a Disconnect message to PBX B.
17	200 OK—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends a 200 OK response to SIP gateway 2. The 200 OK response confirms that the CANCEL request has been received.
18	Release Complete—PBX A to SIP gateway 1	PBX A sends a Release Complete message to SIP gateway 1 and the call session attempt is terminated.
19	Release—PBX B to SIP gateway 2	PBX B sends a Release message to SIP gateway 2.
20	Release Complete—SIP gateway 2 to PBX B	SIP gateway 2 sends a Release Complete message to PBX B.

SIP Gateway-to-SIP Gateway via SIP Redirect Server—Client, Server, or Global Error

Figure 7-40 illustrates an unsuccessful call in which User A initiates a call to User B but SIP gateway 2 determines that User B does not exist at the domain specified in the INVITE request sent by SIP gateway 1. SIP gateway 2 refuses the connection.

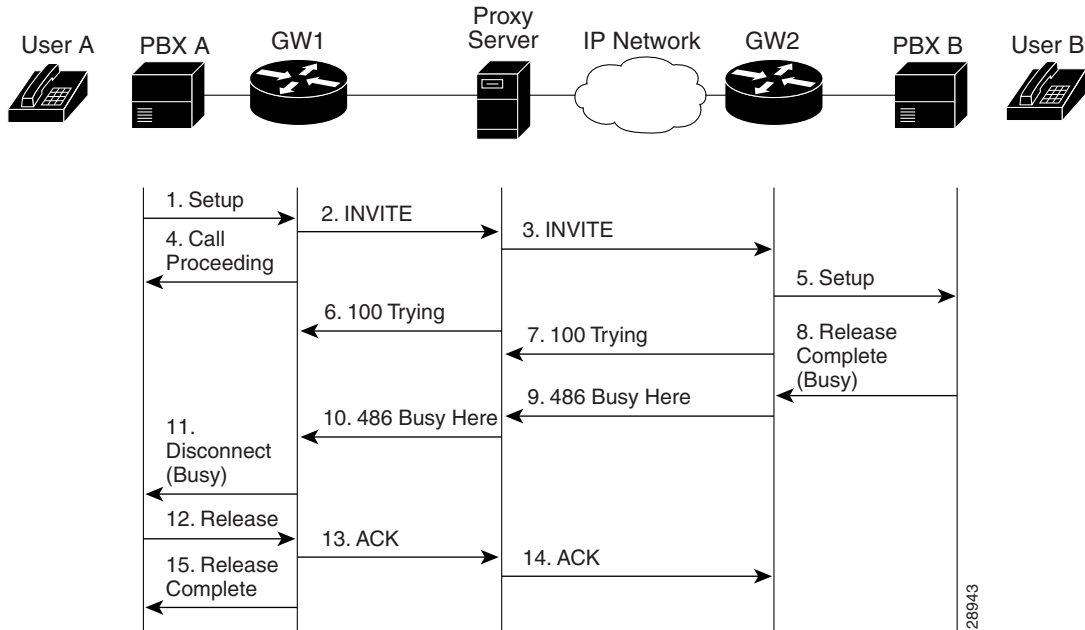*Figure 7-40   SIP Gateway-to-SIP Gateway Call via a SIP Redirect Server—Client, Server, or Global*

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.
2	INVITE—SIP gateway 1 to SIP redirect server	SIP gateway 1 sends an INVITE request to the SIP redirect server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: • The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. • PBX A is identified as the initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready is specified. • The port on which SIP gateway 1 is prepared to receive the RTP data is specified.
3	300 Multiple Choice—SIP redirect server to SIP gateway 1	The SIP redirect server sends a 300 Multiple Choice response to SIP gateway 1. The 300 Multiple Choice response indicates that the SIP redirect server accepted the INVITE request, contacted a location server with all or part of User B's SIP URL, and the location server provided a list of alternative locations where User B might be located. The SIP redirect server returns these possible addresses to User A in the 300 Multiple Choice response.
4	ACK—SIP gateway 1 to SIP redirect server	SIP gateway 1 acknowledges the 300 Multiple Choice response with an ACK.
5	INVITE—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends a new INVITE request to User B. The new INVITE request includes a new address for User B, a higher transaction number in the CSeq field, but the same Call-ID as the first INVITE request.
6	Call Proceeding—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.
7	100 Trying—SIP gateway 2 to SIP gateway 1	SIP gateway 2 sends a 100 Trying response to the INVITE request sent by SIP gateway 1. The 100 Trying message indicates that the INVITE request has been received by SIP gateway 2 but that User B has not yet been located and that some unspecified action, such as a database consultation, is taking place.

Step	Action	Description
8	Class 4xx/5xx/6xx Failure—SIP gateway 2 to SIP gateway 1	SIP gateway 2 determines that User B does not exist at the domain specified in the INVITE request sent by SIP gateway 1. SIP gateway 2 refuses the connection and sends a 404 Not Found response to SIP gateway 1.
		The 404 Not Found response is a class 4*xx* failure response. Depending on which class the failure response is, the call actions differ.
		If SIP gateway 2 sends a class 4*xx* failure response (a definite failure response that is a client error), the request will not be retried without modification.
		If SIP gateway 2 sends a class 5*xx* failure response (an indefinite failure that is a server error), the request is not terminated but rather other possible locations are tried.
		If SIP gateway 2 sends a class 6*xx* failure response (a global error), the search for User B is terminated because the 6*xx* 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.
9	Disconnect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Disconnect message to PBX A.
10	Release—PBX A to SIP gateway 1	PBX A sends a Release message to SIP gateway 1.
11	ACK—SIP gateway 1 to SIP gateway 2	SIP gateway 1 sends an ACK to SIP gateway 2. The ACK confirms that the 404 Not Found failure response has been received.
12	Release Complete—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A and the call session attempt is terminated.

SIP Gateway-to-SIP Gateway via SIP Proxy Server—Called User is Busy

Figure 7-41 illustrates an unsuccessful call in which User A initiates a call to User B but User B is on the phone and is either unwilling or unable to accept another call.

Figure 7-41   SIP Gateway-to-SIP Gateway Call via a SIP Proxy Server—Called User is Busy

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.
2	INVITE—SIP gateway 1 to SIP proxy server	SIP gateway 1 sends an INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• PBX A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which SIP gateway 1 is prepared to receive the RTP data is specified.

Step	Action	Description
3	INVITE—SIP proxy server to SIP gateway 2	The SIP proxy server checks whether its own address is contained in the Via field (to prevent loops), directly copies the To, From, Call-ID, and Contact fields from the request it received from SIP gateway 1, changes the Request-URI to indicate the server to which it intends to send the INVITE request, and then sends a new INVITE request to SIP gateway 2.
4	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.
5	Setup—SIP gateway 2 to PBX B	SIP gateway 2 receives the INVITE request from the SIP proxy server and initiates a Call Setup with User B via PBX B.
6	100 Trying—SIP proxy server to SIP gateway 1	The SIP proxy server sends a 100 Trying response to SIP gateway 1.
7	100 Trying—SIP gateway 2 to SIP proxy server	SIP gateway 2 sends a 100 Trying response to the SIP proxy server.
8	Release Complete (Busy)—PBX B to SIP gateway 2	PBX B sends a Release Complete message to SIP gateway 2. In the Release Complete message, the cause code indicates that User B is busy. The Release Complete message starts the call session termination process.
9	486 Busy Here—SIP gateway 2 to SIP proxy server	SIP gateway 2 maps the Release message cause code (Busy) to the 486 Busy response and sends the response to the SIP proxy server. The 486 Busy Here response is a client error response that indicates that User B's phone was successfully contacted but User B was either unwilling or unable to take another call.
10	486 Busy Here—SIP proxy server to SIP gateway 1	The SIP proxy server forwards the 486 Busy response to SIP gateway 1.
11	Disconnect (Busy)—SIP gateway 1 to PBX A	SIP gateway 1 sends a Disconnect message to PBX A.
12	Release—PBX A to SIP gateway 1	PBX A sends a Release message to SIP gateway 1.
13	ACK—SIP gateway 1 to SIP proxy server	SIP gateway 1 sends an SIP ACK to the SIP proxy server.
14	ACK—SIP proxy server to SIP gateway 2	The SIP proxy server forwards the SIP ACK to SIP gateway 2. The ACK confirms that the 486 Busy Here response has been received.
15	Release Complete—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A and the call session attempt is terminated.

SIP Gateway-to-SIP Gateway via SIP Proxy Server—Client or Server Error

Figure 7-42 illustrates an unsuccessful call in which User A initiates a call to User B but there are no more channels available on SIP gateway 2. Therefore, SIP gateway 2 refuses the connection.

Figure 7-42   SIP Gateway-to-SIP Gateway Call via a SIP Proxy Server—Client or Server Error

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.
2	INVITE—SIP gateway 1 to SIP proxy server	SIP gateway 1 sends an INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• PBX A is identified as the initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which SIP gateway 1 is prepared to receive the RTP data is specified.

Step	Action	Description
3	INVITE—SIP proxy server to SIP gateway 2	The SIP proxy server checks whether its own address is contained in the Via field (to prevent loops), directly copies the To, From, Call-ID, and Contact fields from the request it received from SIP gateway 1, changes the Request-URI to indicate the server to which it intends to send the INVITE request, and then sends a new INVITE request to SIP gateway 2.
4	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.
5	100 Trying—SIP proxy server to SIP gateway 1	The SIP proxy server sends a 100 Trying response to SIP gateway 1.
6	100 Trying—SIP gateway 2 to SIP proxy server	SIP gateway 2 sends a 100 Trying response to the SIP proxy server.
7	Class 4xx/5xx/6xx Failure—SIP gateway 2 to SIP proxy server	SIP gateway 2 determines that it does not have any more channels available, refuses the connection, and sends a SIP 503 Service Unavailable response to the SIP proxy server.
8	Class 4xx/5xx/6xx Failure—SIP proxy server to SIP gateway 1	The SIP proxy server forwards the SIP 503 Service Unavailable response to SIP gateway 1.
9	Disconnect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Disconnect message to PBX A.
10	Release—PBX A to SIP gateway 1	PBX A sends a Release message to SIP gateway 1.
11	ACK—SIP gateway 1 to SIP proxy server	SIP gateway 1 sends an ACK to the SIP proxy server.
12	ACK—SIP proxy server to SIP gateway 2	The SIP proxy server forwards the SIP ACK to SIP gateway 2. The ACK confirms that the 503 Service Unavailable response has been received.
13	Release Complete—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A and the call session attempt is terminated.

SIP Gateway-to-SIP Gateway via SIP Proxy Server—Global Error

Figure 7-43 illustrates an unsuccessful call in which User A initiates a call to User B and receives a class 6*xx* response.

Figure 7-43   SIP Gateway-to-SIP Gateway Call via a SIP Proxy Server—Global Error Response
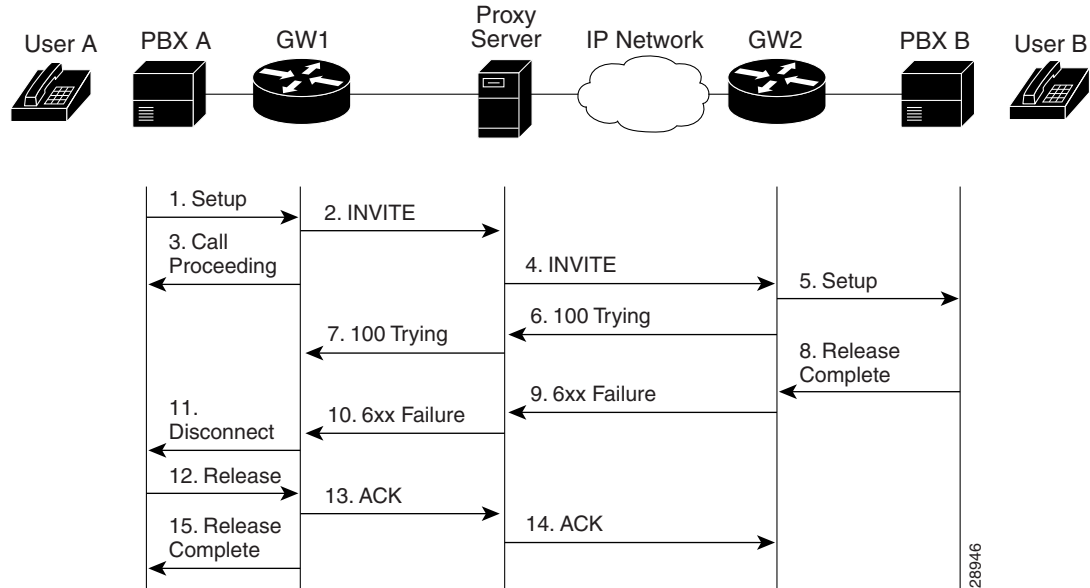

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.
2	INVITE—SIP gateway 1 to SIP proxy server	SIP gateway 1 sends an INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• PBX A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which SIP gateway 1 is prepared to receive the RTP data is specified.
3	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.

Step	Action	Description
4	INVITE—SIP proxy server to SIP gateway 2	The SIP proxy server checks whether its own address is contained in the Via field (to prevent loops), directly copies the To, From, Call-ID, and Contact fields from the request it received from SIP gateway 1, changes the Request-URI to indicate the server to which it intends to send the INVITE request, and then sends a new INVITE request to SIP gateway 2.
5	Setup—SIP gateway 2 to PBX B	SIP gateway 2 receives the INVITE request from the SIP proxy server and initiates a Call Setup with User B via PBX B.
6	100 Trying—SIP gateway 2 to SIP proxy server	SIP gateway 2 sends a 100 Trying response to the SIP proxy server. The SIP proxy server might or might not forward the 100 Trying response to SIP gateway 1.
7	100 Trying—SIP proxy server to SIP gateway 1	The SIP proxy server forwards the 100 Trying response to SIP gateway 1.
8	Release Complete—PBX B to SIP gateway 2	PBX B sends a Release Complete message to SIP gateway 2. The Release Complete message starts the call session termination process.
9	6*xx* Failure—SIP gateway 2 to SIP proxy server	SIP gateway 2 sends a class 6*xx* failure response (a global error) to the SIP proxy server. A class 6*xx* failure response indicates that a server has definite information about User B, but not for the particular instance indicated in the Request-URI field. All further searches for this user will fail, therefore the search is terminated. The SIP proxy server must forward all class 6*xx* failure responses to the client.
10	6xx Failure—SIP proxy server to SIP gateway 1	The SIP proxy server forwards the 6*xx* failure to SIP gateway 1.
11	Disconnect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Disconnect message to PBX A.
12	Release—PBX A to SIP gateway 1	PBX A sends a Release message to SIP gateway 1.
13	ACK—SIP gateway 1 to SIP proxy server	SIP gateway 1 sends an ACK to the SIP proxy server.
14	ACK—SIP proxy server to SIP gateway 2	The SIP proxy server sends an ACK to SIP gateway 2. The ACK confirms that the 6xx failure response has been received.
15	Release Complete—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A and the call session attempt is terminated.

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

Figure 7-44 illustrates an unsuccessful call in which User A initiates a call to User B but User B is on the phone and is either unable or unwilling to take another call.

Figure 7-44   SIP Gateway-to-SIP IP Phone—Called User is Busy

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.
2	INVITE—SIP gateway 1 to SIP IP phone	SIP 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. SIP gateway 1 sends an INVITE request to the address it receives in the dial peer which, in this scenario, is the SIP IP phone.
		In the INVITE request:
		• The IP address of the SIP IP phone is inserted in the Request-URI field.
		• PBX A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which the SIP gateway is prepared to receive the RTP data is specified.
3	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.

Step	Action	Description
4	100 Trying—SIP IP phone to SIP gateway 1	The SIP IP phone sends a 100 Trying response to SIP gateway 1. The 100 Trying response indicates that the INVITE request has been received by the SIP IP phone.
5	486 Busy Here—SIP IP phone to SIP gateway 1	The SIP IP phone sends a 486 Busy Here response to SIP gateway 1. The 486 Busy Here response is a client error response that indicates that User B was successfully contacted but User B was either unwilling or unable to take the call.
6	Disconnect (Busy)—SIP gateway 1 to PBX A	SIP gateway 1 sends a Disconnect message to PBX A.
7	Release—PBX A to SIP gateway 1	PBX A sends a Release message to SIP gateway 1.
8	ACK—SIP gateway 1 to SIP IP phone	SIP gateway 1 sends an ACK to the 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—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A and the call session attempt is terminated.

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

Figure 7-45 illustrates the call flow in which User A initiates a call to User B but User B does not answer.

Figure 7-45   SIP Gateway-to-SIP IP Phone—Called User Does Not Answer
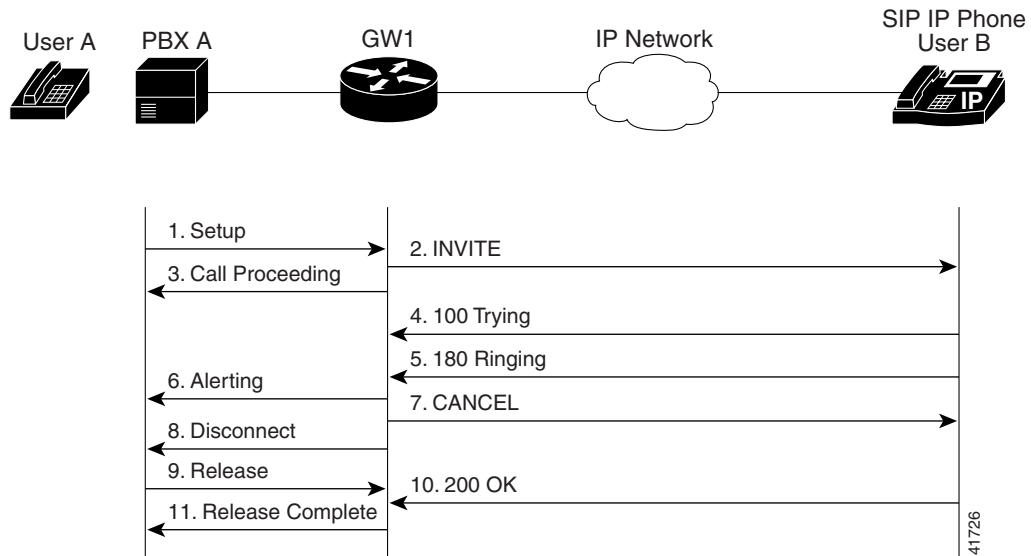

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.
2	INVITE—SIP gateway 1 to SIP IP phone	SIP gateway 1 maps the SIP URL phone number to a dial-peer. The dial-peer includes the IP address and the port number of the SIP enabled entity to contact. SIP gateway 1 sends an INVITE request to the address it receives in the dial peer which, in this scenario, is the SIP IP phone.
		In the INVITE request:
		• The IP address of the SIP IP phone is inserted in the Request-URI field.
		• PBX A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which the SIP gateway is prepared to receive the RTP data is specified.
3	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.

Step	Action	Description
4	100 Trying—SIP IP phone to SIP gateway 1	The SIP IP phone sends a 100 Trying response to SIP gateway 1. The 100 Trying response indicates that the INVITE request has been received by the SIP IP phone.
5	180 Ringing—SIP IP phone to SIP gateway 1	The SIP IP phone sends a 180 Ringing response to SIP gateway 1. The 180 Ringing response indicates that the user is being alerted.
6	Alerting—SIP gateway 1 to PBX A	SIP gateway 1 sends an Alert message to PBX A. The Alert message indicates that SIP gateway 1 has received a 180 Ringing response from the SIP IP phone. User A hears the ringback tone that indicates that User B is being alerted.
7	CANCEL (Ring Timeout)—SIP gateway 1 to SIP IP phone	Because SIP gateway 1 did not return an appropriate response within the time specified by the Expires header in the INVITE request, SIP gateway 1 sends a SIP CANCEL request to SIP gateway 2. A CANCEL request cancels a pending request with the same Call-ID, To, From, and CSeq header field values.
8	Disconnect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Disconnect message to PBX A.
9	Release Complete—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A and the call session attempt is terminated.
10	200 OK—SIP IP phone to SIP gateway 1	The SIP IP phone sends a 200 OK response to SIP gateway 1. The 200 OK response confirms that User A has received the Cancel request. The call session attempt is now being terminated.
11	Release Complete—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A and the call session is terminated.

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

Figure 7-46 illustrates an unsuccessful call in which User A initiates a call to User B and receives a class 4*xx*, 5*xx*, or 6*xx* response.

Figure 7-46   SIP Gateway-to-SIP IP Phone—Client, Server, or Global Error
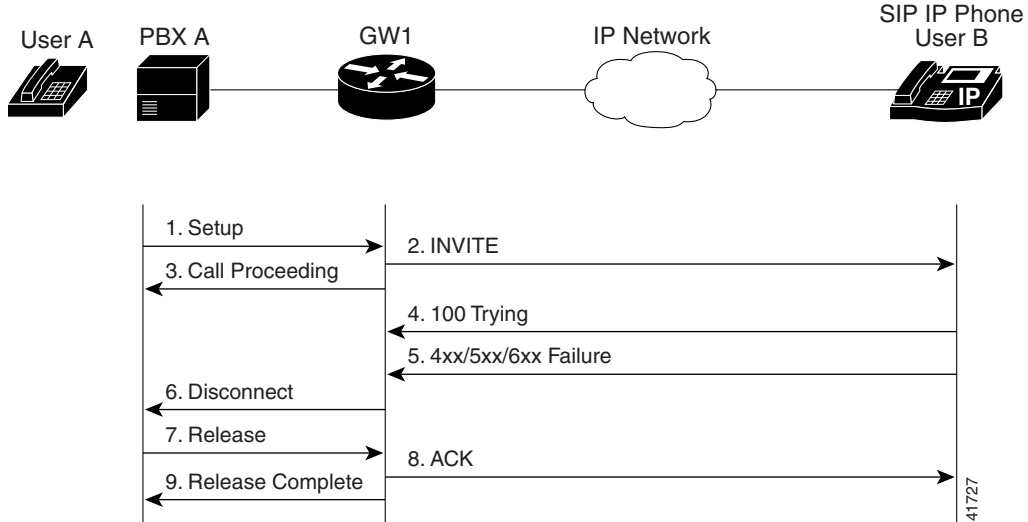

Step	Action	Description
1	Setup—PBX A to SIP gateway 1	Call Setup is initiated between PBX A and SIP gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.
2	INVITE—SIP gateway 1 to SIP IP phone	SIP gateway 1 maps the SIP URL phone number to a dial-peer. The dial-peer includes the IP address and the port number of the SIP enabled entity to contact. SIP gateway 1 sends an INVITE request to the address it receives in the dial peer which, in this scenario, is the SIP IP phone.
		In the INVITE request:
		• The IP address of the SIP IP phone is inserted in the Request-URI field.
		• PBX A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which the SIP gateway is prepared to receive the RTP data is specified.
3	Call Proceeding—SIP gateway 1 to PBX A	SIP gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.

Step	Action	Description
4	100 Trying—SIP IP phone to SIP gateway 1	The SIP IP phone sends a 100 Trying response to SIP gateway 1. The 100 Trying response indicates that the INVITE request has been received by the SIP IP phone.
5	4xx/5xx/6xx Failure—SIP IP phone to SIP gateway 1	The SIP IP phone sends a class 4*xx*, 5*xx*, or class 6*xx* failure response to SIP gateway 1. Depending on which class the failure response is, the call actions differ.
		If the SIP IP phone sends a class 4*xx* failure response (a definite failure response that is a client error), the request will not be retried without modification.
		If the SIP IP phone sends a class 5*xx* failure response (an indefinite failure that is a server error), the request is not terminated but rather other possible locations are tried.
		If the SIP IP phone sends a class 6*xx* failure response (a global error), the search for User B is terminated because the 6*xx* 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.
6	Disconnect—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release message to PBX A.
7	Release—PBX A to SIP gateway 1	PBX A sends a Release message to SIP gateway 1.
8	ACK—SIP gateway 1 to SIP IP phone	SIP gateway 1 sends an ACK to the SIP IP phone. The ACK confirms that User A has received the 4xx/5xx/6xx failure response. The call session attempt is now being terminated.
9	Release Complete—SIP gateway 1 to PBX A	SIP gateway 1 sends a Release Complete message to PBX A and the call session attempt is terminated.

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

Figure 7-47 illustrates an unsuccessful call in which User A initiates a call to User B but User B is on the phone and is either unable or unwilling to take another call.

Figure 7-47   SIP IP Phone-to-SIP IP Phone—Called User is Busy

Step	Action	Description
1	INVITE—SIP IP phone A to SIP IP phone B	SIP IP phone A sends an INVITE request to SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
2	486 Busy Here—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a 486 Busy here message to SIP IP phone A. The message indicates that SIP IP phone B is in use and the user is either unwilling or unable to take additional calls.
3	ACK—SIP IP phone A to SIP IP phone B	SIP IP phone A sends an ACK to SIP IP phone B. The ACK confirms that SIP IP phone A has received the 486 Busy here response from SIP IP phone B.

SIP IP Phone-to-SIP IP Phone—Call Screening Based on Caller

If your SIP proxy server has the capability, you can configure the proxy with lists that restrict incoming calls to only those from a list of allowed numbers. Figure 7-48 illustrates an unsuccessful call in which User A initiates a call to User B but User B has implemented a call screening list on the SIP proxy server and User A is not on that list.

Figure 7-48   SIP IP Phone-to-SIP IP Phone—Call Screening Based on Caller

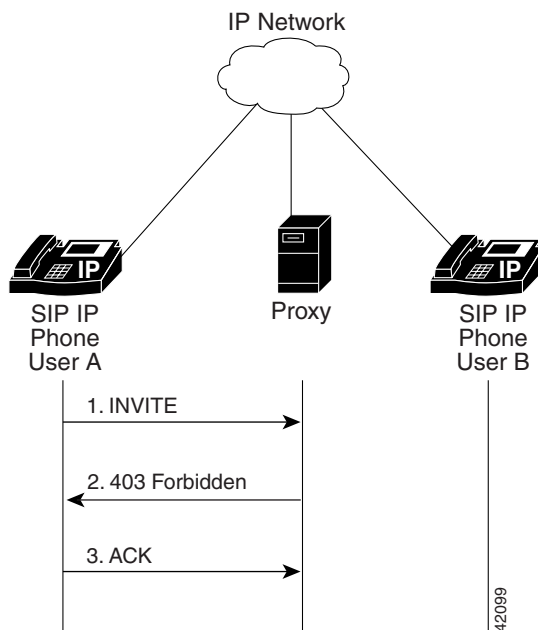| Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	SIP IP phone A sends an INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
2	403 Forbidden—SIP proxy server to SIP IP phone A	The SIP proxy server sends a 403 Forbidden message to SIP IP phone A. The message indicates that the SIP proxy server has received and understood the request but will not provide the service. In this instance, it is because the administrator has implemented a call screening list for User B and User A is not on that list.

| 3 | ACK—SIP IP phone A to SIP proxy server | SIP IP phone A sends an ACK to the SIP proxy server. The ACK confirms that SIP IP phone A has received the 403 Forbidden response from the SIP proxy server. |

SIP IP Phone-to-SIP IP Phone—Disallowed List

If your SIP proxy server has the capability, you can configure the proxy with lists that block outgoing calls to certain numbers or certain classes of numbers, such as 900 numbers.

Figure 7-49 illustrates an unsuccessful call in which User A initiates a call to User B but the SIP proxy server has been configured to block calls from User A to User B.

Figure 7-49   SIP IP Phone-to-SIP IP Phone—Disallowed List

Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	SIP IP phone A sends an INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: • The phone number of User B is inserted in the Request-URI field in the form of a SIP URL. • SIP IP phone A is identified as the call session initiator in the From field. • A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. • The transaction number within a single call leg is identified in the CSeq field. • The media capability User A is ready to receive is specified.

2	403 Forbidden—SIP proxy server to SIP IP phone A	The SIP proxy server sends a 403 Forbidden message to SIP IP phone A. The message indicates that the SIP proxy server has received and understood the request but will not provide the service. In this instance, it is because the administrator has implemented a disallow list that prevents User A from making calls to User B.
3	ACK—SIP IP phone A to SIP proxy server	SIP IP phone A sends an ACK to the SIP proxy server. The ACK confirms that SIP IP phone A has received the 403 Forbidden response from the SIP proxy server.

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

Figure 7-50 illustrates an unsuccessful call in which User A initiates a call to User B but User B does not answer.

Figure 7-50   SIP IP Phone-to-SIP IP Phone—Called User Does Not Answer

Step	Action	Description
1	INVITE—SIP IP phone A to SIP IP phone B	SIP IP phone A sends an INVITE request to SIP IP phone B. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
2	180 Ringing—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a 180 Ringing response to SIP IP phone A.
3	CANCEL (Ring Timeout)—SIP IP phone A to SIP IP phone B	SIP IP phone A sends a CANCEL request to SIP IP phone B to cancel the invitation.

Step	Action	Description
4	200 OK—SIP IP phone B to SIP IP phone A	SIP IP phone B sends a 200 OK response to SIP IP phone A. The response confirms receipt of the cancellation request.

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

Figure 7-51 illustrates an unsuccessful call in which User A initiates a call to User B but User B does not answer.

Figure 7-51   SIP IP Phone-to-SIP IP Phone—Authentication Error

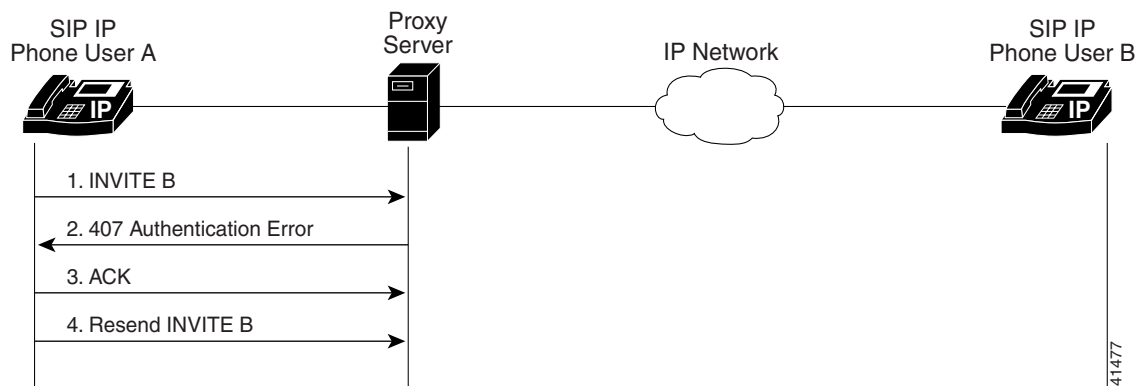

Step	Action	Description
1	INVITE—SIP IP phone A to SIP proxy server	SIP IP phone A sends an INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The phone number of User B is inserted in the Request-URI field in the form of a SIP URL.
		• SIP IP phone A is identified as the call session initiator in the From field.
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
2	407 Authentication Error—SIP proxy server to SIP IP phone A	SIP proxy server sends a 407 Authentication Error response to SIP IP phone A.
3	ACK—SIP IP phone A to SIP proxy server	SIP IP phone A sends a ACK to the SIP proxy server acknowledging the 407 error message.
4	Resend INVITE—SIP IP phone A to SIP proxy server	SIP IP phone A resends an INVITE to the SIP proxy server. The INVITE includes the Proxy-authenticate header with authentication credentials.

A

AAA   authentication, authorization, and accounting. The network security services that provide the primary framework through which you set up access control on your router or access server.

address resolution   Generally, a method for resolving differences between computer addressing schemes. Address resolution usually specifies a method for mapping network layer (Layer 3) addresses to data link layer (Layer 2) addresses.

agent   An object or application that can be a server, a client, or both.

ASCII   American Standard Code for Information Interchange. 8-bit code for character representation (7 bits plus parity).

C

call   Establishment of (or attempt to establish) a voice or data connection between two endpoints, or between two points which provide a partial link (e.g. a trunk) between two endpoints.

CAS   Channel Associated Signaling. In E1 applications, timeslot 16 is used to transmit CAS information. Each frame's timeslot 16 carries signaling information (ABCD bits) for two of the B channel timeslots.

CDR   Call Record Detail. A term used to describe log records for calling services. This includes such information as where the call originated, what the start time was, who the call was made to, what time the call ended, etc.

CO   central office. A local switching system that connects lines to lines and lines to trunks. Sometimes used to refer to the building in which a switching system is located and the associated equipment. Also the physical point where calls enter the long distance network. Sometimes referred to as Class 5 office, end office, or Local Dial Office.

Codec   Coder-Decoder. Transforms analog voice into digital bit stream and vice-versa.

D

DAL   Dedicated Access Line. An analog special-access line that runs from a caller's own equipment directly to a long distance company's switch or POP. Usually provided by a local telephone company. The line may go through the local telco central office, but the local telco does not switch calls on this line.

DHCP   Dynamic Host Control Protocol. A protocol that is used to dynamically allocate and assign IP addresses. DHCP allows you to move network devices from one subnet to another without administrative attention. RFC 2131 and RFC 2132

dial peer   An addressable call endpoint. In Voice over IP (VoIP), there are two types of dial peers: POTS and VoIP.

dial plan   A description of the dialing arrangements for customer use on a network.

DNIS   Dialed Number Identification Service. A feature of 800 and 900 lines that provides the number the caller dialed. DNIS allows one trunk group to service multiple applications, thus requiring fewer phone lines. For example, you could give one 800 number to callers in New York, one to callers in Chicago, and one to callers in LA. With DNIS, one trunk could be used to answer all those calls, playing a different, customized recording for each number called.

DNS   Domain Name System. System used in the Internet for translating names of network nodes into addresses.

DSL   Digital Subscriber Line. Public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: ADSL, HDSL, SDSL, and VDSL. All are provisioned via modem pairs, with one modem located at a central office and the other at the customer site. Because most DSL technologies do not use the whole bandwidth of the twisted pair, there is room remaining for a voice channel.

DTMF   Dual Tone Multi Frequency: The paired, high- and low-frequency tones which make up touch tone dialing.

E

E1   Wide-area digital transmission scheme. E1 is the European equivalent of a T1 line. The E1's higher clock rate (2.048 MHz) allows for 32 64 Kbps channels, which include one channel for framing and one channel for D-channel information.

E.164   ITU-T recommendation for international telecommunication numbering, especially in ISDN, BISDN, and SMDS. An evolution of standard telephone numbers.

end point   SIP or H.323 terminal or gateway. An endpoint can call and be called. It generates and terminates the information stream.

G

G.729   An ITU-T algorithm for voice encoding that produces an 80-bit voice sample every 10 msec (bit rate of 8 kbps). The codec works in blocks of 10 msec and so it is possible to generate frames of multiple 10 msec duration.

Gateway   The server that connects the VoIP network with PBXs and PSTN devices.

H

H.323   Recommendation from the ITU that sets standards for multimedia communications over IP networks. It also addresses call control, multimedia management, and bandwidth management.

HTTP   Hypertext Transfer Protocol. The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.

HTTP digest A password-based authentication method supported by LDAP servers.

I

ICMP   Internet Control Message Protocol. A network-layer Internet protocol that reports errors and provides other information relevant to IP packet processing. RFC792

IE   Information element.

IETF   Internet Engineering Task Force. Task force consisting of over 80 working groups responsible for developing Internet standards. The IETF operates under the auspices of ISOC.

IMAP   Internet Message Access Protocol. A UNIX server protocol allowing users to scan message headers, download selected messages, and administer e-mail folders.

IP   Internet Protocol. A network-layer protocol in the TCP/IP stack that offers a connectionless internetwork service. IP provides features for addressing, type-of-service (ToS) specification, fragmentation and reassembly, and security. RFC791

IPSec   IP Security. An IETF standard that is used to provide security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices ("peers"), such as Cisco routers.

ISDN   Integrated Services Digital Network. A communications protocol, offered by telephone companies, that permits telephone networks to carry data, voice, and other traffic.

ISP   Internet Service Provider. Company that provides Internet access to other companies and individuals.

ITU   International Telecommunications Union. Established by the United Nations, with membership from virtually every world government. Three primary goals are: defining and adopting telecommunications standards; regulating use of the radio frequency spectrum; and furthering world-wide telecommunications development.

IVR   Integrated voice response. Consists of simple voice prompting and digit collection to authenticate user and identify call destination.

L

LDAP Lightweight Directory Access Protocol. An emerging software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network.

LEC Local Exchange Carrier. Local or regional telephone company that owns and operates a telephone network and the customer lines that connect to it.

location server A device that processes requests (typically from a redirect or proxy server) to provide information about the possible location of a target end user.

M

MGC Media gateway controller. A device that provides control of media and signalling gateways.

MGCP Media Gateway Control Protocol. Protocol that helps bridge the gap between circuit-switched and IP networks. A combination of Internet Protocol Device Control (IPDC) and Simple Gateway Control Protocol (SGCP). MGCP allows external control and management of data communications devices, or "media gateways" at the edge of multiservice packet networks by software programs.

MIB Management Information Base - A directory of logical names of information resources residing in a network and pertaining to the network's management.

MIME Multipurpose Internet Mail Extension. A set of extensions to the SMTP message syntax allowing various file types to be attached to text mail.

Mu-Law The PCM voice coding and companding standard used in Japan and North America. A PCM algorithm yielding a raw 64-kbps transmission rate.

N

name mapping Generally, the process of associating a name with a network location.

NTP Network Time Protocol. The recommended protocol for synchronizing the time of hosts in the uOne network.

P

PBX Private Branch Exchange. Privately-owned central switching office.

PCM Pulse Code Modulation. The form of modulation in which the information signals are sampled at regular intervals and a series of pulses in coded form are transmitted representing the amplitude of the information signal at that time. For T1 applications, a method of converting successive (every 125 us) analog samples of a voice waveform to successive 8-bit codes, to be transmitted in an 8-bit timeslot of a T1 frame. In "robbed bit" frames, only the most significant 7 bits are used to encode the sample. The total bit rate for such a channel is (8000 samples/sec) x (8-bits/sample) = 64000 bits/sec.

POTS	Plain Old Telephone Service. Basic telephone service supplying standard single line telephones, telephone lines, and access to the Public Switched Telephone Network.
PRA	Primary Rate Access. A Canadian term synonymous with ISDN PRI.
PRI	Primary Rate Interface. PRI is an ISDN interface to primary rate access. Primary rate access consists of a single 64 Kbps D channel plus 23 T1 or 30 E1 B channels for voice or data.
proxy server	An intermediate device that receives SIP requests from a client and then initiates requests on the client's behalf.
PSTN	Public Switched Telephone Network. PSTN refers to the local telephone company.

Q

Q.931	Call signaling protocol for setup and termination of calls.
Q.SIG	Q Signaling. An inter-PBX signaling protocol for networking PBX supplementary services in a multi- or uni-vendor environment.

R

RADIUS	Remote Authentication Dial-In User Service. An authentication and accounting system used by many Internet Service Providers (ISPs).
RAS	Registration, Admission, Status. Protocol used in the H.323 protocol suite for discovering and interacting with a Gatekeeper.
redirect server	A device that 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.
registrar server	A device that processes requests from UACs for registration of their current location. Registrar servers are often co-located with a redirect or proxy server.
RFC	Request For Comments. Document series used as the primary means for communicating information about the Internet. Some RFCs are designated by the IAB as Internet standards. Most RFCs document protocol specifications such as Telnet and FTP, but some are humorous or historical. RFCs are available online from numerous sources.
RPC	Remote Procedure Call. An external form of communication that allows objects to communicate with each other over the network. The RPC programming interface is built into each server's Client and Server subsystems to provide external communication among servers.
RSVP	IETF specification that allows applications to request dedicated bandwidth.

RTP/RTCP   Real-time Transfer Protocol/RTP Control Protocol. An IETF specification for audio and video signaling management. Allows applications to synchronize and spoil audio and video information. RTP connections are established between DAP servers across the Internet after voice has been converted to IP format.

RTSP   Real Time Streaming Protocol. Proposed standard for controlling streaming data over the World Wide Web.

S

SAP   Session Announcement Protocol. A protocol used to assist in the advertisement of multicast multimedia conferences and other multicast sessions, and to communicate the relevant session setup information to prospective participants.

SDP   Session Description Protocol. A protocol used to describe the characteristics of multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation. RCS 2327

signaling   Process of sending a transmission signal over a physical medium for purposes of communication.

SIP   Session Initialization Protocol. Offers many of the same architectural features as H.323, but relies on IP-specific technologies, such as DNS. It also incorporates the concept of fixed port numbers for all devices and allows for the use of proxy servers.

SNMP   Simple Network Management Protocol. The Internet standard protocol developed to manage nodes on an IP network.

SS7   Signaling System 7. The protocol used to communicate between components of the AIN. The SS7 protocol is used to set up and tear down phone calls as well as to enable "intelligent" services. The SS7 network is a physically separate network from the phone network used to transmit voice data.

T

T1   Digital WAN carrier facility. T1 transmits DS-1 formatted data at 1.544 Mbps through the telephone-switching network, using AMI or B8ZS coding. T1 is the North American equivalent of an E1 line.

TCL   Tool command language.

TCP   Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

TFTP   Trivial File Transfer Protocol. Allows files to be transferred from one computer to another over a network.

U

UA	User Agent. See **UAC** and **UAS**.
UAC	User Agent Client. In SIP, a client application that initiates the SIP request.
UAS	User Agent Server. In SIP, 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.
UCS	Unified call services.
UDP	A connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. RFC768
URL	Uniform Resource Locator. An identifier used to locate content that is transported via the HTTP protocol.

V

VFC	Voice feature card.
VNM	Voice network module.
VoIP	Voice over IP. The ability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality.