

Large-Scale H.323 Network Design for Service Providers

by Vikas Butaney and Stephen Liu

TME's VoIP

Introduction

In today's highly competitive communications industry, service providers must find new ways to increase revenue and leverage their existing network infrastructure. Many service providers have already deployed networks consisting of Cisco solutions to provide data services to their subscribers. For them, packet telephony is a readily deployable, value-added, revenue-generating application that leverages the Cisco technology's data-handling capabilities.

What is Packet Telephony?

Packet-switched technology has expanded from data-only applications to take on the functions of traditional circuit-switched equipment. While the lower cost of packet-switched networks initially drove this change, the improving quality and reliability of voice over these networks is speeding integration of voice and data services. As a result, today's voice networks will eventually be replaced by packet infrastructure over the next decade.

Cisco open packet telephony (OPT) is the foundation for these new services. Because it opens the call-control function to new services, it enables service providers to get to market faster with best-of-class solutions. Furthermore, OPT delivers carrier-class voice quality, so service providers can deploy packet voice services with confidence as they seamlessly extend the reach of traditional voice networks. OPT is based on open interfaces and standards, allowing an ecosystem of partners to work together to develop innovative network services. Built for both IP and ATM transport, OPT offers integrated services for subscribers using a wide variety of access technologies including analog, DSL, ISDN, wireless, wireless local loop, and cable. Thus OPT makes optimal use of existing bandwidth to support migration, rather than replacement, of existing equipment. This standards-based, multivendor approach also allows OPT networks to scale cost-effectively. Service providers can therefore profitably expand into new locales and additional consumer and enterprise markets.

Where Is Packet Telephony Technology Today?

While various packet telephony solutions exist, H.323 is available with the features to deploy networks today. Cisco solutions incorporating H.323 are mature, widely accepted, and currently shipping, while other options are still maturing. This design guide has been created to help the reader understand the Cisco implementation of H.323 and, through a typical design example, illustrate how service providers can successfully and profitably deploy H.323v2-based packet telephony services.

An H.323 Primer

H.323 is an existing specification defined by the International Telecommunication Union (ITU), which has been available since 1996. Version 2 was approved in January 1998 and Version 3 is currently being defined. The wide acceptance and maturity of this standard offers service providers a high level of confidence when deploying packet telephony solutions with Cisco equipment.

H.323 is a specification for transmitting multimedia (data, voice, and video) across any packet-based network. This packet-based network can be IP, IPX, or any other protocol. Cisco supports H.323 over IP networks. H.323 also allows for standards-based interoperability with other vendors' H.323-compatible equipment.

H.323 defines four functional components: H.323 terminals, H.323 Multi-point Control Units (MCUs), H.323 gateways, and H.323 gatekeepers, as well as the protocols used by these devices to communicate with each other.

The most elemental component of H.323 is the H.323 terminal. Other endpoints, such as gateways and MCUs, leverage the definitions specified in the H.323 terminal. The H.323 terminal is described by audio, video, data, system control, and media-streaming capabilities. At a minimum, H.323-compliant terminals are required to carry voice, while video and data are optional. For voice, H.323 mandates that the G.711 audio CODEC is supported while G.722, G.723, G.723.1, G.728, and G.729 CODECs are optional. For video CODECs, H.261 is mandatory while H.263 is an option. The T.120 specification is used for applications such as workgroup data collaboration.

In addition to referencing T.120 and various codec specifications, H.323 is further defined by a mixture of existing recommendations for call control, system control, and endpoint communication with gatekeepers. H.225 messages define call control functions and utilize a scaled-down version of Q.931 to set up the connection between two H.323 endpoints. These H.225 messages consist of Q.931 setup, call proceeding, alerting, connect, facility, and release.

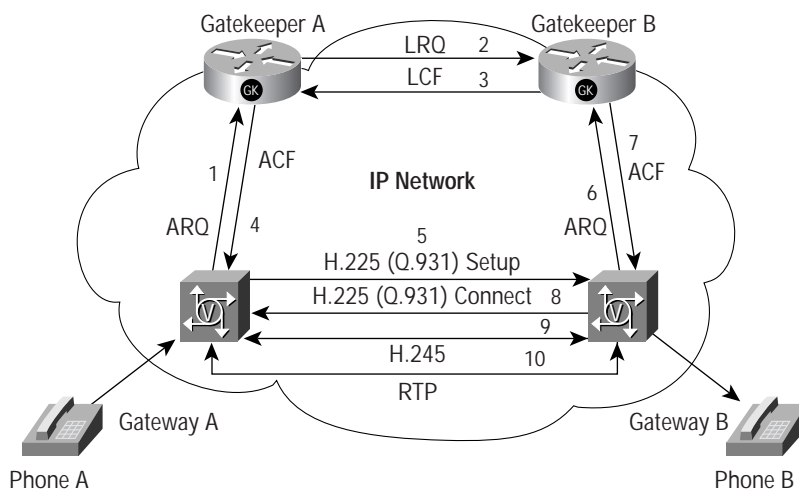
H.245 specifies the system control messages in H.323. It uses TCP to provide reliable transport for capabilities exchange, mode preference from the receiving end, master/slave determination, logical channel signaling, and control and indication. Capabilities exchange specifics include things such as which CODECs are available for use in the VoIP call leg.

Registration, admission, and status (RAS) messages are used for H.323 endpoints to communicate with H.323 gatekeepers. RAS discovery messages help the end point "discover" a gatekeeper by sending a gatekeeper request (GRQ) message. After receiving a gatekeeper request, a gatekeeper can respond with a gatekeeper confirm (GCF) message, or a gatekeeper reject (GRJ) message.

Once an endpoint has discovered the available gatekeepers, it attempts to register with one of them using a registration request (RRQ) RAS message that contains information about the endpoint. The gatekeeper then responds with a registration confirm (RCF) message if it is alright to register with that gatekeeper, or a registration reject (RRJ) if it is not. Having responded with an RCF, the gatekeeper creates a table from this information that defines with which IP address each E.164 address and H.323 alias corresponds.

After successfully registering with the gatekeeper, the endpoint must ask permission of the gatekeeper before sending or receiving a phone call using admission request (ARQ) RAS messages. Figure 1 demonstrates how a gateway (GW) places a H.323 call with the help of a gatekeeper (GK). The gatekeeper then replies with an admission confirm (ACF), or an admission reject (ARJ).

Figure 1 RAS Messages



There are several other useful types of RAS messages. Disconnect request (DRQ/DCF/DRJ) is invoked upon completion of the call. If the local gatekeeper cannot handle the call, the location request (LRQ/LCF/LRJ) can be sent to other gatekeepers to determine which one can service the particular number. Information request (IRQ/ICF/IRR) can be used to provide the periodic status of active calls. Bandwidth request (BRQ/BCF/BRJ) can increase or decrease available bandwidth to support active calls. Finally, an unregistration request (URQ/UCF/URJ) message can enable a gatekeeper to disassociate itself from an endpoint, or an endpoint to disassociate itself from a gatekeeper.

