CHAPTER 2

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

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 using Cisco products. This is the second of a series of releases of this solution, which provides basic services and works with a number of enhanced services. The first release enabled the components to be used to implement toll bypass, effect dedicated-access-line (DAL) replacement, and 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. This second release introduces the following additional capabilities:

- Enhanced SIP proxy-server administration
- Integration of MSN’s SIP VoIP-enabled Messenger
- RSVP and TEL url
- SIP T.38 fax relay
- SIP INVITE request with malformed Via header
- SIP gateway support for the bind command
- Configurable PSTN cause code to SIP response mapping

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, 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 Implementation

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

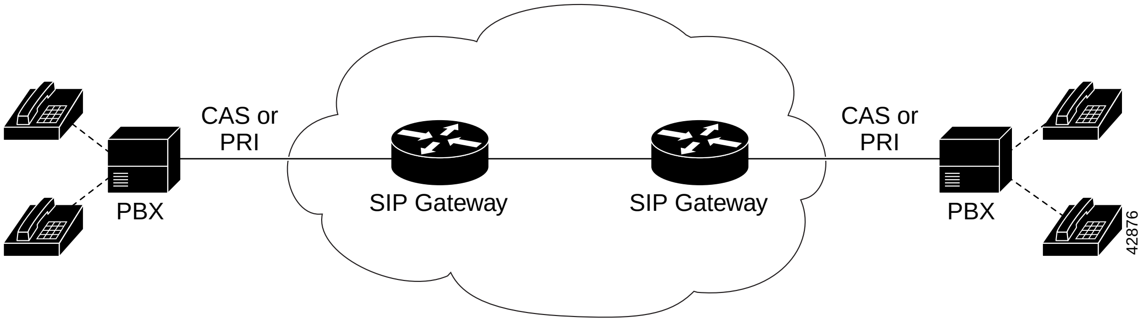
Intranetwork Phased Approach Implementation

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

Phase 1: Toll Bypass 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 bypass carrier toll lines. In Figure 2-1, Cisco SIP gateways and an IP network have been introduced between the private branch exchanges (PBXs).

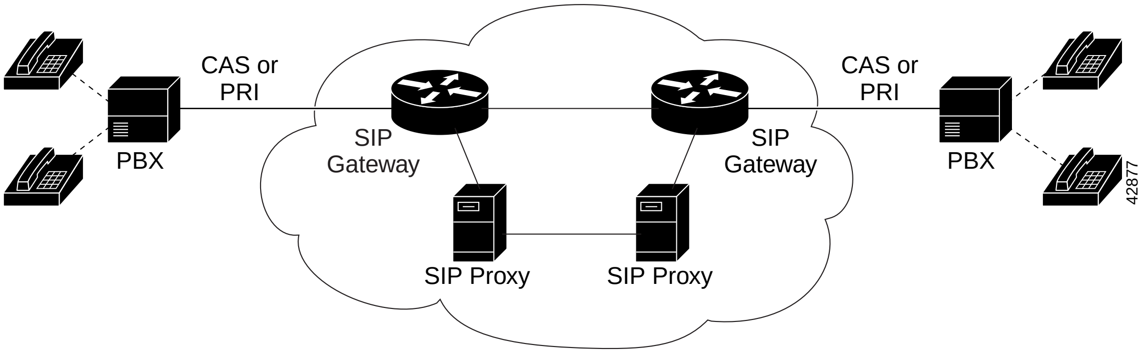
Figure 2-1 Toll Bypass and DAL Replacement



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.

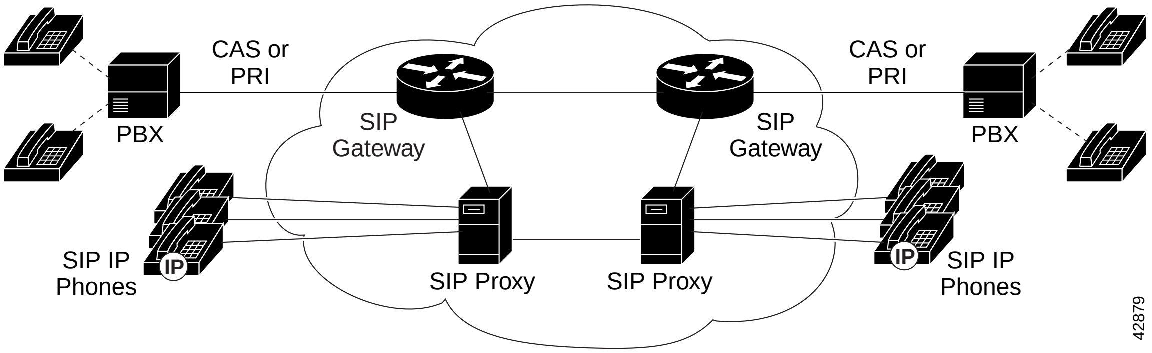
Figure 2-2 Scalable Private Number Plan Support



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.

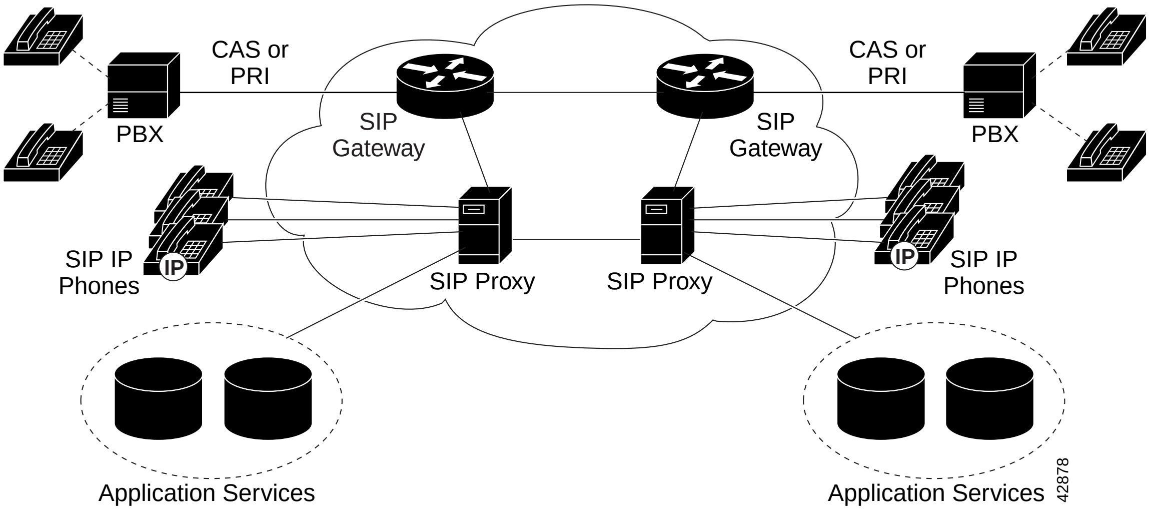
Figure 2-3 Cisco SIP IP phone Support



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 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.

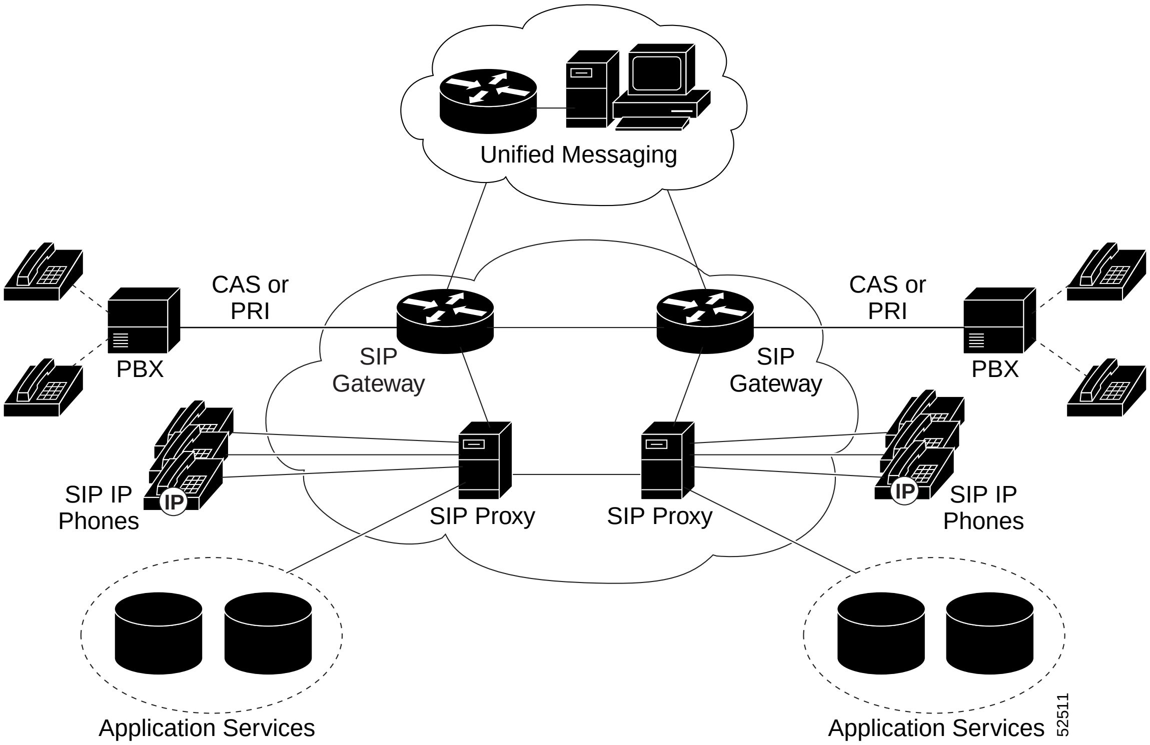
Figure 2-4 Application Services Support



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, Cisco SIP IP phones, Cisco SIP gateways, and 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.

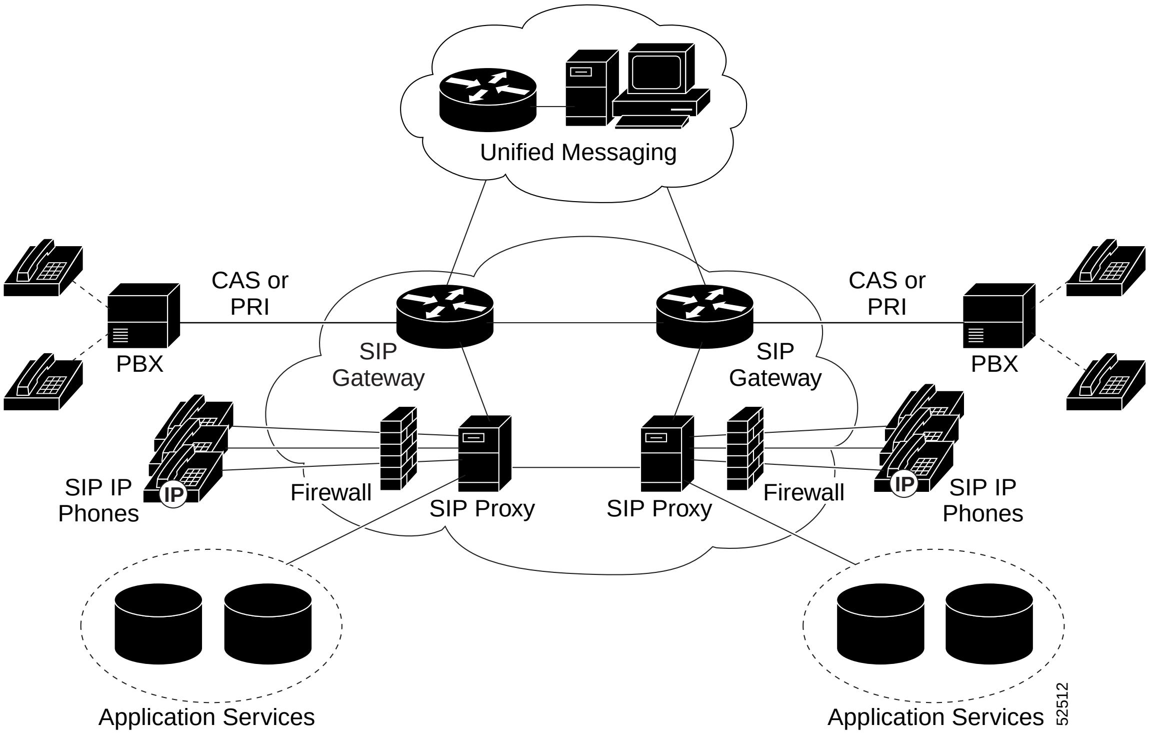
Internetwork Phased Approach Implementation

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-switched-telephone-network (PSTN) infrastructure. This phased approach builds on an existing SIP VoIP network as outlined in the "Intranetwork Phased Approach Implementation" section on page 2-2.

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.

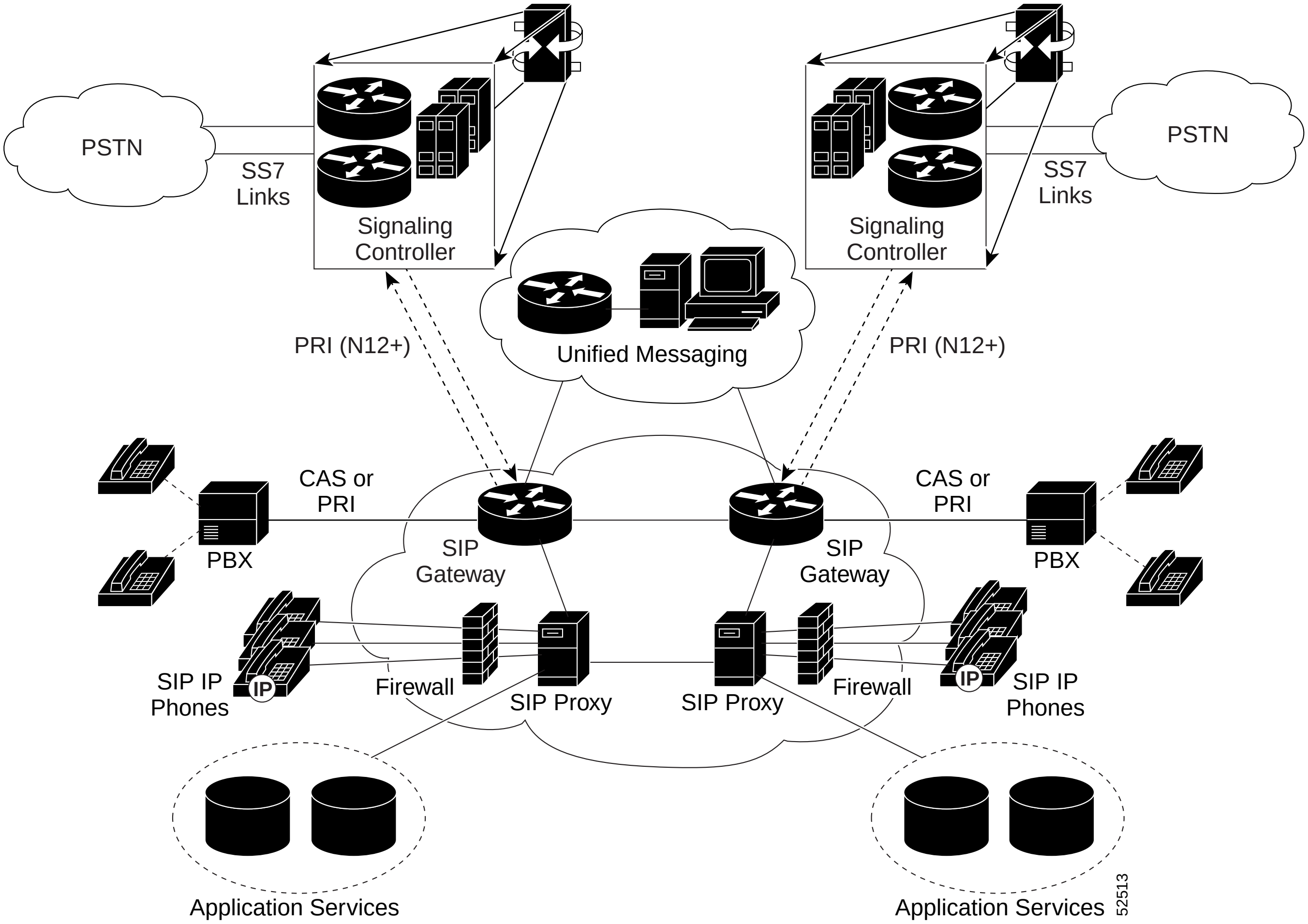
Figure 2-6 The Cisco Secure PIX Firewall in a SIP Network



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

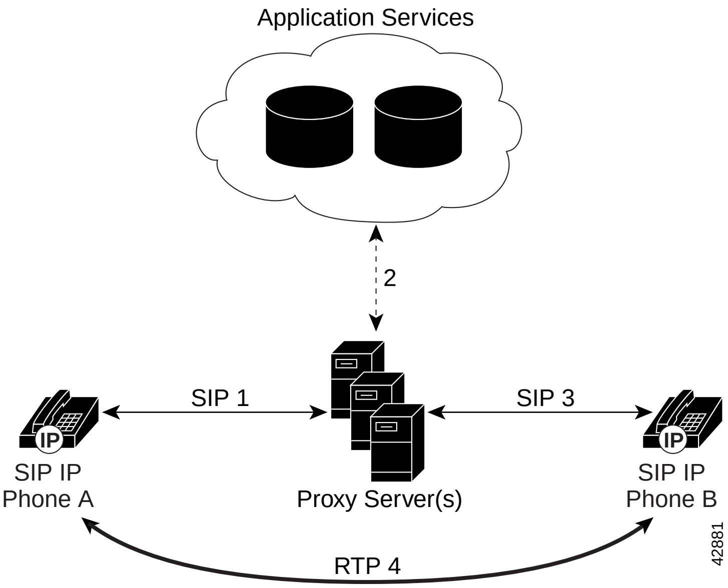
Figure 2-7 Cisco SS7 Interconnect for Voice Gateways Solution Implemented with a SIP VoIP Network



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, the following sequence occurs:

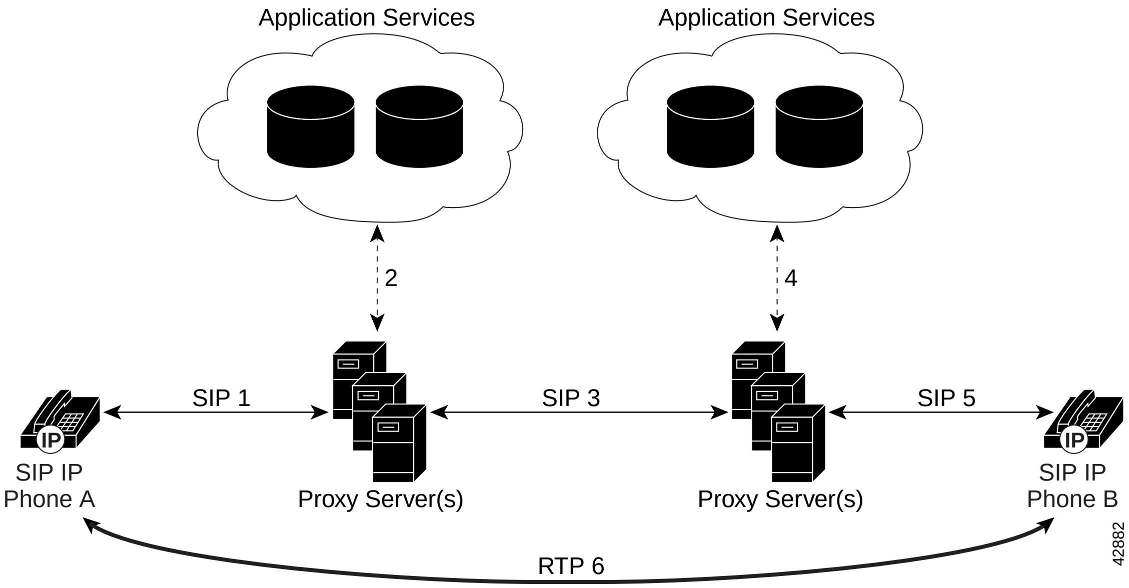
1. Cisco SIP IP phone A initiates a call by sending an INVITE message to the SIP proxy server. (There can be more than one proxy server for redundancy.)
2. The SIP proxy server interacts with the location server and possibly with application services to determine user addressing, location, or features.
3. The SIP proxy server then proxies the INVITE message to the destination phone.
4. Responses and acknowledgments are exchanged, and 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, the following sequence occurs:

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 contacts the destination phone (Cisco SIP IP phone B).
6. Responses and acknowledgments are exchanged, and an RTP session is established between Cisco SIP IP phones A and B.

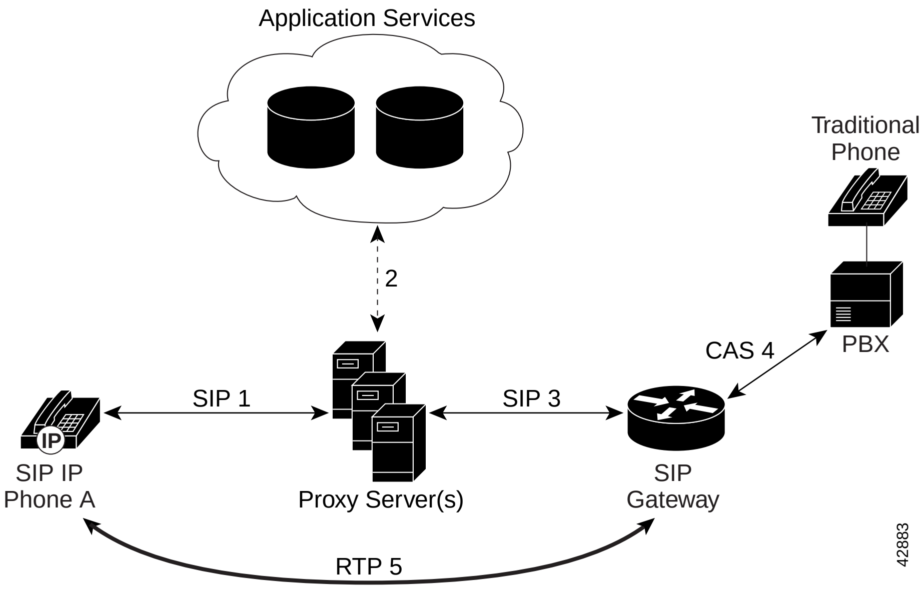
Note SIP 200 OK, 180 Ringing, and 183 Session Progress messages pass through the same set of proxies, for they are in the same call sequence (cseq). SIP CANCEL or BYE requests sent by a terminating user agent might or might not pass through the same set of proxies.

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 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 PSTN.

Figure 2-10 Calls Between a SIP IP Telephony Network and a Traditional Telephony Network



In this illustration, the following sequence occurs:

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. Responses and acknowledgments are exchanged, and 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.

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

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 voice-mail server.

Components of the Cisco VoIP Infrastructure Solution for SIP

The Cisco VoIP Infrastructure Solution for SIP is composed of the following components:

- SIP IP phone (Cisco Systems’ SIP IP Phone 7960)
- SIP gateway (integrated with Cisco Systems’ IOS software)
- SIP proxy server (Cisco SIP Proxy Server)
- Firewall (Cisco Secure PIX Firewall)
- 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 telephone 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 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 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.

Tip To learn more about how to use and administer the Cisco SIP IP phone model 7960, see documentation available from the following website: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/ipp7960/index.htm

Cisco SIP IP Phone Features

The Cisco SIP IP phone provides the following operating features:

- Adjustable ring tone
- Hearing-aid compatible handset
- Headset compatibility
- Integrated two-port Ethernet switch that allows the telephone and a computer to share a single Ethernet jack
- Direct connection to a 10BaseT or 100BaseT Ethernet (RJ-45) network (half- or full-duplex connections are supported)
- Large (4.25 x 3 in.) display with adjustable contrast
- G.711 (mu-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

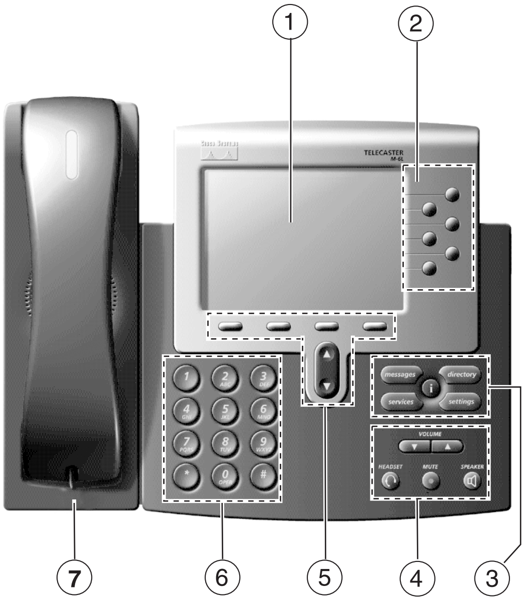
- Local directory configuration (save and recall) and automatic dial completion—Each time a call is successfully made or received, the number is stored in a local directory that is maintained on the phone. The maximum number of entries is 32. Entries are aged-out based on their usage and age. The oldest 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 appears as shown in Figure 2-11.

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

Figure 2-11 Cisco Systems' SIP IP Phone



The areas noted above are as follows:

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 buttons.

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 supports the following features:

- Variety of signaling protocols, including Integrated Services Digital Network (ISDN) PRI and CAS
- Variety of interfaces, including:
  - Analog interfaces: FXS/FXO/E&M analog interfaces
  - Digital interfaces: T1 CAS, E1 CAS, and PRI
- 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
- SIP over TCP and UDP network protocols
- RTP/RTCP for media transport in VoIP networks
- The following codecs:

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

- Record-route headers
- IP Security (IP Sec) for SIP signaling messages
- AAA . 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.
- Call hold. A mid-call INVITE message is received, which requests that the remote endpoint stop sending media streams.
- 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.

- Configurable expiration time for SIP INVITEs and maximum number of proxies or redirect servers that can forward a SIP request
- 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
- Early media from PSTN

The Cisco SIP Proxy Server

The Cisco SIP Proxy Server 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. It can also be configured to provide additional server modes and features. For example, the Cisco server can be configured to do the following:

- 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, messaging server, and 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 the following:

- Storage of subscriber personal greetings and distribution list recorded names
- Temporary storage of faxes to be printed, messages that cause SMS notifications, and outbound AMIS-A messages

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

- 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 profiles.

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

- 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 do the following:
  - Manage special administrative accounts
  - Broadcast lists and user mailbox security
  - Administer subscribers and AMIS-A users, classes of service, and pager and SMS notification
  - Validate subscriber entries

  uOne Administration updates both the directory and messaging servers.
- PMA—This web-based tool allows subscribers 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 batch mode. It 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 2-1)
- Subscriber services (Table 2-2)

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 the following:
  - CODEC switching within a call
  - Single Number Reach (SNR) services
- A uOneSIP system supports Netscape messaging and directory servers for Internet Message Access Protocol (IMAP) / Lightweight Directory Access Protocol (LDAP) servers.

Note Table 2-1 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, and 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)

Feature	Description
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.
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 urgent, new messages and skip to 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 “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.

Table 2-3 Subscriber Services (continued)

Feature	Description
Standard voice-message handling	Standard voice messages are played in “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 indicates 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 reinventory is on, voice messages are reinventoried when a subscriber returns to the main menu. If reinventory is off, the voice messages are inventoried only once (at the beginning of a session).

Table 2-3 Subscriber Services (continued)

Feature	Description
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.

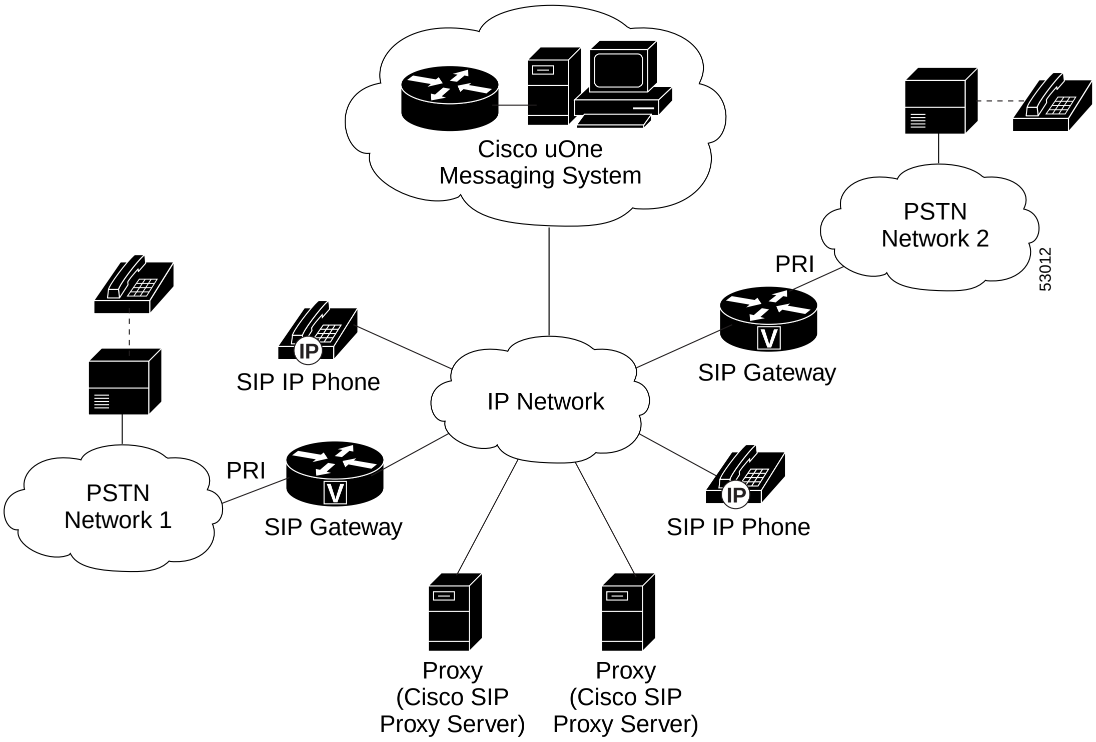
Flexible Deployment Scenarios

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*