Finally, the H.323 terminal defines the use of Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP) for streaming media over IP. After the H.323 call setup and control process is completed, audio and video packets are sent via User Datagram Protocol (UDP). To assist with streaming audio and video, the specification calls for an RTP header. RTP headers contain a time stamp and sequence number, allowing the receiving device to buffer as much as necessary to remove jitter and latency by synchronizing the packets to play back a continuous stream of sound.

The RTP specification stipulates that the RTP server is to use an even port number, whereas RTCP is to use the next-available odd number. RTCP, used to control RTP, gathers reliability information and periodically passes this information onto session participants. RTCP cannot use more than 5 percent of the session bandwidth used by RTP.

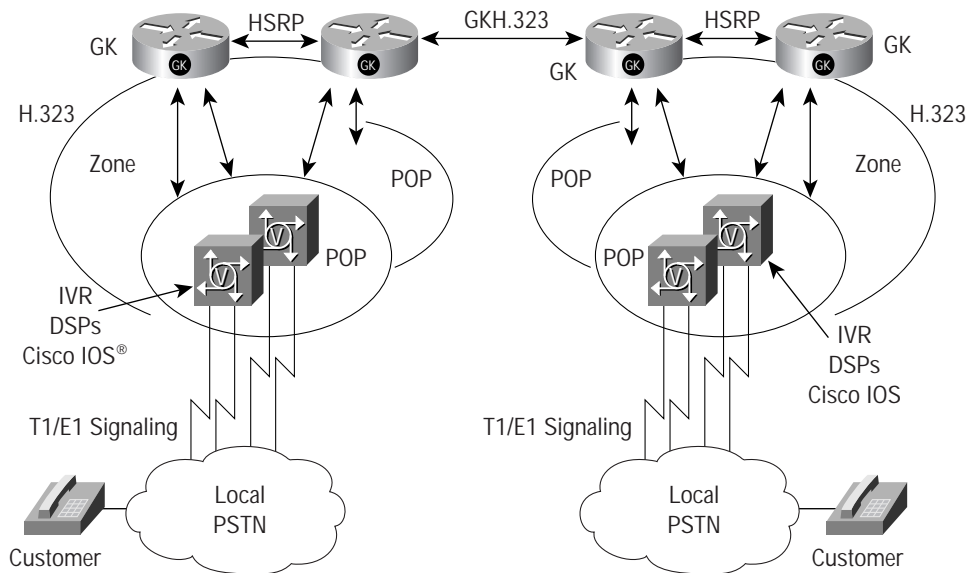
The H.323 gateway is simply an H.323 terminal with added responsibility. An H.323 gateway provides a gate between the IP world and other network types such as the Public Switched Telephone Network (PSTN), H.320, V.70, and H.324. To do this, the gateway must reflect all characteristics on one network to the other. For example, call signaling from the PSTN side must be accurately mapped into the Voice over IP (VoIP) side and vice versa. Likewise, media from the PSTN side must be reflected into the VoIP side and vice versa. Cisco gateways currently provide PSTN to H.323 gateway functions.

An H.323 gatekeeper performs address translation, admission control, bandwidth management, and zone management. Cisco 2600 and Cisco 3600 are examples of multimedia gatekeepers (data, voice, and video)—but cannot currently function as gateways and gatekeepers simultaneously.

Anatomy of a VoIP Network

To understand a Cisco VoIP network, it is important to analyze its components and features. Figure 2 schematically depicts a typical VoIP network. At a very high level, a Cisco H.323 VoIP network consists of gatekeepers that control H.323 zones. Each zone consists of one or more points of presence (POPs), and each POP can contain one or more Cisco AS5300s.

Figure 2 Anatomy of a Packet Telephony Network



T1/E1 Support

When initially released, the Cisco AS5300 with voice feature card (VFC) supported T1 PRI signaling. With the service provider feature set release in Cisco IOS® 11.3(6) NA2, T1 CAS (both immediate and wink start) was added. The Cisco AS5300 also supports E1 PRI and, with the Cisco IOS 11.3(7) release, added support for E1 R2.

Interactive Voice Response Support

Interactive voice response (IVR) support was added as a part of the service provider features in Cisco IOS 11.3(6) NA2. Among the scripts included in that release were “clid_authen,” which can authenticate users either by the Automatic Number Identification (ANI) and the DNIS or by prompting the user to enter a username and password.

These scripts enable a service provider to provide second dial-tone types of services by authenticating the user based on their ANI or unique username and passcode. Since the initial release, Cisco has added additional scripts and is adding support such that Cisco staff can help customers create their own IVR scripts.

CODEC Support

The initial version of the AS5300 voice feature card supported the TI 542 DSPs, and G.711 (u-law and A-law) and G.729 CODECs. In the future, support will be added for G.723.1 (both 5.3 and 6.3 Kbps CODECs), and G.729 Annex B. These CODECs will be available on 542 DSPs and also on the higher density VFCs.

Gatekeeper Platform Support

Gatekeeper functionality is supported on the Cisco 2500, 2600, and 3600 series routers (models 3620 and 3640). For environments with large, scalable requirements, Cisco 3640 routers with the full 128 MB of DRAM are recommended. Cisco IOS gatekeeper software will always carry an “ix” in the image name.

H.323 Case Study

To illustrate the concepts just described, we will look at an actual case study. This service provider wants to add voice on the network and expand its current services. The service provider is a tier-two/tier-three Internet Service Provider (ISP) with a base that includes business and residential subscribers within the U.S. The service provider currently has 20 dial POPs.

The new packet telephony network will support second dial tone for voice calls only (no fax), and will interface to the PSTN via T1 Primary Rate Interfaces (PRIs). Four POPs will be initially deployed in New York, Chicago, Los Angeles, and Miami with the remainder deployed within one year. The packet telephony network must be designed to facilitate this rapid expansion.

Based on the current traffic projections, the service provider wants to initially offer 96 voice ports in each of the POPs today. Cisco 7206 routers will be used for backhauling calls. Because Cisco AS5300s currently support 48 ports each, two AS5300s will be required per POP. Subscribers will dial the ISP's local access number. An IVR script on the gateway will prompt the user to authenticate based upon account number and password. The ISP is familiar with, and prefers to use, RADIUS, an accounting feature employed in VoIP gateways for producing accurate, timely billing and usage information.

Network Dimensioning—How Assumptions Affect Design

The assumptions made above will have some impact on the network design, as seen in Table 1 below. Some major issues a designer must consider when designing a VoIP Network are the number of gateway ports, gatekeeper availability, and the amount of wide-area bandwidth required to support a given call load. The designer must also be aware of how various design variables impact these requirements. For example, silence suppression only affects the wide-area bandwidth, but does not affect gatekeeper or gateway sizing. Similarly, CODEC choice, e.g. G.711 or G.729, impacts only wide-area bandwidth. Other factors such as average holding time, the time a customer is on a call, can affect both wide-area bandwidth and the ports required on a gatekeeper and gateway. Tools such as header compression can alleviate some wide-area bandwidth requirements, but this is not supported or recommended for large ISP environments.

Table 1 How Assumptions Affect Design

	Areas of Impact	
	WAN Bandwidth	GW Ports/GK
Silence Suppression: Can't Be Applied to Applications (Such As Fax) Percent Reduction in Per-Call Bandwidth will Vary by Application.	X	
CODEC Type: Bandwidth Per Call Varies by CODEC Type (for example G.711 Bandwidth Is Greater than G.729)	X	
Average Hold Time: Varies by Application, User Type, and Even Market (for example Fax Has Shorter Average Holding Time than Voice)	X	X
Header Compression: Reduces Bandwidth Per Call for Lower-Speed Links	X	

Sizing the POPs

The ISP has made some assumptions regarding the sizing of the four POPs. Voice ports will be utilized 100 percent during busy hour (36 Centum Call Seconds [CCS]). Statistically, silence is present 50 percent of the time on a voice call. With the default configuration using the G.729 CODEC, a Cisco AS5300 gateway will generate a 20-byte voice sample every 20 ms or 50 pps. Adding the 12-byte RTP header, eight-byte Unreliable Datagram Protocol (UDP) header, and 20-byte IP header to the packet, the IP datagram will total 60 bytes. With 6 bytes of link-layer overhead, this generates a 66-byte packet every 20 msec (without voice activity detection [VAD]). With VAD enabled, this translates to:

$$66 \text{ bytes/packet} * 8 \text{ bits/byte} * 1/2 * 50 \text{ pps} = 13.2 \text{ kbps per call or DSO}$$

Assuming that VAD will reduce bandwidth utilization by approximately half, supporting 96 calls from each POP will require 1.27 Mbps which is less than one T1 for backhaul.

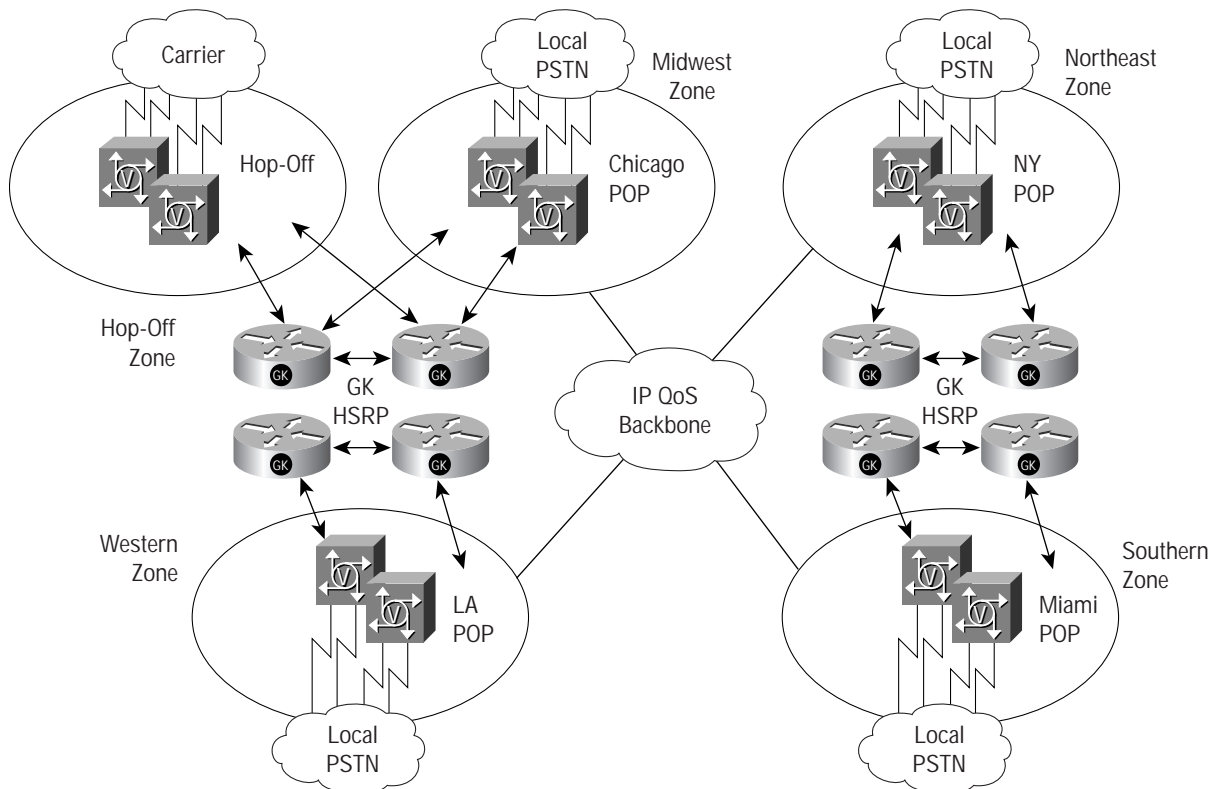
Network Design

Assuming the above requirements and considerations, the network is illustrated in Figure 3. The nationwide network will be divided geographically into four zones (a Chicago Midwestern zone, a New York Northeastern zone, a Miami Southern zone, and a Los Angeles Western zone) to anticipate future growth. All of these nodes are connected via an existing quality-of-service (QoS)-enabled IP backbone.

Each zone will have redundant Hot-Standby Router Protocol (HSRP)-enabled Cisco 3640 gatekeepers to ensure that another redundant gatekeeper takes over, should the active gatekeeper fail. Since a gatekeeper can handle approximately 1000 active calls, 20 AS5300s (or 10 POPs) can be serviced with the current 48-port capacity of the AS5300s.

For the purposes of this example, we will assume that the PSTN circuits are in the same rate center. A rate center is a calling area consisting of several central offices usually concentrated in a geographic area. Usually a LEC will charge for intra-LATA calls crossing these rate centers. Assuming that each POP will not service calls outside it's rate center and because the network is being deployed with just four cities the network will not service the entire U.S. market. Therefore, PSTN calls to areas not covered will need to be handed off to another service provider for termination. This is referred to as off-net traffic. In this example, calls to off-net cities will hop off at the Chicago POP to a wholesale long distance carrier that offers a flat-rate charge on a per-minute basis.

Figure 3 The Packet Telephony Network Initially Consists of Four POPs

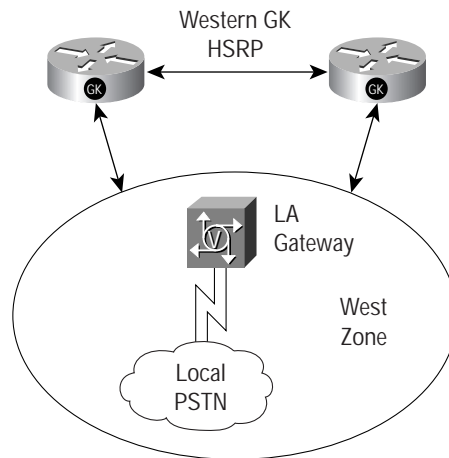


Consider a simplified example, shown in Figure 4, illustrating our dial plan based on number planning areas (NPAs) or area codes only. A real-life network would require a more detailed dial plan containing NPA-NXX (area codes and local prefixes). Furthermore, there are many NPAs in Chicago and Los Angeles. However, this example addresses the following sample configuration:

- Los Angeles NPAs: 213, 310, 323
- Chicago NPAs: 224, 312, 630

Finally, we assume the gatekeepers will use direct end-point signaling to reach other zones in this network and proxy mode to protect this network from access by external zones. Although a Cisco AS5300 has two Ethernet interfaces, the H.323 process should not be bound to one or the other. Rather, a more reliable network is created if it is bound to a loopback (logical) interface.

Figure 4 A Simplified Three-Zone Network



Let's start by looking at a fundamental block of the network. Let's focus on the western zone which contains the western-GK and a GW to look at the configurations.

Gateway Configuration—Los Angeles

Table 2 shows the configuration for the LA gateway.

Table 2 LA Gateway Configuration

Command	Description
<pre> Hostname la1-gw.west.acme.com </pre>	The host name of this gateway is la1-gw.west.acme.com. This is the first gateway in the western zone in the Acme Corporation.
<pre> aaa new-model aaa authentication login default radius aaa accounting connection h323 start-stop radius ! gw-accounting h323 ! radius-server host 10.1.11.11 auth-port 1645 acct-port 1646 radius-server key testing123 ! </pre>	<p>To allow for the billing and collection of the user name and password, "aaa new model" is enabled. For VoIP authentication and accounting Cisco gateways use RADIUS.</p> <p>The gateway will send both the start and the stop records to the RADIUS server.</p> <p>The "gw-accounting h323" command instructs the gateway to perform accounting for the H.323 calls.</p> <p>And the following commands define the properties for the RADIUS server (these commands will appear at the end of the configuration).</p>
<pre> isdn switch-type primary-5ess ! </pre>	This gateway will use an ISDN PRI connection to the network, and a global switch-type command has been enabled. Specific properties have also been enabled on each of the controllers.
<pre> Controller T1 0 Framing esf Clock source line primary Linecode b8zs pri-group timeslots 1-24 ! </pre>	Extended Super Frame (ESF) is used for framing and Binary 8 Zero Suppression (B8ZS) for line code. Clock will be taken from the T1 interface connected to the PSTN. ISDN PRI interface is defined, with 1 to 24 timeslots.
<pre> dial-peer voice 2 voip destination-pattern 2..... session target ras precedence 5 ! </pre>	The dial-peer commands define the dial plan for the gateway. These commands instruct the gateway to check with the gatekeeper, use a TDM interface for the call, or signal to the terminating gateway directly. In this example, "dial-peer voice 2" is a VoIP-type of dial-peer and the destination pattern is a "2" followed by 9 dots. This maps to any destination 10-digit phone number that begins with a "2." Once the DNIS has been identified, we need to examine what to do with the call. In this example, we refer to the gatekeeper for address resolution, and when the call is set up the RTP packets will be marked with a precedence of 5. Other routers that the VoIP packets will traverse can use the precedence to prioritize the VoIP packets over other traffic traversing the network, providing good-quality voice.
<pre> Repeat till 9..... ! </pre>	The same command will need to be repeated for numbers that begin with "3, 4, 5, 6, 7, 8," and "9" plus nine dots to address all possible numbers.
<pre> dial-peer voice 213 pots destination-pattern 213..... application clid_authen_collect port 0:D ! Repeat for other NPAs served ! </pre>	<p>Previously we defined the dial-peers for calls going to the packet network. Now we will define the dial-peers for TDM basic telephone service. In addition to routing the calls to the packet network, we also need to tell the gateway what the phone numbers on the TDM/plain old telephone service (POTS) interfaces are. This is referred to as a POTS dial-peer. For calls coming in from the VoIP side, a called number that begins with 213 will be sent out on port 0:D. The same command must be repeated for the other NPA and NXX peers served within the cities and also for the other controller, such as controller 1 or port 1:D.</p> <p>For an incoming call from the TDM port 0:D, this command will launch the clid_authen_collect script, which will authenticate based on ANI and DNIS and, if that fails, prompt the user for USERNAME and PASSWORD for authentication.</p>
<pre> gateway ! </pre>	The gateway command is enabled, which is the global command to enable the RAS (Registration, Admission and Status) functionality on a gateway. RAS allows the gateway to communicate with the gatekeeper.
<pre> Interface Loopback0 ip address 10.10.250.1255.255.255.0 h323-gateway voip interface h323-gateway voip id gk.west.acme.com ipaddr 10.10.254.10 1719 h323-gateway voip h323-id la1-gw.west.acme.com h323-gateway voip tech-prefix 1# ! </pre>	<p>The next section concerns the interface loopback 0. As discussed earlier, the Loopback interface helps build a more redundant and reliable network.</p> <p>Next we specify that this interface will be used for H.323-based communications. The following command defines the gatekeeper's properties, such as the name and the IP address where it is available. The next command indicates that the local gateway has the H.323-ID of gw.west.acme.com. The last command will register a technology prefix of 1# to identify the capabilities of this gateway.</p>
<pre> Interface Ethernet0 ip address 10.10.254.5 255.255.255.0 ! </pre>	The interface Ethernet 0 is then defined. Typically, both Ethernet 0 and Fast Ethernet 0 will be enabled.
<pre> Interface Serial0:23 isdn switch-type primary-5ess isdn incoming-voice modem ! </pre>	The serial interface 0:23 in the next section refers to the D Channel of the 0th PRI interface and its properties. A 5E custom switch is specified, and incoming voice calls are directed to the DSPs/modem.
<pre> La1-gw.west.acme.com#show gateway Gateway la1-gw.west.acme.com is registered to Gatekeeper gk.west.acme.com </pre>	Once the configuration is complete, the user will need to make sure that the commands are accurate. By typing "show gateway" the system administrator can determine whether the gateway was able to register with the gatekeeper. This confirms that the gatekeeper and the gateway were configured correctly and that there are no connectivity problems.

Gatekeeper Configuration—Los Angeles

Table 3 shows the gatekeeper configuration for the Western zone. These commands are for a GK running IOS 12.0(3)T or earlier.

Table 3 Western GK Configuration

Command	Description
<pre> Hostname gk1.west.acme.com !</pre>	The host name is gk1.west.acme.com, because this is the first gatekeeper in the Western zone in this network.
<pre> interface Ethernet0/0 ip address 10.10.254.4 255.255.255.0 standby 1 priority 110 <-- Primary standby 1 ip 10.10.254.10</pre>	Under the Ethernet interface definition is the IP address. The HSRP commands are enabled and this is the first HSRP group. This gatekeeper has been given a priority of 110, which will force it to assume the primary role over the other gatekeeper. An IP address is specified that all gateways and other gatekeepers will refer to, ensuring a seamless failover between gatekeepers.
<pre> Gatekeeper zone local gk.west.acme.com acme.com 10.10.254.10 zone remote gk.hopoff.acme.com acme.com 10.10.253.10 1719 zone remote gk.mwest.acme.com acme.com 10.10.253.10 1719 zone access gk.west.acme.com remote-zone gk.mwest.acme.com direct zone access gk.west.acme.com remote-zone gk.hopoff.acme.com direct zone access gk.west.acme.com remote-zone gk.west.acme.com direct zone access gk.west.acme.com remote-zone gk.neast.acme.com direct zone access gk.west.acme.com remote-zone gk.south.acme.com direct</pre>	Next comes the gatekeeper commands. The local gatekeeper properties for gatekeeper.west.acme.com are defined, and the IP address where the service will be running is specified. Then the remote zones within this network are defined. The hop-off gatekeeper has an IP address of 10.10.253.10, and the IP address of 1719. Similarly, the other Midwestern gatekeeper zone is defined. The zone access is then defined, which describes how this zone can be accessed from other gateways and gatekeepers in this network. The Western zone can be approached by the Midwestern gatekeeper and the corresponding gateways in a direct signaling mode. The same properties are applied for the other gateways and other gatekeepers within the network.
<pre> zone access gk.west.acme.com default proxied</pre>	The next command, "zone access gk.west.acme.com default proxied," forces the remaining gatekeepers to use a proxied mode. This protects the gatekeeper or the gateways from other gatekeepers that are not authorized to approach this site.
<pre> zone subnet gk.west.acme.com 10.10.250.0/24 enable</pre>	The "zone subnet" command defines who can register with this gatekeeper, providing a security mechanism that restricts only the gateways within the 10.10.250.0 subnet to register with this gatekeeper.
<pre> zone prefix gk.west.acme.com 213* zone prefix gk.west.acme.com 310* zone prefix gk.west.acme.com 323* zone prefix gk.mwest.acme.com 630* zone prefix gk.mwest.acme.com 312* zone prefix gk.hopoff.acme.com *</pre>	"Zone prefix" is a routing command, and the next six commands define how routing is set up in this network. Area code 213, or the NPA 213, resides in the Western zone, as do 310 and 323. NPA 630 resides in the Midwestern zone, as well as 224 and 312. The last prefix command specifies that any other NPA that does not match the first six commands resides in the hop-off gatekeeper. Depending on the requirements of a specific network, all gatekeepers may have identical zone prefix commands. If routing is based on NPA and NXX, however, the local gatekeeper will have more granularity and other gatekeepers can point to the local gatekeeper for the entire NPA.
<pre> gw-type-prefix 1#* default-technology</pre>	The next command, "gw-type-prefix 1#* default-technology," specifies the default technology. This simplifies the design, since all gateways will use the same tech prefix and there is no reason to put the tech prefix command in the dial-peer statements.
<pre> no shutdown</pre>	The last command, "no shutdown," enables the gatekeeper service on this particular platform.

Show Commands—Los Angeles

Once these commands are entered, the show commands, below, indicate how they have taken effect and how the gatekeeper is functioning. The first command, “show gatekeeper endpoints,” identifies which gateways have already registered with this gatekeeper. In this example, la1.gw.west.acme.com has registered with this gatekeeper in the zone gk.west.acme.com.

The following command, “show gatekeeper zone prefix,” describes the routing table for this given gatekeeper. Confirming the configuration, 213 resides within the Western gatekeeper; 224 resides within the Midwestern gatekeeper, and so on.

The last line in the output, “gk.hopoff.acme.com,” confirms that the remainder of the NPA NXXs or any phone numbers would be sent to the gatekeeper in the hop-off zone.

Show commands include:

```
gk1.west.acme.com#show gatekeeper endpoints
GATEKEEPER ENDPOINT REGISTRATION
=====
CallSignalAddr  Port  RASignalAddr  Port  Zone Name          Type    F
-----
10.10.250.1     1720  10.10.250.1   4461  gk.west.acme.com  VOIP-GW
      H323-ID: la1-gw.west.acme.com
gk1.mwest.acme.com#show gatekeeper zone prefix
      ZONE PREFIX TABLE
      =====
GK-NAME          E164-PREFIX
-----
gk.west.acme.com  213*
gk.mwest.acme.com 224*
gk.west.acme.com  310*
gk.mwest.acme.com 312*
gk.west.acme.com  323*
gk.mwest.acme.com 630*

gk.hopoff.acme.com *
```

Gateway Configuration—Chicago

Next, the Chicago gateway is configured as shown in Table 4. It is very similar to the Los Angeles gateway.

Table 4 GW-Chicago

Command	Description
hostname ch1-gw.mwest.acme.com !	The host name for this gateway is ch1-gw.midwest.acme.com, the first gateway within the Midwestern zone in Chicago.
aaa new-model aaa authentication login default radius aaa accounting connection h323 start-stop radius ! gw-accounting h323 radius-server host 10.1.11.11 auth-port 1645 acct-port 1646 radius-server key testing123	To allow for the billing and collection of the user name and password, "aaa new model" is enabled. For VoIP authentication and accounting Cisco gateways use RADIUS. The gateway will send both the start and the stop records to the RADIUS server. The "gw-accounting h323" command instructs the gateway to perform accounting for the H.323 calls. And the following commands define the properties for the RADIUS server (these commands will appear at the end of the configuration).
isdn switch-type primary-5ess !	This gateway will use an ISDN PRI connection to the network, and a global switch-type command has been enabled. Specific properties have also been enabled on each of the controllers.
controller T1 0 framing esf clock source line primary linecode b8zs pri-group timeslots 1-24 !	The "controller T1 0" command enables the controller T1 0 and the framing and line code properties.
dial-peer voice 2 voip destination-pattern 2..... session target ras precedence 5 !	The dial-peer commands define the dial plan for the gateway. These commands instruct the gateway to check with the gatekeeper, or use a TDM interface for the call, or signal to the terminating gateway directly. In this example, "dial-peer voice 2" is a VoIP-type of dial-peer and the destination pattern is a "2" followed by 9 dots. This maps to any destination 10 digit phone number that begins with a "2." Once the DNIS has been identified, you must examine what to do with the call. In this example, the gatekeeper is referred to for address resolution, and when the call is set up, the RTP packets will be marked with a precedence of 5. Other routers that the VoIP packets will traverse can use the precedence to prioritize the VoIP packets over other traffic traversing the network, leading to good quality voice.
<i>Repeat till 9.....</i> !	Some of the other commands have been deleted due to space constraints. In a real network, the same command will need to be repeated with "3, 4, 5, 6, 7, 8," and "9" plus nine dots to address all possible numbers with the E.164 dial plan.
dial-peer voice 312 pots application cli_d_authen_collect destination-pattern 312..... port 0:D ! <i>Repeat for other NPAs served</i>	Previously we defined the dial-peers for calls going to the packet network. Now we will define the dial-peers for the TDM or basic telephone service. "Dial-peer" is the basic telephone service dial-peer that picks up. In addition to the VoIP matching to the gateway, we also need to tell the gateway the phone numbers on the TDM/POTS interfaces. This is referred to as a basic telephone service dial-peer. For an incoming call from the TDM port 0:D, this command will launch the cli_d_authen_collect script, which will authenticate based on ANI and DNIS and, if that fails, prompt the user for USERNAME and PASSWORD for authentication. For calls coming in from the VoIP side, a called number that begins with 213 will be sent out on port 0:D. The same command must be repeated for the other NPA and NXX peers served within the cities and also for the other controller.
gateway !	The gateway command is enabled, which is the global command to enable the RAS functionality on a gateway. RAS allows the gateway to communicate with the gatekeeper.
interface Loopback0 ip address 10.10.249.1 255.255.255.0 h323-gateway voip interface h323-gateway voip id gk.mwest.acme.com ipaddr 10.10.253.10 1719 h323-gateway voip h323-id ch1-gw.mwest.acme.com h323-gateway voip tech-prefix 1# !	The next section concerns the interface loopback 0. As discussed earlier, the loopback interface helps build a more redundant and reliable network. Next we specify that this interface will be used for H.323-based communications. The following command defines the gatekeeper's properties, such as the name and the IP address where it is available. The next command indicates that the local gateway has the H.323-ID of gw.mwest.acme.com. The last command will register a technology prefix of 1# to identify the capabilities of this gateway.
interface Ethernet0 ip address 10.10.253.5 255.255.255.0 no ip directed-broadcast ntp broadcast client !	The interface Ethernet 0 is then defined. Typically, both Ethernet 0 and Fast Ethernet 0 will be turned on.
interface Serial0:23 isdn switch-type primary-5ess isdn tei-negotiation first-call isdn incoming-voice modem !	The serial interface 0:23 in the next section refers to the D Channel of the 0th PRI interface and its properties. A 5E custom switch is specified, and incoming voice calls are directed to the DSPs/modem.
ch1-gw.mwest.acme.com#sh gateway Gateway ch1-gw.mwest.acme.com is Registered to Gatekeeper gk.mwest.acme.com	Once the configuration is complete, the user will need to make sure that the commands are accurate. By typing "show gateway" the system administrator can determine whether the gateway was able to register with the gatekeeper. This confirms that the gatekeeper and the gateway were configured correctly and that there are no connectivity problems.

Gatekeeper Configuration—Chicago

Because the same Cisco 3640 routers are used for both the hop-off zone and Midwestern zone (a Cisco gatekeeper can support more than one local zone), the Chicago gatekeeper configuration differs from the Los Angeles configuration (Table 5).

Table 5 Midwest-GK Configuration

Command	Description
hostname gk1.mwest.acme.com !	The host name is gk1.mwest.acme.com because this is the first gatekeeper in the Midwestern zone in this network.
interface Ethernet0/0 ip address 10.10.253.4 255.255.255.0 standby 1 priority 110 <--- Primary GateKeeper standby 1 ip 10.10.253.10 !	Under the Ethernet interface definition is the IP address. The HSRP commands are turned on and this is the first HSRP group. This gatekeeper has been given a priority of 110, which will force it to assume the primary role over the other gatekeeper. An IP address is specified that all gateways and other gatekeepers will refer to, ensuring a seamless failover between gatekeepers.
Gatekeeper zone local gk.mwest.acme.com acme.com 10.10.253.10 zone local gk.hopoff.acme.com acme.com zone remote gk.west.acme.com acme.com 10.10.254.10 1719	Next comes the gatekeeper commands. The local gatekeeper properties for gatekeeper.mwest.acme.com are defined, and the IP address where the service will be running is specified. Then the remote zones within this network are defined. The hop-off gatekeeper has an IP address of 10.10.253.10, and the IP address of 1719. Similarly, the other West gatekeeper zone is defined.
zone access gk.mwest.acme.com remote-zone gk.hopoff.acme.com direct zone access gk.mwest.acme.com remote-zone gk.neast.acme.com direct zone access gk.mwest.acme.com remote-zone gk.south.acme.com direct zone access gk.mwest.acme.com remote-zone gk.west.acme.com direct	The zone access is then defined, which describes how this zone can be accessed from other gateways and gatekeepers in this network. The Midwestern zone can be approached by the Western gatekeeper and the corresponding gateways in a direct signaling mode. The same properties are applied for the other gateways and other gatekeepers within the network.
zone access gk.mwest.acme.com default proxied	The next command, "zone access gk.mwest.acme.com default proxied," forces the remaining gatekeepers, beyond the first five defined, to use a proxied mode. This protects the gatekeeper or the gateways from other gatekeepers that are not authorized to approach this site.
zone access gk.hopoff.acme.com remote-zone gk.neast.acme.com direct zone access gk.hopoff.acme.com remote-zone gk.south.acme.com direct zone access gk.hopoff.acme.com remote-zone gk.west.acme.com direct zone access gk.hopoff.acme.com remote-zone gk.mwest.acme.com direct	Similar to the previous definitions, these commands define the access rights for the hop-off zone. Since there are five zones all together, the user needs to define the rights between all of the zones.
zone access gk.hopoff.acme.com default proxied	For this particular gatekeeper, because there are two local zones, the commands must be repeated for both the Midwestern and the hop-off zones.
zone prefix gk.mwest.acme.com 224* zone prefix gk.mwest.acme.com 312* zone prefix gk.mwest.acme.com 630* zone prefix gk.west.acme.com 213* zone prefix gk.west.acme.com 310* zone prefix gk.west.acme.com 323* zone prefix gk.hopoff.acme.com *	"Zone prefix" is a routing command, and the next six commands define how routing is set up in this network. Area code 224, or the NPA 224, resides in the Midwestern zone, as do 312 and 630. NPA 213 resides in the Western zone, as well as 310 and 323. The last prefix command specifies that any other NPA that does not match the first six commands resides in the hop-off gatekeeper. Depending on the requirements of a specific network, all gatekeepers may have identical zone prefix commands. If routing is based on NPA and NXX, however, the local gatekeeper will have more granularity and other gatekeepers can point to the local gatekeeper for the entire NPA.
gw-type-prefix 1#* default-technology	The next command, "gw-type-prefix 1#* default-technology," specifies the default technology. The tech prefix is 1#. This simplifies the design, since all gateways will use the same tech prefix and there is no reason to put the tech prefix command in the dial-peer statements.
no shutdown	The last command, "no shutdown," enables the gatekeeper service on this particular platform.

Show Commands—Chicago

Show commands for the Chicago gatekeeper are illustrated below. Two zones are defined: gk.hopoff.acme.com and gk.midwest.acme.com. Two gateways have already registered with this gatekeeper. The first one is the first gateway in the hop-off zone and the other one is the first Chicago gateway. The zone gatekeeper routing table is very similar to the Los Angeles gatekeeper because we are using NPA-based routing only.

Show commands:

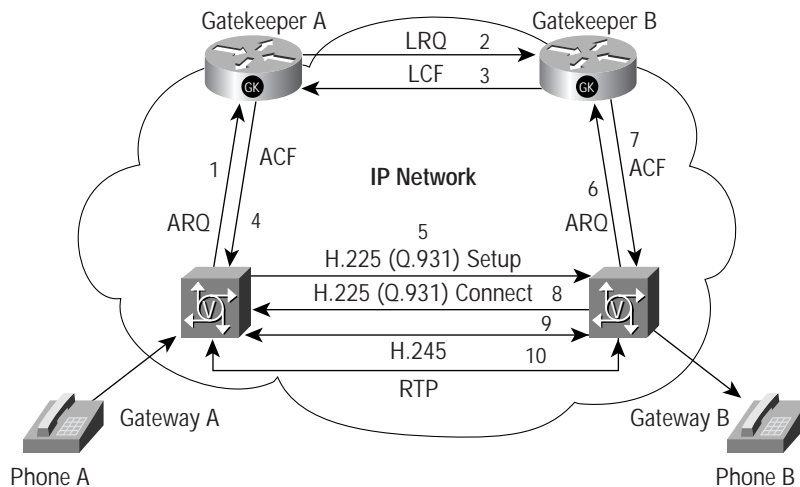
```
gk1.mwest.acme.com#show gatekeeper endpoints
GATEKEEPER ENDPOINT REGISTRATION
=====
CallSignalAddr Port  RASignalAddr  Port  Zone Name          Type  F
-----
10.10.248.1     1720  10.10.248.1   3361  gk.hopoff.acme.co VOIP-GW
      H323-ID: gw1.hopoff.acme.com
10.10.249.1     1720  10.10.249.1   6883  gk.mwest.acme.com VOIP-GW
      H323-ID: chl-gw.mwest.acme.com
```

```
gk1.mwest.acme.com#show gatekeeper zone prefix
ZONE PREFIX TABLE
=====
GK-NAME          E164-PREFIX
-----
gk.west.acme.com 213*
gk.mwest.acme.com 224*
gk.west.acme.com 310*
gk.mwest.acme.com 312*
gk.west.acme.com 323*
gk.mwest.acme.com 630*
gk.hopoff.acme.com *
```

Call Flow

Once the network is configured, calls follow the flow illustrated in Figure 5. A call travels from Phone A to Phone B. Upon receipt of the setup message from phone A, Gateway A consults with Gatekeeper A through an ARQ (1) message. Since Gatekeeper A knows Gatekeeper B services Phone B, Gatekeeper A forwards that message via LRQ (2) to Gatekeeper B. Gatekeeper B then consults its routing table and returns an LCF (3) back to Gatekeeper A. Then Gatekeeper A responds back to Gateway A with an ACF (4).

Figure 5 RAS Message Exchange

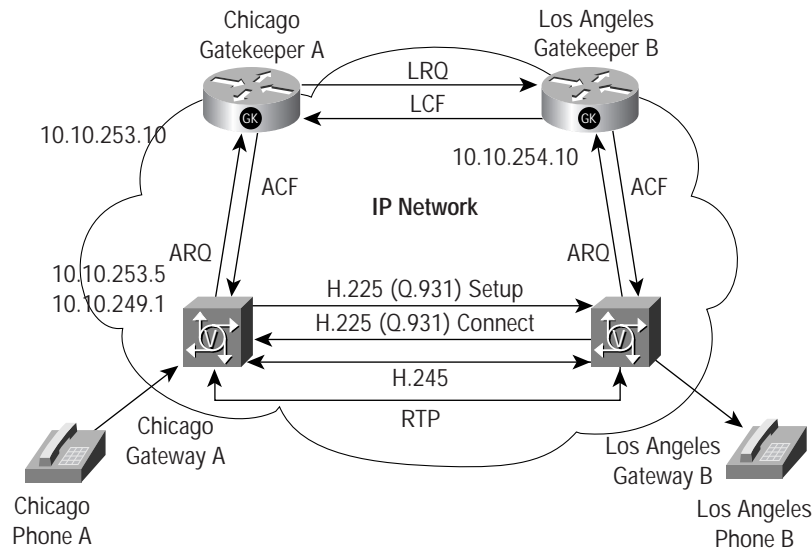


On admission is confirmed, Gateway A sends a H.225 (5) setup message to Gateway B which then sends out an ARQ (6) to Gatekeeper B to request permission to answer the call. The gatekeeper confirms that it can terminate the call and replies with an ACF (7) message. This ACF message, allows Gateway B to acknowledge the setup message with an H.225 connect (8). At that point, H.245 exchange occurs (9), which opens up the logical channels, and the call proceeds (10).

Debug Commands

Gateways and gatekeepers have debug commands that can be used as troubleshooting tools. Ideally, the network should come up, but engineers prefer to test the network to ensure that it works as planned. The output generated by the debug commands enable them to do this. Figure 6 demonstrates a call going from the Chicago gateway to the LA gateway. The diagram also contains the IP addresses to make the debugs clearer.

Figure 6 RAS Messages with IP Addresses



Originating Gateway Debugs

In Figure 6, “debug RAS” has been enabled, as the call travels from Chicago to Los Angeles. Upon receipt of the message from the PSTN, the Chicago gateway sends out an ARQ to its gatekeeper in the Midwestern zone. The Midwestern zone then consults the Los Angeles gatekeeper and returns an ACF. Upon receipt of the ACF, the originating gateway in Chicago contacts the terminating gateway in Los Angeles and the call is initiated.

```
chl-gw.mwest.acme.com# debug ras
chl-gw.mwest.acme.com#
RASLibRASSendARQ ARQ (seq# 3365) sent to 10.10.253.10

RASLibRASRecvData ACF (seq# 3365) rcvd from 10.10.253.10
```

The Call is in progress ... and once the caller or the callee hang up the call will be disconnected with the DRQ and the DCF messages.

```
RASlibras_sendto msg length 55 from 10.10.253.56 to 10.10.253.10
RASLibRASSendDRQ DRQ (seq# 3366) sent to 10.10.253.10
RASLibRASRecvData successfully rcvd message of length 3 from 10.10.253.101719
RASLibRASRecvData DCF (seq# 3366) rcvd from 10.10.253.10
```

Originating Gatekeeper Debugs

Next we will look at the gatekeeper in Chicago. Events are triggered when the gatekeeper receives an ARQ from the originating gateway and proceeds to the gatekeeper, sending an LRQ to the terminating gatekeeper, and then responding with an ACF to the originating gateway.

```
gk1.mwest.acme.com# debug ras
gk1.mwest.acme.com#
RASLibRASRecvData ARQ (seq# 3365) rcvd from [10.10.253.56883] on sock [0x60AF038C]
RASLibRAS_WK_TInit ipsock [0x60A7A68C] setup successful
RASlibras_sendto msg length 61 from 10.10.253.107624 to 10.10.254.101719
RASLibRASSendLRQ LRQ (seq# 5) sent to 10.10.254.10
RASLibRASRecvData successfully rcvd message of length 160 from 10.10.254.101719
RASLibRASRecvData LCF (seq# 5) rcvd from [10.10.254.101719] on sock [0x60A7A68C]
  RASLibparse_lcf_nonstd
LCF Nonstd decode succeeded, remlen = 0
RASlibras_sendto msg length 16 from 10.10.253.101719 to 10.10.249.16883
RASLibRASSendACF ACF (seq# 3365) sent to 10.10.249.1
```

The call is in progress

```
RASLibRASRecvData successfully rcvd message of length 55 from 10.10.253.56883
RASLibRASRecvData DRQ (seq# 3366) rcvd from [10.10.253.56883] on sock [0x60AF038C]
RASlibras_sendto msg length 3 from 10.10.253.101719 to 10.10.249.16883
RASLibRASSendDCF DCF (seq# 3366) sent to 10.10.249.1
RASLibRASRecvData successfully rcvd message of length 124 from 10.10.253.56883
```

Terminating Gatekeeper Debugs

Next, we look at the same call from the terminating gatekeeper's point of view. This call started in the gateway in Chicago, which approached the gatekeeper in Chicago. The gatekeeper in Chicago referenced its routing table and consulted the gatekeeper in Los Angeles.

An LRQ message was received by the gatekeeper in Los Angeles. The Los Angeles gatekeeper references its routing table and returns an LCF message with an IP address off the gateway in the Western zone. This information, via the originating gatekeeper in Chicago, progresses to the originating gateway. The originating gateway then sends a setup message to the gateway in LA to terminate the call.

Upon receipt of the setup message, the Los Angeles gateway consults its gatekeeper (the terminating gatekeeper) with an ARQ message. The gatekeeper responds to the ARQ message with an ACF allowing it to accept the call. After the call is in progress, DRQ and the DCF messages tear down the call.

```
gk1.west.acme.com# debug ras
gk1.west.acme.com#
RASLibRASRecvData LRQ (seq# 5) rcvd from [10.10.253.107624] on sock [0x60A014FC]
RASlibras_sendto msg length 160 from 10.10.254.101719 to 10.10.253.107624
RASLibRASSendLCF LCF (seq# 5) sent to 10.10.253.10
RASLibRASRecvData successfully rcvd message of length 72 from 10.10.254.54461
RASLibRASRecvData ARQ (seq# 3426) rcvd from [10.10.254.54461] on sock [0x60A014FC]
RASlibras_sendto msg length 16 from 10.10.254.101719 to 10.10.250.14461
RASLibRASSendACF ACF (seq# 3426) sent to 10.10.250.1
RASLibRASRecvData successfully rcvd message of length 120 from 10.10.254.54461 from 10.10.254.54461
```

The Call is in progress

```
RASLibRASRecvData successfully rcvd message of length 55 from 10.10.254.54461
RASLibRASRecvData DRQ (seq# 3428) rcvd from [10.10.254.54461] on sock [0x60A014FC]
RASlibras_sendto msg length 3 from 10.10.254.101719 to 10.10.250.14461
RASLibRASSendDCF DCF (seq# 3428) sent to 10.10.250.1
```

Terminating Gateway Debugs

The job of the terminating gateway is much simpler than that of the gatekeeper. In this example, an ARQ is sent from the terminating gateway to the terminating gatekeeper. This is triggered by the setup message sent by the originating gateway to this gateway.

The gatekeeper confirms the admission with an admission confirmation or an ACF message and, once the call is in progress, the DRQ and the DCF messages, again, tear down the call properly.

```
lal-gw.west.acme.com# debug ras
RASLibRASSENDARQ ARQ (seq# 3426) sent to 10.10.254.10

RASLibRASRECVData ACF (seq# 3426) rcvd from [10.10.254.10]
```

The call is in progress

```
RASLibRASSENDDRQ DRQ (seq# 3428) sent to 10.10.254.10
RASLibRASRECVData DCF (seq# 3428) rcvd from [10.10.254.101719]
```

Upcoming Scalability Improvement Features

Cisco is planning a number of improvements that will help make VoIP networks even more scalable. Current networks create a full mesh between all of the gatekeepers. Each gatekeeper needs to know about every other gatekeeper in the network, which can be tedious and burdensome as the network grows.

With LRQ forwarding, Cisco is enabling a directory gatekeeper or super-gatekeeper. With a directory gatekeeper, individual gatekeepers do not need to know about other gatekeepers. Instead, a gatekeeper consults its routing table, which provides a default route to a directory gatekeeper. This directory gatekeeper is more knowledgeable about the topology of the network and can forward messages onto the right egress gatekeeper. The egress gatekeeper can then contact the originating gatekeeper to complete the call. This feature is referred to as LRQ forwarding, and is in the Cisco IOS 12.0(3)T gatekeeper images.

Another improvement available in the Cisco IOS 12.0(4)XH timeframe will allow a gatekeeper to individually select a gateway. Today, with an NPA dialing plan, the egress gateway is selected only based upon the entire NPA. As ISPs scale their networks, however, they will terminate their T1s into individual rate centers. To terminate calls into rate centers, a single gatekeeper must be able to identify one gateway that can terminate that call without picking up the intra-LATA toll charges. With new gateway preference commands, a gatekeeper can instruct a specific gateway to handle a call based on rate centers.

Also scheduled for Cisco IOS 12.0(4)XH is the resource availability indicator (RAI) message, which will allow a gateway to inform the gatekeeper that it is short on resources (such as DS0s and DSPs). Once the gatekeeper receives the RAI, it will not assign a call to a gateway that is low on resources. Other important enhancements in Cisco IOS 12.0(4)XH include H.323V.2 support and the transport of DTMF tones over H.245 channels.

Summary

For service providers considering the deployment of VoIP services, H.323 provides a proven, dependable solution today. The Cisco implementation of H.323 offers an easy migration strategy to begin deploying additional revenue-generating services to compete in the New World of telecommunications.



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

European Headquarters

Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
<http://www-europe.cisco.com>
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

**Americas
Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-7660
Fax: 408 527-0883

Asia Headquarters

Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
<http://www.cisco.com>
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco Connection Online Web site at <http://www.cisco.com/offices>.

For more information about services solutions for service providers,

visit <http://www.cisco.com/spservices>

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela