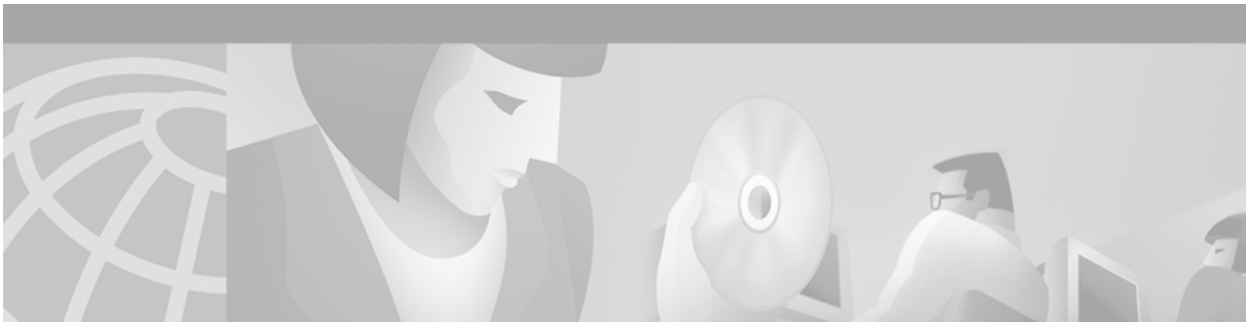


H.323 Applications

This chapter provides an overview of the H.323 standard from the International Telecommunication Union Telecommunication Standardization Sector (ITU-T), of the Cisco H.323-compliant gatekeeper, of the Cisco H.323-compliant gateway, and of the Cisco H.323-compliant features. Cisco IOS software complies with the mandatory requirements and several of the optional features of the H.323 Version 2 specification. The chapter contains the following sections:

Refer to the ITU-T H.323 standard for more in-depth information about the overall H.323 standard.

For a complete description and for examples of configuring Cisco gatekeepers, see the chapter "Configuring H.323 Gatekeepers and Proxies."

For a complete description and for examples of configuring Cisco gateways, see the chapter "Configuring H.323 Gateways."

For more information on configuring Cisco H.323 features, see the "MGCP and Related Protocols," "Configuring SIP," "Voice over IP Overview," and "Dial Plans, Dial Peers, and Digit Manipulation" chapters. For general information regarding the H.323 Standard, refer to the ITU-T H.323 specifications.

For a more complete description of the H.323-compliant gatekeeper and H.323 Version 2 standard support upgrade commands used in this chapter, refer to the *Cisco IOS Voice, Video, and Fax Command Reference*. To locate documentation for other commands that appear in this chapter, use the command reference master index or search online.

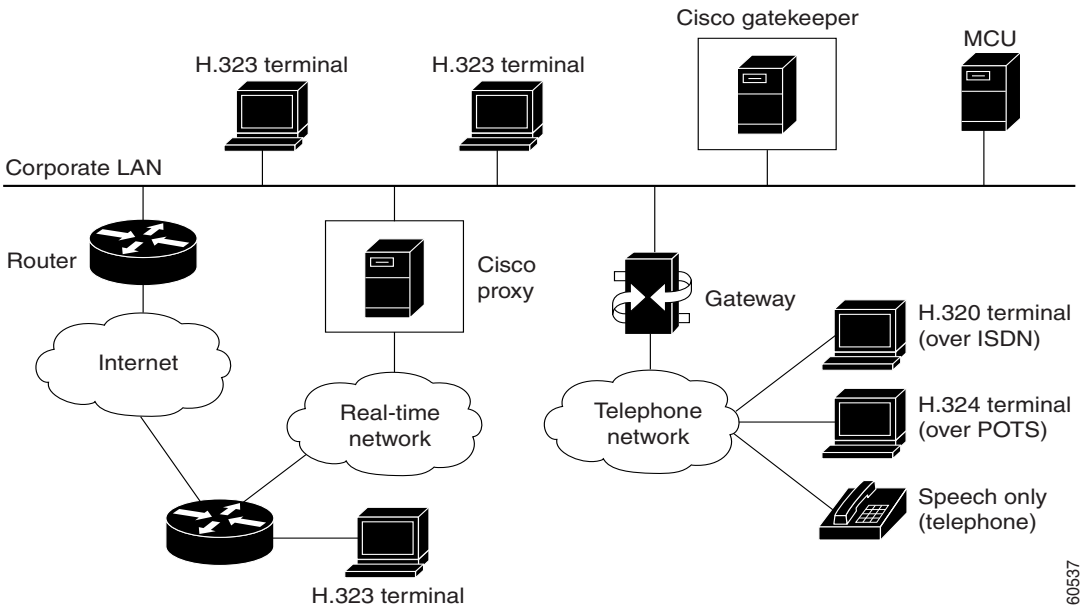
To identify the hardware platform or software image information associated with a feature in this chapter, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Supported Platforms" section in the "Using Cisco IOS Software" chapter.

The H.323 Standard

The H.323 standard provides for sending and receiving audio, video, and data on an IP-based internetwork. The following sections provide a basic overview of network components and how they relate to each other:

Figure 39 shows a typical H.323 network.

Figure 39 Gatekeeper in an H.323 Network



H.323 Terminals

An H.323 terminal is an endpoint in the network that provides for real-time, two-way communications with another H.323 terminal, gateway, or multipoint control unit (MCU). The communications consist of control, indications, audio, moving color video pictures, or data between the two terminals. A terminal may provide audio only; audio and data; audio and video; or audio, data, and video. The terminal can be a computer-based video conferencing system or other device.

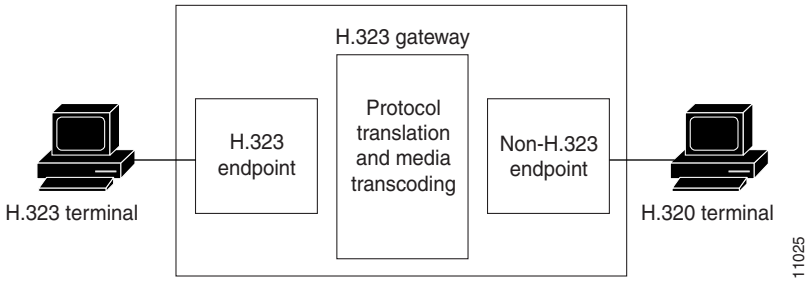
A gatekeeper supports a broad variety of H.323 terminal implementations from many different vendors. These terminals must support the standard H.323 Registration, Admission, and Status (RAS) protocol to function with the gatekeeper.

H.323 Gateways

An H.323 gateway is an endpoint on the LAN that provides real-time communications between H.323 terminals on the LAN and other ITU terminals on a WAN or to other H.323 gateways.

Gateways allow H.323 terminals to communicate with devices that are running other protocols. They provide protocol conversion between the devices that are running different types of protocols. For example, Figure 40 shows a gateway between an H.323 terminal and a non-H.323 terminal.

Figure 40 Gateway Between an H.323 Terminal and an H.320 Terminal



Configuring ISDN Redirect Number Support

Voice over IP (VoIP) supports the redirecting call feature of the VoIP gateway for ISDN calls. The redirecting number is an optional field of the Q.931 setup message.

When a local exchange carrier (LEC) switch detects an incoming call that is destined for a busy or nonanswering party, the switch formulates a Q.931 setup message with the redirecting number field set to the original destination number and sends it to the gateway. The called party number of the setup message will be set to one of the destination number (Dialed Number Identification Service [DNIS]) access numbers of the gateway.

If a redirect number is present on an incoming call, it is used in place of the DNIS. To configure ISDN redirect number support, see the “Dial Plans, Dial Peers, and Digit Manipulation” chapter.

H.323 Proxies

H.323 proxies are special types of gateways that relay H.323 calls to another H.323 endpoint. They can be used to isolate sections of an H.323 network for security purposes, to manage quality of service (QoS), or to perform special application-specific routing tasks.

H.323 Gatekeepers

An H.323 gatekeeper is an H.323 entity on the LAN that provides address translation and that controls access to the LAN for H.323 terminals, gateways, and MCUs.

Gatekeepers are optional nodes that manage endpoints in an H.323 network. The endpoints communicate with the gatekeeper using the RAS protocol.

Endpoints attempt to register with a gatekeeper on startup. When they wish to communicate with another endpoint, they request admission to initiate a call using a symbolic alias for the endpoint, such as an E.164 address or an e-mail address. If the gatekeeper decides that the call can proceed, it returns a destination IP address to the originating endpoint. This IP address may not be the actual address of the destination endpoint, but it may be an intermediate address, such as the address of a proxy or a gatekeeper that routes call signaling.

Note Although the gatekeeper is an optional H.323 component, it must be included in the network if proxies are used.

Gatekeeper Zones

An H.323 endpoint is an H.323 terminal, gateway, or MCU. An endpoint can call and be called.

H.323 endpoints are grouped into zones. Each zone has one gatekeeper that manages all the endpoints in the zone. A zone is an administrative convenience similar to a Domain Name System (DNS) domain. (Because a zone is, by definition, the area of control of a gatekeeper, you will find the terms “zone name” and “gatekeeper name” used synonymously in this chapter.)

Note The maximum number of local zones defined in a gatekeeper should not exceed 100.

MCUs

An MCU is an endpoint on the network that allows three or more endpoints to participate in a multipoint conference. It controls and mixes video, audio, and data from endpoints to create a robust multimedia conference. An MCU may also connect two endpoints in a point-to-point conference, which may later develop into a multipoint conference.

Note Some terminals have limited multipoint control built into them. These terminals may not require an MCU that includes all the functionality mentioned.

How Terminals, Gatekeepers, and Proxies Work Together

When endpoints are brought online, they first attempt to discover their gatekeeper. They discover their gatekeeper either by sending multicast a discovery request or by being configured with the address and, optionally, with the name of the gatekeeper and by sending a unicast discovery request. Following successful discovery, each endpoint registers with the gatekeeper. The gatekeeper keeps track of which endpoints are online and available to receive calls.

There are three ways to set up calls between various endpoints, as described in the following sections:

- Interzone Call with Proxy, page 204
- Interzone Call Without Proxy, page 203
- Interzone Call with Proxy, page 204

Intrazone Call

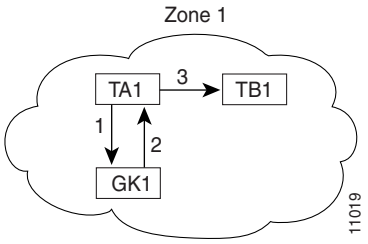
Intrazone calls occur within the same zone.

If terminal TA1 wants to make an intrazone call to terminal TB1 in Zone 1, the following sequence of events occurs:

1. TA1 asks GK1 for permission to call TB1.
2. GK1 returns the address of TB1 to TA1.
3. TA1 then calls TB1.

Figure 41 illustrates these events.

Figure 41 Intrazone Call



Interzone Call Without Proxy

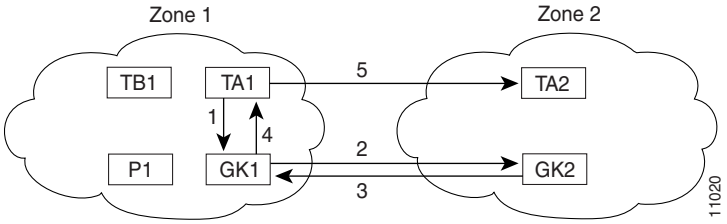
Interzone calls occur between two or more zones.

If terminal TA1 in Zone 1 wants to call terminal TA2 in Zone 2 without the use of a proxy, the following sequence of events occurs:

1. TA1 asks GK1 for permission to call TA2.
2. TA2 is not in the GK1 zone. GK1 locates GK2 as the TA2 gatekeeper. GK1 then asks GK2 for the TA2 address.
3. GK2 returns the TA2 address to GK1.
4. GK1 returns the address to TA1.
5. TA1 calls TA2.

Figure 42 illustrates these events.

Figure 42 Interzone Call Without Proxy



Interzone Call with Proxy

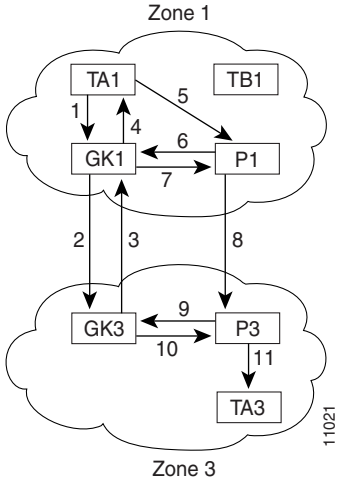
One reason for using a proxy is to isolate addressing information in one zone from another. When such isolation is desired, zones are configured as inaccessible on the gatekeepers. (Other reasons for using proxies are discussed later in this document.)

If terminal TA1 in Zone 1 wants to call terminal TA3 in Zone 3, the following sequence of events occurs:

1. TA1 asks GK1 for permission to call TA3.
2. GK1 locates GK3 as the TA3 gatekeeper. GK1 asks GK3 for the TA3 address.
3. GK3 responds with the P3 address instead of the TA3 address, to hide the TA3 identity.
4. GK1 knows that to get to P3, the call must go through P1. So GK1 returns the P1 address to TA1.
5. TA1 calls P1.
6. P1 consults GK1 to discover the true destination of the call (which is TA3 in this example).
7. GK1 instructs P1 to call P3.
8. P1 calls P3.
9. P3 consults GK3 for the true destination, which is TA3.
10. GK3 gives the TA3 address to P3.
11. P3 completes the call to TA3.

Figure 43 illustrates these events.

Figure 43 Interzone Call with Proxy



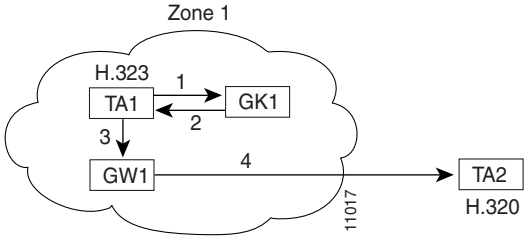
How Terminals, Gatekeepers, and Gateways Work Together

Gateways provide protocol conversion between terminals that run different types of protocols. Gateways communicate with gatekeepers using the RAS protocol. The gatekeeper maintains resource availability information, which it uses to select the appropriate gateway during the admission of a call. In Figure 44, the following conditions exist:

- TA1 is an H.323 terminal that is registered to GK1.
- GW1 is an H.323-to-H.320 gateway that is registered to GK1.
- TA2 is an H.320 terminal.

Figure 44 illustrates these events.

Figure 44 Intrazone Call Through Gateway



A call from TA1 to TA2 is set up as follows:

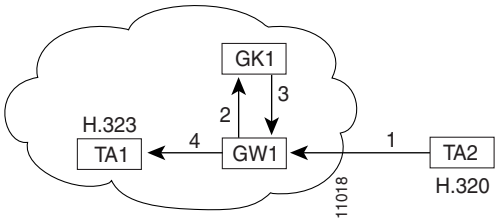
1. TA1 asks GK1 for permission to connect to the TA2 E.164 address.
2. The gatekeeper looks through its local registrations and does not find any H.323 terminals that are registered with that E.164 address, so the gatekeeper assumes that it is an H.320 terminal that is outside the scope of H.323. The gatekeeper instructs TA1 to connect to the GW1 IP address.
3. TA1 connects to GW1.
4. GW1 completes the call to TA2.

A call from TA2 to TA1 is set up as follows:

1. TA2 calls GW1 and provides the TA1 E.164 address as the final destination.
2. GW1 sends a message to GK1 asking to connect to that address.
3. GK1 gives GW1 the address of TA1.
4. GW1 completes the call with TA1.

Figure 45 illustrates these events.

Figure 45 Gateways Provide Translation Between Terminal Types



How Terminals, Gatekeepers, Proxies, and MCUs Work Together

When MCUs are brought online, they first attempt to discover their gatekeeper. As with terminals and proxies, MCUs discover their gatekeeper either by multicasting a discovery request or by being configured with the name and address of the gatekeeper and unicasting a discovery request. Following successful discovery, the MCU registers with the gatekeeper. The gatekeeper keeps track of which endpoints are online and available to receive calls.

There are three ways to set up an MCU conference call, as described in the following sections:

- Intrazone MCU Conference Call, page 207
- Interzone MCU Conference Call Without Proxy, page 207
- Interzone MCU Conference Call with Proxy, page 208

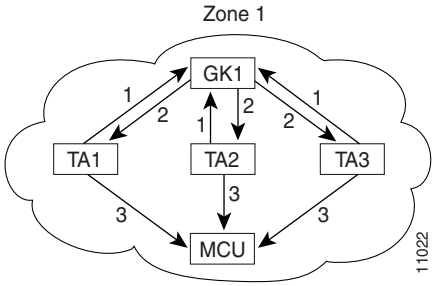
Intrazone MCU Conference Call

An MCU conference in Zone 1 is created with the conference ID CompanyMeeting. The MCU reregisters itself with the gatekeeper, with the new conference ID appended to its list of existing aliases. If terminals TA1, TA2, and TA3 in Zone 1 want to join CompanyMeeting, the following sequence of events occurs:

1. TA1, TA2, and TA3 join the conference by asking GK1 for permission to call the given conference ID.
2. GK1 returns the address of the MCU to TA1, TA2, and TA3.
3. TA1, TA2, and TA3 then call the MCU.

Figure 46 illustrates these events.

Figure 46 Intrazone Call with MCU



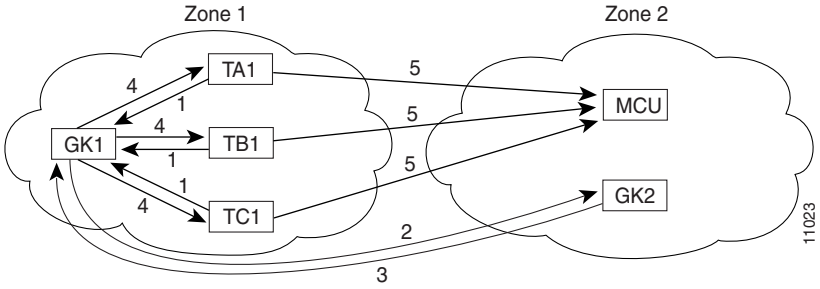
Interzone MCU Conference Call Without Proxy

The MCU in Zone 2 creates a conference with conference ID CompanyMeeting@zone2.com. The MCU reregisters itself with GK2, with the new conference ID appended to its list of existing aliases. Terminals TA1, TB1, and TC1 in Zone 1 want to join the MCU conference call with the conference ID CompanyMeeting@zone2.com in Zone 2. The following sequence of events occurs:

1. TA1, TB1, and TC1 ask GK1 for permission to join the conference.
2. GK1 locates GK2 for the remote zone that contains conference CompanyMeeting@zone2.com using DNS or information configured on GK1. GK1 sends a request to GK2 to recover the MCU address.
3. GK2 gives the MCU address to GK1.
4. GK1 gives the MCU address to TA1, TB1, and TC1, and it instructs these endpoints to set up the call with the MCU.
5. TA1, TB1, and TC1 then call the MCU.

Figure 47 illustrates these events.

Figure 47 Interzone MCU Conference Call Without Proxies



Interzone MCU Conference Call with Proxy

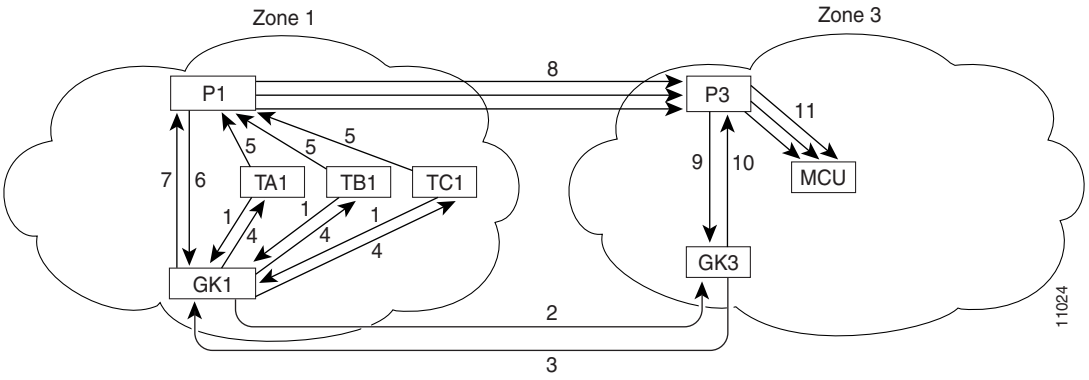
One main reason for using a proxy is to isolate addressing information in one zone from another. When such isolation is desired, zones are configured to be inaccessible on the gatekeepers.

The MCU in Zone 3 creates a conference with the conference ID CompanyMeeting@zone3.com. The MCU reregisters itself with the gatekeeper, using the new conference ID appended to its list of existing aliases. Terminals TA1, TB1, and TC1 in Zone 1 want to join the MCU conference with the conference ID CompanyMeeting@zone3.com in Zone 3. The following sequence of events occurs:

1. TA1, TB1, and TC1 ask GK1 for permission to join the conference CompanyMeeting@zone3.com.
2. GK1 locates GK3 for the remote zone that contains conference CompanyMeeting@zone3.com. GK1 asks GK3 for the MCU address.
3. GK3 responds with the PX3 address instead of the MCU address. GK1 knows that to get to PX3 the call should go through P1.
4. GK1 gives the P1 address to TA1, TB1, and TC1.
5. TA1, TB1, and TC1 call P1.
6. P1 consults GK1 to discover the true call destination, which is CompanyMeeting@zone3.com in this example.
7. GK1 instructs P1 to call P3.
8. P1 calls P3.
9. P3 consults with GK3 to discover the true call destination, which is CompanyMeeting@zone3.com in this example.
10. GK3 gives the MCU address to PX3.
11. P3 completes the call with the MCU.

Figure 48 illustrates these events.

Figure 48 Interzone MCU Conference Call with Proxy



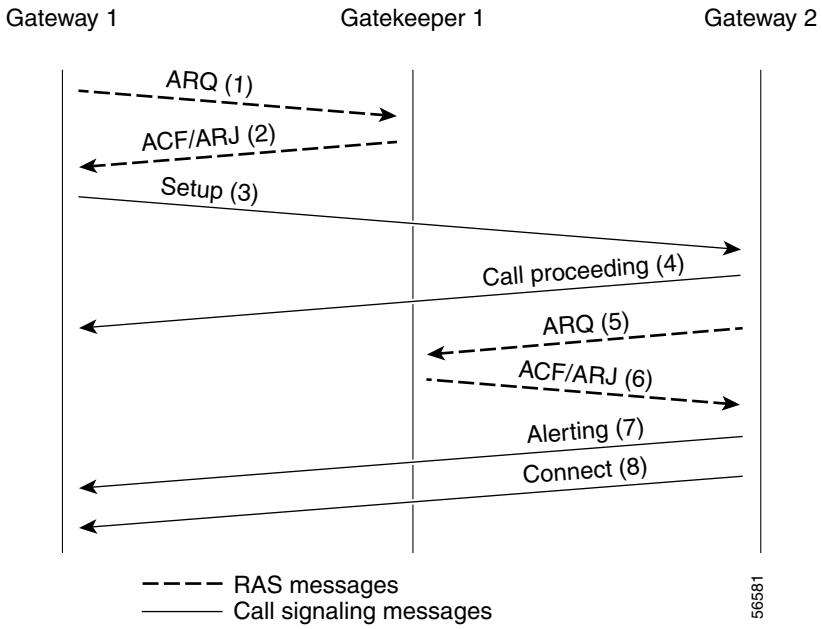
Call Signaling Procedures

Two important phases of H.323 call signaling are call setup and call termination. The following two examples demonstrate the call setup and call termination processes in relation to gatekeepers and gateways.

Call Setup—Both Gateways Registered to the Same Gatekeeper

In Figure 49, both gateways are registered to the same gatekeeper, and the gatekeeper has chosen direct call signaling. Gateway 1 (the calling gateway) initiates the admission request (ARQ) (1)/admission confirmation (ACF) (2) exchange with that gatekeeper. The gatekeeper returns the call signaling channel address of Gateway 2 (the called gateway) in the ACF. Gateway 1 then sends the setup (3) message to Gateway 2 using that transport address. If Gateway 2 wishes to accept the call, it initiates an ARQ (5)/ACF (6) exchange with the gatekeeper. Gateway 2 sends an alerting (7) message to Gateway 1. (If Gateway 2 receives an admission reject [ARJ] (6) message instead of an ACF message, it sends a release complete message to Gateway 1 instead of the alerting message.) Gateway 2 responds with the connect (8) message, which contains an H.245 control channel transport address for use in H.245 signaling.

Figure 49 Both Gateways Registered to the Same Gatekeeper



Call Termination

Either gateway may terminate a call in one of the following ways:

1. It discontinues transmission of video at the end of a complete picture and then closes all logical channels for video.
2. It discontinues transmission of data and then closes all logical channels for data.
3. It discontinues transmission of voice and then closes all logical channels for voice.
4. It transmits the H.245 endSessionCommand message in the H.245 control channel, indicating to the far end that it wishes to disconnect the call and then discontinues H.245 message transmission.
5. It waits to receive the endSessionCommand message from the other gateway and then closes the H.245 control channel.
6. If the call signaling channel is open, a release complete message is sent and the channel is closed.
7. The gateway clears the call by using the procedures defined below.

An endpoint receiving an endSessionCommand message without first having transmitted it carries out steps 1 and 7 above, except that in Step 5, the gateway waits for the endSessionCommand message from the first endpoint.

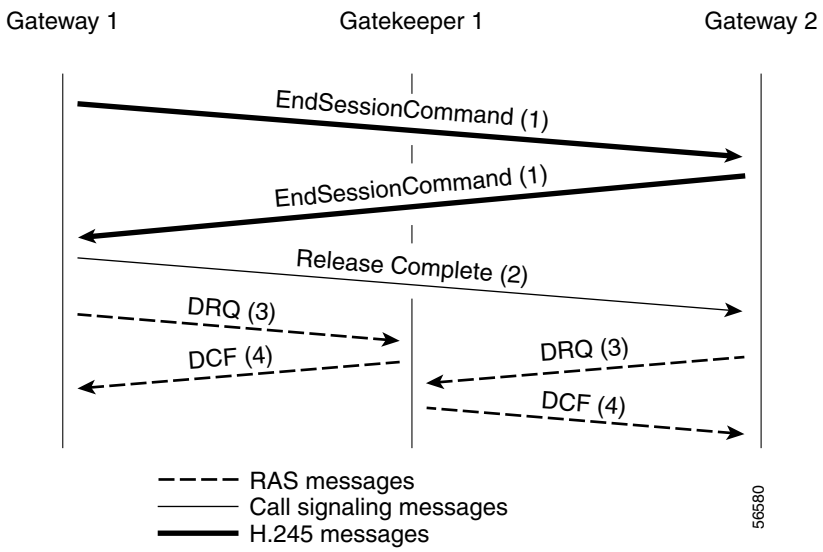
Terminating a call may not terminate a conference; a conference may be explicitly terminated using an H.245 message (**dropConference**). In this case, the gateways wait for the multipoint controller to terminate the calls as described.

Call Clearing with a Gatekeeper

In networks that contain a gatekeeper, the gatekeeper needs to know about the release of bandwidth. After performing steps 1 to 6 above, each endpoint transmits an H.225.0 disengage request (DRQ) message (3) to its gatekeeper (shown in Figure 50). The gatekeeper responds with a disengage confirm (DCF) message (4). After sending the DRQ message, the endpoints do not send further unsolicited information request response (IRR) messages that relate to that call to the gatekeeper. At this point, the call is terminated. Figure 50 shows the direct call model.

The DRQ and DCF messages are sent on the RAS channel.

Figure 50 Call Termination Direct Call Model



H.323 Feature Overview

This section includes the following subsections:

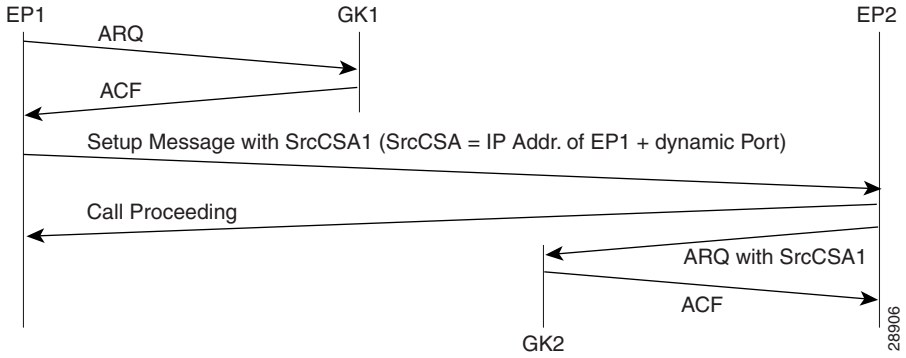
Source Call Signal Address

Source call signal address allows a source call-signal address field to be included in the ARQ.

Previously, in the Cisco IOS implementation of H.323 gateway software, if the terminating gateway was registered to an H.323 gatekeeper and used RAS, the ARQ message sent for each incoming call did not contain the H.225.0 source call signal address (CSA). The source CSA is an optional parameter in the ARQ message. The source CSA is also an optional parameter in the H.225.0 call setup message sent by the originating endpoint.

Source call signal address also allows for the source CSA parameter to be included in the ARQ message, as illustrated by the message sequence shown in Figure 51.

Figure 51 Source Call Signal Message Sequence



In the message sequence shown in Figure 51, the ARQ messages are enhanced to send the source CSA. The originating gateway (EP1) sends the H.225.0 setup message to the destination gateway. The setup message contains the source CSA parameter, which is the combination of the IP address of the originator and the dynamic TCP port number used or obtained for the H.225.0 call signaling channel. If the terminating gateway (EP2) accepts the call upon receipt of the setup message, the gateway sends an ARQ message to the gatekeeper. The terminating gateway retrieves the source CSA parameter sent by the originating gateway in the setup message. It then sends an ARQ message to the gatekeeper with the source CSA parameter. The CSA parameter is optional and has the same value as the source CSA in the received setup message. If the setup message does not contain the source CSA parameter, the terminating gateway determines the source CSA by using the H.225.0 call-signaling TCP socket connection of the peer endpoint, which it uses in the ARQ message.

If the originating gateway is registered to a gatekeeper and RAS is used as the session target, the originating gateway also sends an ARQ message. This ARQ does not include the optional source CSA parameter.

H.323 Version 2 Support

Cisco software complies with the mandatory requirements and several of the optional features of the H.323 Version 2 specification. Cisco H.323 Version 2 software enables gatekeepers, gateways, and proxies to send and receive all the required fields in H.323 Version 2 messages. Cisco H.323 Version 2 features include the following:

Lightweight Registration

Before the release of its H.323 Version 2 software, Cisco gateways reregistered with the gatekeeper every 30 seconds. Each registration renewal used the same process as the initial registration, even though the gateway was already registered with the gatekeeper. These registration renewals generated considerable overhead at the gatekeeper.

Cisco H.323 Version 2 software defines a lightweight registration procedure that still requires the full registration process for initial registration but that uses an abbreviated renewal procedure to update the gatekeeper and minimize overhead.

Lightweight registration requires each endpoint to specify a time-to-live (TTL) value in its registration request (RRQ) message. When a gatekeeper receives an RRQ message with a TTL value, it returns an updated TTL timer value in a registration confirmation (RCF) message to the endpoint. Shortly before the TTL timer expires, the endpoint sends an RRQ message with the KeepAlive field set to TRUE, which refreshes the existing registration.

It is not required that an H.323 Version 2 endpoint indicate a TTL in its registration request. If the endpoint does not indicate a TTL, the gatekeeper assigns one and sends it to the gateway in the RCF message. No configuration changes are permitted during a lightweight registration, so all fields other than the endpointIdentifier, gatekeeperIdentifier, tokens, and TTL are ignored. In the case of H.323 Version 1 endpoints that cannot process the TTL field in the RCF, the gatekeeper probes the endpoint with information requests (IRQs) for a predetermined grace period to see if the endpoint is still alive.

Improved Gateway Selection Process

Cisco H.323 Version 2 software improves the gateway selection process as follows:

- When more than one gateway is registered in a zone, the updated **zone prefix** command allows selection priorities to be assigned to these gateways on the basis of the dialed prefix.
- Gateway resource reporting allows the gateway to notify the gatekeeper when H.323 resources are getting low. The gatekeeper uses this information to determine which gateway it will use to complete a call.

The gatekeeper maintains a separate gateway list, ordered by priority, for each of its zone prefixes. If a gateway does not have an assigned priority for a zone prefix, it defaults to priority 5, which is the median. To explicitly bar the use of a gateway for a zone prefix, the gateway must be defined as having a priority 0 for that zone prefix.

When selecting gateways, the gatekeeper identifies a target pool of gateways by performing a longest zone prefix match; then it selects from the target pool according to priorities and resource availability. If all high-priority gateways are busy, a low-priority gateway might be selected.

Gateway Resource Availability Reporting

To allow gatekeepers to make intelligent call routing decisions, the gateway reports the status of its resource availability to its gatekeeper. Resources that are monitored are digital signal level 0 (DS0) channels and digital signal processor (DSP) channels. In Cisco IOS Release 12.1, this feature is available only on the AS5300 platform.

The gateway reports its resource status to the gatekeeper using the RAS Resource Availability Indication (RAI). When a monitored resource falls below a configurable threshold, the gateway sends a RAI to the gatekeeper indicating that the gateway is almost out of resources. When the available resources then cross over another configurable threshold, the gateway sends a RAI indicating that the resource depletion condition no longer exists. Resource reporting thresholds are configured by using the **resource threshold** command. The upper and lower thresholds are separately configurable to prevent the gateway from operating sporadically because of the availability or lack of resources.

Support for Single-Proxy Configurations

Cisco H.323 Version 2 software supports single-proxy, two-proxy, and no-proxy calls. Proxies can also be independently configured to meet the needs of inbound and outbound call scenarios.

Registration of E.164 Addresses for Gateway-Attached Devices

If phones are connected directly to the gateway, the Cisco H.323 Version 2 gateway allows fully qualified E.164 numbers to be registered with the gatekeeper. When configuring the gateway, use the **register** command to register these E.164 numbers.

Tunneling of Redirecting Number Information Element

An incoming PRI setup message may contain either a Redirecting Number (RDN) Information Element (IE) or an Original Called Number (OCN) IE. These IEs indicate that the call has been redirected (forwarded) and that each message contains the following:

- The destination number (DN) that was originally called
- The reason for the call being redirected
- Other related information

OCN IE is a Nortel variant of the RDN IE.

The H.323 Version 2 gateway passes the entire RDN or OCN IE from an incoming PRI message into the H.225.0 setup message. The IE is encapsulated in the nonStandardData field within the user-to-user information element (UUIE) of the H.225.0 setup message. The nonStandardData field can contain the encapsulated RDN or OCN IE and a tunneled global, signaling, and control standard QSIG message, or it can contain only the OCN or RDN. Cisco and other third-party H.323 endpoints can access the redirected information by decoding the nonStandardData field. In accordance with the H.225.0 specification, the nonStandardData is ignored by third-party endpoints and causes no interoperability problems.

For redirected PRI calls that are routed to a Cisco gateway, that are sent using H.323 to another Cisco gateway, and that exit the gateway using PRI, the RDN/OCN IE is tunneled from the source gateway to the destination gateway. The incoming PRI setup message is tunneled through H.225.0 and is encoded into the outgoing PRI setup message by the destination gateway.

Tunneling the RDN or OCN IE is important for applications such as Unified Messaging servers that need to know the telephone number that was originally dialed so as to access the correct account information.

DTMF Relay

Dual-Tone Multifrequency (DTMF) is the tone generated on a touchtone phone when the keypad digits are pressed. During a call, DTMF may be entered to access interactive voice response (IVR) systems, such as voice mail and automated banking services.

In previous releases of Cisco IOS software, DTMF is transported in the same way as voice. This approach can result in problems accessing IVR systems. Although DTMF is usually transported accurately when using high-bit-rate voice codecs such as G.711, low-bit-rate codecs such as G.729 and G.723.1 are highly optimized for voice patterns and tend to distort DTMF tones. As a result, IVR systems may not correctly recognize the tones.

DTMF relay solves the problem of DTMF distortion by transporting DTMF tones "out-of-band" or separate from the encoded voice stream. Cisco H.323 Version 2 software introduces the following three options to the existing **dtmf-relay** command for sending DTMF tones out-of-band:

- A Cisco proprietary RTP-based method (**dtmf-relay cisco-rtp** command)
- H.245 signal (**dtmf-relay h245-signal** command)
- H.245 alphanumeric (**dtmf-relay h245-alphanumeric** command)

If none of these options is selected, DTMF tones are transported in-band and encoded in the same way as voice traffic.

The **dtmf-relay cisco-rtp** command sends DTMF tones in the same Real-Time Protocol (RTP) channel as voice. However, the DTMF tones are encoded differently from the voice samples and are identified by a different RTP payload type code. This method accurately transports DTMF tones, but because it is proprietary, it requires the use of Cisco gateways at both the originating and terminating endpoints of the H.323 call.

The **dtmf-relay h245-signal** and **dtmf-relay h245-alphanumeric** commands are modes of DTMF transport defined by the ITU H.245 standard. These methods separate DTMF digits from the voice stream and send them through the H.245 signaling channel instead of the RTP channel. The tones are transported in H.245 user input indication messages. The H.245 signaling channel is a reliable channel, so the packets that transport the DTMF tones are guaranteed to be delivered. However, because of the overhead that is generated by using a reliable protocol, and depending on network congestion conditions, the DTMF tones may be slightly delayed. This delay is not known to cause problems with existing applications.

The **dtmf-relay h245-signal** command relays a more accurate representation of a DTMF digit than does the **dtmf-relay h245-alphanumeric** command because tone duration information is included along with the digit value. This information is important for applications requiring that a key be pressed for a particular length of time. For example, one popular calling card feature allows the caller to terminate an existing call by pressing the # key for more than 2 seconds and then making a second call without having to hang up in between. This feature is beneficial because the access number and personal identification number (PIN) code do not need to be dialed again. Outside-line access charges, which are common at hotels, may also be avoided.

The **dtmf-relay h245-alphanumeric** command simply relays DTMF tones as ASCII characters. For instance, the DTMF digit 1 is transported as the ASCII character 1. There is no duration information associated with tones in this mode. When the Cisco H.323 gateway receives a DTMF tone using this method, it will generate the tone on the Public Switched Telephone Network (PSTN) interface of the call using a fixed duration of 500 milliseconds. All systems that are H.323 Version 2-compliant are required to support the **dtmf-relay h245-alphanumeric** command, but support of the **dtmf-relay h245-signal** command is optional.

The ability of a gateway to receive DTMF digits in a particular format and the ability to send digits in that format are independent functions. No configuration is necessary to receive DTMF digits from another H.323 endpoint using any of the methods described. The Cisco H.323 Version 2 gateway is capable of receiving DTMF tones transported by any of these methods at all times.

However, to send digits out-of-band using one of these methods, two conditions must be met:

- The chosen method of DTMF relay must be enabled during dial-peer configuration using the **dtmf-relay** command.
- The peer (the other endpoint of the call) must indicate during call establishment that it is capable of receiving DTMF in that format.

More than one DTMF relay option may be enabled for a particular dial peer. If more than one option is enabled, and if the peer indicates that it is capable of receiving DTMF in more than one of these formats, the gateway will send DTMF using the method among the supported formats that it considers to be the most preferred. The preferences are defined as follows:

- **dtmf-relay cisco-rtp** (highest preference)
- **dtmf-relay h245-signal**
- **dtmf-relay h245-alphanumeric**

If the peer is not capable of receiving DTMF in any of the modes that were enabled, DTMF tones will be sent in-band.

When the Cisco H.323 Version 2 gateway is involved in a call to a Cisco gateway that is running a version of Cisco IOS software prior to Release 12.0(5)T, DTMF tones will be sent in-band because those systems do not support DTMF relay.

See the “Configuration Task List” section in the “Configuring H.323 Gateways and Proxies” chapter for an example of configuring DTMF relay.

H.245 Tunneling of DTMF Relay in Conjunction with Fast Connect

Through H.245 tunneling, H.245 messages are encapsulated within H.225.0 messages without using a separate H.245 TCP connection. When tunneling is enabled, one or more H.245 messages can be encapsulated in any H.225.0 message. H.245 tunneling is not supported as a stand-alone feature; initiation of H.245 tunneling procedures can be initiated only by using the **dtmf-relay** command and only from an active fast connect call. Furthermore, if **dtmf-relay** is configured on a Version 2 VoIP dial peer and the active call has been established by using fast connect, tunneling procedures initiated by the opposite endpoint are accepted and supported.

H.245 tunneling is backward compatible with H.323 Version 1 configurations.

Translation of FXS Hookflash Relay

A hookflash indication is a brief on-hook condition that occurs during a call. It is not long enough in duration to be interpreted as a signal to disconnect the call. Create a hookflash indication by quickly depressing and then releasing the hook on your telephone.

PBXs and telephone switches are frequently programmed to intercept hookflash indications and use them as a way to allow a user to invoke supplemental services. For example, your local service provider may allow you to enter a hookflash as a means of switching between calls if you subscribe to a call waiting service.

In the traditional telephone network, a hookflash results in a voltage change on the telephone line. Because there is no equivalent of this voltage change in an IP network, the ITU H.245 standard defines a message representing a hookflash. To send a hookflash indication using this message, an H.323 endpoint sends an H.245 user input indication message containing a "signal" structure with a value of "!". This value represents a hookflash indication.

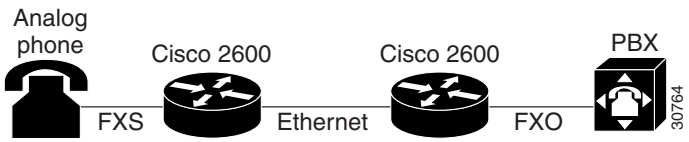
Cisco H.323 Version 2 software includes limited support for relaying hookflash indications using the H.245 protocol. H.245 user input indication messages containing hookflash indications that are received on the IP call leg are forwarded to the plain old telephone service (POTS) call leg if the POTS interface is Foreign Exchange Office (FXO). If the interface is not FXO, any H.245 hookflash indication that is received is ignored. This support allows IP telephony applications to send hookflash indications to a PBX through the Cisco gateway and thereby invoke the IOS supplementary services of the PBX if the PBX supports access to those features using hookflash.

The gateway does not originate H.245 hookflash indications in this release. For example, it does not forward hookflash indications from Foreign Exchange Station (FXS) interfaces to the IP network over H.245.

The acceptable duration of a hookflash indication varies by equipment vendor and by country. Although one PBX may consider a 250-millisecond on-hook condition to be a hookflash, another PBX may consider this condition to be a disconnect. Therefore, the **timing hookflash-out** command allows the administrator to define the duration of a hookflash signal generated on an FXO interface.

Figure 52 illustrates an FXS hookflash being translated to an H.245 user input.

Figure 52 Translating an FXS Hookflash to an H.245 User Input



In the Cisco H.323 Version 2 software, an FXS hookflash relay is generated only if the following two conditions are met:

- The other endpoint must support the reception of an H.245 hookflash and advertise this using the "Receive User Input Capability" message during H.245 capabilities exchange.
- The call must be established with either the **h245-alphanumeric** or **h245-signal** variant of the **dtmf-relay** command.

This implies that the VoIP dial peer must be configured for **dtmf-relay h245-alphanumeric** or **h245-signal**, but not **cisco-rtp**.

Enter the **timing hookflash-input** command on FXS interfaces to specify the maximum length in milliseconds of a hookflash indication. If the hookflash lasts longer than the specified limit, then the FXS interface processes the indication as an onhook.

The acceptable duration of a hookflash indication varies by equipment vendor and by country. One PBX may consider a 250 milliseconds on-hook condition to be a hookflash; another PBX may consider this condition to be a disconnect.

H.235 Security

Security for RAS protocol signaling between H.323 endpoints and gatekeepers is enhanced in H.323 Version 2 software by including secure endpoint registration of the Cisco gateway to the Cisco gatekeeper and secure per-call authentication. In addition, it provides for the protection of specific messages related to Open Settlement Protocol (OSP) and to other messages as required via encryption tokens. The authentication type is "password with hashing" as described in the ITU H.235 specifications. Specifically, the encryption method is to use the MD5 algorithm, with password hashing. This functionality is provided by the **security token required-for** command on the gatekeeper and the **security password** command on the gateway.

The gatekeeper can interact with a RADIUS security server to perform the authentications. The gateway can also authenticate an external application by using the Gatekeeper Transaction Message Protocol (GKTMP) application programming interface (API).

Per-call authentication is accomplished by validating account and pin numbers that are entered by the user connected to the calling gateway by using an IVR prompt.

The security mechanisms described above require the gateway and gatekeeper clocks to be synchronized within 30 seconds of each other by using a Network Time Protocol (NTP) server.

GKTMP and RAS Messages

The GKTMP for the Cisco gatekeeper provides a transaction-oriented application protocol that allows an external application to modify gatekeeper behavior by processing specified RAS messages.

A set of triggers can be specified that use RAS messages that can be recognized by the gatekeeper. Triggers are specified filter conditions that must match each type of RAS message. The triggers can be dynamically registered by using the external application, or this information can be configured by using the command-line interface (CLI) on the gatekeeper.

When the gatekeeper receives a RAS message that meets the specified trigger conditions, it forwards the message to the external application in a GKTMP message format. This message is text encoded and sent over TCP. The external application can then modify fields in the message before returning it to the gatekeeper for further processing, or it may return a RAS response to the gatekeeper to be forwarded to the RAS client.

The following messages can be sent in GKTMP:

- ACF—admission confirm
- ARJ—admission reject
- ARQ—admission request
- LCF—location confirm
- LRJ—location reject
- LRQ—location request
- RCF—registration confirm
- RRJ—registration reject
- RRQ—registration request
- URQ—unregistration request

The application server interprets RAS messages in the following ways:

- For RRQ and URQ, the application server performs gatekeeper authorization, storing endpoint RAS gatekeeper IP addresses and maintaining gatekeeper resource control.

- For ARQ and LRQ, the application server performs authorization and digit translation functions and returns terminating IP addresses or a new E.164 address to the gatekeeper for reorigination by the originating gateway.
- For LCF and LRJ, the application server intercepts location responses from a distant gatekeeper and modifies the message fields before responding to the originating gateway.

Note Cisco has developed an API that can be used to provide an interface to the Cisco gatekeeper. Refer to the *Cisco Gatekeeper External Interface Reference*.

To configure the gatekeeper to receive trigger registrations from the external applications, specify the registration port of the server using the **server registration-port** command. This command tells the gatekeeper to listen for server connections.

You can also configure the gatekeeper to initiate the connection to a specified external application by using the **server trigger** command to specify a set of static trigger conditions for a specified server. Only one application server can be specified for each **server trigger** command. All RAS messages that do not match the selection criteria for any external application are processed normally by the gatekeeper. The **show gatekeeper servers** and **debug gatekeeper servers** commands can be entered to assist in the configuration.

See the "Gatekeeper Transaction Message Protocol and RAS Messages Example" in the "Configuring H.323 Gatekeepers and Proxies" chapter of this configuration guide.

RAS Message Fields

In support of the H.323 security and accounting features, fields have been added to several of the RAS messages effective with Cisco IOS Release 12.0(7)T. In general, all the RAS messages sent by the gateway, with the exception of the gateway request (GRQ), include authentication data in the cryptoToken field. This section lists each of the messages that changed effective with Cisco IOS Release 12.0(7)T and describes the fields that have been added.

GRQ Message

When H.323 security is enabled on the gateway, the following fields are added to the GRQ message:

Field	Description
authenticationCapability	This field should have a value of pwdHash.
algorithmOIDs	The object ID for the MD5 algorithm. The object identifier (OID) used to indicate MD5 will be {1 2 840 113549 2 5}.

GCF Message

When H.323 security is enabled on the gateway, the following fields should be in the gateway confirmation (GCF) message:

Field	Description
authenticationMode	This field should have a value of pwdHash.
algorithmOIDs	The object ID for the MD5 algorithm. The OID used to indicate MD5 will be {1 2 840 113549 2 5}.

If the authenticationMode or the algorithm OIDs fields do not contain the values specified above, the gatekeeper responds with a gatekeeper rejection (GRJ) message that contains a reject reason of securityDenial. This prompts the gateway to resend the GRQ .

RRQ Message

If H.323 security is enabled on the gateway, the following fields are added to the RRQ message:

Field	Description
cryptoTokens	This field contains one of the cryptoToken types defined for the CryptoH323Token field specified in H.225.0. Currently, the only type of cryptoToken supported is cryptoEPPwdHash.

The following fields are contained within the cryptoEPPwdHash structure:

Field	Description
alias	The gateway alias, which is the H.323 ID of the gateway.
timestamp	The current time stamp.
token	The MD5 encoded PwdCertToken. This field contains the following: timestamp—The same as the time stamp of cryptoEPPwdHash. password—The password of the gateway. generalID—The same gateway alias as the one included in the cryptoEPPwdHash. tokenID—The object ID.

ARQ Message

When H.323 security is enabled on the gateway, additional fields are included in the ARQ message. The contents of the field depend on whether the ARQ message is sent from the source gateway or the destination gateway.

Source Gateway ARQ Message

If the ARQ message is sent from the source gateway, the following fields are included:

Field	Description
cryptoTokens	This field contains one of the cryptoToken types defined for the CryptoH323Token field specified in H.225.0. Currently, the only type of cryptoToken supported is cryptoEPPwdHash.

The following fields are contained within the cryptoEPPwdHash structure:

Field	Description
alias	The account number of the user or the H.323 ID of the gateway if endpoint authentication is selected.
timestamp	The current time stamp.
token	The MD5 encoded PwdCertToken. This field contains the following: • timestamp—The same as the time stamp of cryptoEPPwdHash. • password—If "endpoint" is selected, this is the security password of the gateway. Otherwise, it is the password or PIN of the user. • generalID—If "endpoint" is selected, this is the H.323 ID of the gateway. Otherwise, it is the ID or account number of the user. • tokenID—The object ID.

Destination Gateway ARQ Message

If the ARQ message is sent from the destination gateway, the following fields are included:

Field	Description
cryptoTokens	This field contains one of the cryptoToken types defined for the CryptoH323Token field specified in H.225.0. Currently, the only type of cryptoToken supported is cryptoEPPwdHash.

The following fields are contained within the cryptoEPPwdHash structure:

Field	Description
alias	The alias (H.323 ID or E.164 address) of the destination gateway.
timestamp	The current time stamp.

Field	Description
token	The MD5 encoded PwdCertToken. This field contains the following: timestamp—The same as the time stamp of cryptoEPPwdHash. password—The password of the destination gateway. generalID—The same gateway alias as the one included in cryptoEPPwdHash. tokenID—The object ID.

ACF Message

If H.323 security is enabled on the gateway, the gatekeeper should include the billing-related information from the nonStandardParameter field of the clearTokens structure. If the call is using a prepaid call service, the clearTokens field should indicate the maximum call duration. In the case of prepaid call service, the gateway will terminate the call if it exceeds the allowed time.

The following clearToken fields should be included in the ACF message:

Field	Description
nonStandard	The billing information for the call.
tokenOID	The generic billing object ID.

The following fields are contained within the nonStandardParameter structure:

Field	Description
nonStandardIdentifier	The generic billing object ID.
BillingInfo	The billing information. This field can contain the following: • bill_to—A string that identifies the subscriber that should be billed for this call. • reference_id—A unique ID generated by the billing system. • billing_mode—Whether the call is being made using prepaid call service (debit_mode) or not (credit_mode). • max_duration—The maximum duration allowed for the call. Used only for prepaid call service. • balance—The account balance of the caller. For a billing mode of credit_mode, this should be a negative value that represents the current amount owed by the subscriber. Otherwise, this should be a positive value that represents the credit remaining on the debit account of the subscriber. • currency—The currency used in reporting the balance. • timezone—The time zone of the call, represented by a hexadecimal string that indicates the difference in seconds between the location of the caller and the Universal Time Coordinated (UTC).

DRQ Message

The gateway sends a DRQ message when the call ends. If H.323 security is enabled on the gateway, the call usage information is included in the DRQ message. The call usage information is sent in the nonStandardParameter field of the ClearToken structure.

The following fields are contained within the nonStandardParameter structure:

Field	Description
duration	The duration of the call in seconds.
callLog	The call usage information. This field contains the following information: • DISCONNECT_REASON—The disconnect reason. Possible values are as follows: – DISCONNECT_NORMAL—The call ended normally. – DISCONNECT_DISCONNECT—The call ended because of a technical failure. – DISCONNECT_ABANDONED—The call never took place; for example, the remote phone was not answered. – DISCONNECT_PREEMPT—The call was ended by the gateway. This would be the disconnect reason issued if the call was ended because the max_duration was exceeded. • DISCONNECT_STRING—A string that further describes the disconnect reason. • TIME—The time at which the call started, indicated by a hexadecimal string that represents the time, in seconds, since 00:00 January 1, 1970 UTC. • ORIGIN—Whether the call was inbound or outbound.

Multizone Features

Cisco multizone software enables the Cisco gateway to provide information to the gatekeeper using additional fields in the RAS messages. The gatekeeper no longer terminates a call if it is unable to resolve the destination E.164 phone number with an IP address.

Previously, the source gateway attempted to set up a call to a destination IP address as provided by the gatekeeper in an admission confirm (ACF) message. If the gatekeeper was unable to resolve the destination E.164 phone number to an IP address, the incoming call was terminated.

Multizone software allows a gatekeeper to provide additional destination information and modify the destinationInfo field in the ACF message. The gateway will include the canMapAlias-associated destination information in setting up the call to the destination gateway.

The gatekeeper indicates to the gateway that the call should be destined to a new E.164 number by sending an ACF message with an IP address of 10.0.0.0 in the destCallSignalAddress field and the new destination E.164 phone number in the destinationInfo field.

The gateway that receives such an ACF will fall back to routing the call on the basis of this new E.164 address and performing a relookup of the configured dial plan for the gateway. If the gateway routes the call on the basis of the new E.164 address, the call might be routed back to the PSTN or to an H.323 endpoint.

Codec Negotiation

Codec negotiation allows the gateway to offer several codecs during the H.245 capability exchange phase and to ultimately settle on a single common codec during the call establishment phase. Offering several codecs increases the probability of establishing a connection because there will be a greater chance of overlapping voice capabilities between endpoints. Normally, only one codec can be specified when a dial peer is configured, but codec negotiation allows a prioritized list of codecs associated with a dial peer to be specified. During the call establishment phase the router will use the highest priority codec from the list that it has in common with the remote endpoint. It will also adjust to the codec selected by the remote endpoint so that a common codec is established for both the receive and send voice directions.

When a call is originated, all the codecs associated with the dial peer are sent to the terminating endpoint in the H.245 terminal capability set message. At the terminating endpoint, the gateway will advertise all the codecs that are available in firmware in its terminal capability set. If there is a need to limit the codecs advertised to a subset of the available codecs, a terminating dial peer must be matched that includes this subset. The **incoming called-number** command in dial peer configuration mode can be used to force this match.

Supported Codecs

The supported codecs are available for use with Cisco H.323 Version 2 software. Table 18 lists each codec with a default packet size (in bytes) and a range.

Table 18 Codec Default Packet Size

Codecs	Range (in bytes)	Default (in bytes)	Bit Rate
G.711ulaw	40–240	160	64 kbps
G.711alaw	40–240	160	64 kbps
G.723r63	24–240	24	6.3 kbps
G.723r53	20–240	20	5.3 kbps
G.723ar63	24–240	24	6.3 kbps
G.723ar53	20–240	20	5.3 kbps
G.726r32	20–240	40	32 kbps
G.726r24	15–240	30	24 kbps
G.726r16	10–240	20	16 kbps
G.728	10–240	10	16 kbps
G.729br8	10–240	20	8 kbps
G.729r8 pre-ietf	10–240	20	8 kbps
G.729r8	10–240	20	8 kbps

Note A separate codec for G.729 Annex B is included, which adds Annex B functionality to G.729. A separate codec for G.723.1 Annex A adds Annex A functionality to G.723.1.

Note The Annex B functionality added to G.729 and the Annex A functionality added to G.723.1 are the built-in, codec-specific voice-activated detection/calling tone (VAD/CNG) functions.

H.245 Empty Capabilities Set

Empty capabilities set support is a mandatory part of the H.323 Version 2 standard. It is used by applications to redirect the voice media stream. This feature is particularly useful for applications such as the following:

- Selsius IP phones, which rely on a hub or call manager to direct the media stream to IP phones.
- Unified messaging for which it is desirable to redirect the media stream to various message servers for message playout.

The empty capabilities set feature was added to provide a way to redirect RTP streams. The RTP streams are redirected as follows:

- The sequence starts with the an empty capabilities set being received at an endpoint.
- After an open logical channel (OLC) is established (or if in the middle of this process) one of the endpoints sends an empty capabilities set message.
- When the empty capabilities set message is received, the other endpoints close the logical channel if any was opened with that endpoint and move to a pause state, waiting for a nonempty capability set message.

After receiving the nonempty capabilities set message, the endpoint moves to the beginning of Phase B, which is the initial communication and capabilities exchange, as described in H.323 Version 3 (June 1999), item 8.4.6.

In other words, the exchange of the capabilities message determines a master/slave relationship, and a new OLC message is created to open a new logical channel with another endpoint. From this point on, the RTP streams are sent to the new endpoint.

H.323 Version 2 Fast Connect

Fast connect allows endpoints to establish media channels without waiting for a separate H.245 connection to be opened. This streamlines the number of messages that are exchanged and the amount of processing that must be done before endpoint connections can be established. A high-level view of the fast connect procedures within the H.323 protocol follows:

1. The calling endpoint transmits a setup message containing the fastStart element that contains a sequence of encoded logical channel structures, each representing a different capability media type for both “send” and “receive” directions.
2. The called endpoint selects one or more of the media types offered by the calling endpoint for the send and receive directions and returns its selections in a fastStart element in any H.225.0 message up to and including connect. At this point, the called endpoint must be prepared to receive media along any of the channels it selected.
3. If H.245 procedures are needed and one or both of the endpoints do not support tunneling, a separate H.245 connection is used.

Fast Connect is not explicitly configurable. All H.323 Version 2 VoIP endpoints are capable of initiating or accepting fast connect calls. It is assumed that the gateway is capable of sending and receiving fast connect procedures unless its corresponding dial peer has been configured for the Resource Reservation Protocol (RSVP). (In other words, the req-qos is set to a value other than the default of best-effort.) If the dial peer has been configured for RSVP, traditional "slow" connect procedures are followed, and the endpoint neither attempts to initiate fast connect nor responds to a fast connect request from its peer.

A terminating endpoint can reject fast connect by simply omitting the fastStart element from all H.225.0 messages up to and including connect. In this case, normal H.245 procedures are followed and a separate H.245 TCP connection is established. So, if an endpoint does not support the fast connect procedures, normal H.245 procedures are followed. In addition, certain conditions can cause a fast connect call to fall back to normal H.245 procedures to complete the call.

Once a media connection has been opened (an audio path has been established), either endpoint has the option of switching to H.245 procedures (if they are needed) by using H.245 tunneling, whereby H.245 messages are encapsulated within the h245Control element of H.225.0 messages.

The **dtmf-relay** command is the only H.245 cognizant command that can initiate H.245 tunneling procedures from a fast connect call. If H.245 tunneling is active on the call, switching to a separate H.245 connection is not supported.

A Cisco terminating endpoint accepts a fast connect request only if a pair of symmetric codecs (codecs that in both directions are equivalent or identical) can be selected from a list that has been offered. The originating endpoint is constrained only by what it can send through the codec (or voice class codec list) associated with the dial peer.

If the Cisco originating endpoint has offered multiple codecs and the terminating endpoint selects a pair of asymmetric (mismatched) codecs, the originating endpoint initiates separate H.245 procedures to correct the asymmetric codec situation.

Fast connect is backward compatible with H.323 Version 1 configurations.

Note Because fast connect is compliant with H.323 Version 2 and because the majority of endpoints prefer to establish a call by using fast connect procedures, this feature is not configurable. The H.323 fast connect feature does not require any additional configuration beyond a working voice configuration.

H.450.2 Call Transfer

Call transfer allows an H.323 endpoint to redirect an answered call to another H.323 endpoint. Cisco gateways support H.450.2 call transfer as the transferring and transferred-to party. The transferring endpoint must be an H.450-capable terminal; the Cisco gateway cannot act as the transferring endpoint. Gatekeeper-controlled or gatekeeper-initiated call transfer is not supported.

Note Certain devices are limited in their support of H.450. The Cisco 1700 and uBR820 platforms do not support IVR. Therefore, these platforms are not able to act as H.450 transferring endpoints.

H.450.2 specifies two variants of call transfer:

- Transfer without consultation—The transferring endpoint supplies the number of the transferred-to endpoint as part of the transfer request, and the two remote endpoints are transferred together. A Cisco gateway cannot be the transferring endpoint.
- Transfer with consultation—This feature is not currently supported.

H.450.3 Call Deflection

Call deflection is a feature under H.450.3 Call Diversion (Call Forwarding) that allows a called H.323 endpoint to redirect the unanswered call to another H.323 endpoint. Cisco gateways support H.450.3 call deflection as the originating, deflecting, and deflected-to gateway. The Cisco gateway as the deflecting gateway supports invocation of call deflection only by using an incoming PRI QSIG message (call deflection cannot be invoked by using any other trunk type).

If the deflecting endpoint is a Cisco gateway, the telephony endpoint on the PRI of the deflecting gateway invokes call deflection by sending an equivalent QSIG reroute invoke request within a FACILITY message to the gateway. The deflecting gateway then uses the procedures outlined in the H.450.3 call deflection standard to transfer the call to another endpoint. Note that the initiation of deflection using QSIG reroute invoke is valid only on calls that arrived as H.323 calls at the deflecting gateway. In other words, for calls that arrive at the gateway through a telephony interface (such as a hairpin call) or by using a non-H.323 IP protocol, QSIG reroute invoke is ignored.

Cisco H.323 Version 2 software does not support gatekeeper-controlled or gatekeeper-initiated call deflection.

Note Certain devices are limited in their support of the H.450 standard. The Cisco AS5800 universal access server is not able to convert QSIG to H.450. The Cisco 1700 and uBR820 platforms do not support IVR. Therefore, these devices are not able to act as H.450 deflecting endpoints.

Gateway Support for Alternate Endpoints

Alternate endpoints allow a gatekeeper to specify alternative destinations for a call when queried with an ARQ by an originating gateway. If the first destination gateway fails to connect, the gateway tries all the alternate destinations before going to the next dial peer rotary (if a rotary is configured).

Note This feature is not supported by the Cisco gatekeeper; it is intended for use with third-party gatekeepers that implement the alternate endpoint field in the ACF message. No support is provided for the gateway to send a list of alternate endpoints in RRQ messages.

Gatekeeper C Code Generic API for GKTMP in a UNIX Environment

This API allows third-party applications that run in a UNIX host to send GKTMP messages to a Cisco gatekeeper and receive GKTMP messages from a Cisco gatekeeper. This API may be used to develop back-end services such as authentication, billing, and address translation.

Gateway Support for a Network-Based Billing Number

Gateway support for a network-based billing number informs the gatekeeper of the specific voice port or T1/E1 span from which an incoming call entered the ingress gateway. This is done using a Cisco proprietary, nonstandard field that has been added to the ARQ message sent by the ingress gateway. No configuration is necessary for this feature.

Gateway Support for Voice-Port Description

Gateway support for voice-port description provides the gatekeeper with a configurable string that identifies the voice port or T1/E1 span from which an incoming call entered the ingress gateway. This is done using a Cisco proprietary, nonstandard field that has been added to the ARQ message sent by the ingress gateway. The string in the ARQ message corresponds to the setting of the **voice-port description** command.

Gateway support for voice-port description is similar to the network-based billing number feature, but it differs in two important respects:

- The voice-port description field is only included in the ARQ message if the voice-port description is configured through the CLI for the applicable voice port.
- Because the voice-port description is configurable, the user can provide customer-specific information to the gatekeeper. For example, the voice-port description can be configured to correspond to the carrier identification code (CIC) for calls received on a particular T1/E1 span.

H.323 Signaling

When interworking with ISDN, with T-1 channel-associated signaling (CAS), and with E-1 R2 services from the PSTN, H.323 signaling enables VoIP networks to properly signal the setup and teardown of calls. In-band tones and announcements are generated as needed at the originating or terminating switch. When a tone is played at the destination switch, the backward voice path from the called party to the calling party is cut through early so that the calling party can hear the tone or announcement. To prevent fraudulent calls, the voice path is cut through in both directions only after the connect message is received from the destination. The call progress indicator, which signals the availability of in-band communication, is carried end to end as required when interworking with ISDN and CAS protocols.

The H.323 signaling feature prevents unexpected behavior, such as early alerting (when an alert message is returned immediately after a call proceeding message is sent), to ensure that the calling party does not hear conflicting call progress information, such as a ringback tone followed by a busy tone, and does not miss hearing a tone or announcement when one should play. Support for network-side ISDN and reduction in the risk of speech clipping is also addressed.

The H.323 signaling feature is dependent on Cisco H.323 gateways, gatekeepers, and VoIP features.

H.323 signaling provides the following:

- In-Band Tones and Announcements, page 229
- End-to-End Alerting, page 231
- Cut-Through of Voice Path, page 231
- H.245 Initiation, page 231
- Overlap Dialing, page 232

In-Band Tones and Announcements

In-band progress tones and announcements are required for PSTN services and for ISDN speech and 3.1 kHz voice services, per Bellcore and American National Standards Institute (ANSI) specifications. To guarantee that in-band tones and announcements are generated when required and at the appropriate switch, Cisco H.323 signaling software ensures that the progress indicator (PI) is carried end to end in call-signaling messages between the called party and the calling party. The PI in outbound dial peers can also be configured at the H.323 VoIP gateway, if necessary.

The PI is an IE that signals when in-band tones and announcements are available. The PI controls whether the local switch generates the appropriate tone or announcement or whether the remote switch is responsible for the generation. For example, if the terminating switch generates the ringback tone, it sends a PI of 1 or 8 in the alerting message. If the originating switch receives an alerting message without a PI, it generates the ringback tone.

The specific PI that a switch sends in call messages, if any, depends on the model of the switch. To ensure that in-band communication is generated appropriately, it may be necessary in some instances to override the default behavior of the switch by manually configuring the PI at the Cisco H.323 gateway.

The PI is configurable in setup messages from the outbound VoIP dial peer, typically at the originating gateway, and in alert, progress, and connect messages from the outbound POTS dial peer, typically at the terminating gateway. The PI is configured by using the **progress_ind** dial-peer configuration command. Table 19 shows the PI values that may be configured on the H.323 gateway.

Table 19 Configurable Progress Indicator Values for H.323 Gateways

PI	Description	Message Type
0	No progress indicator is included.	Setup
1	Call is not end-to-end ISDN; further call progress information may be available in-band.	Alert, setup, progress, connect
2	Destination address is non-ISDN.	Alert, progress, connect
3	Origination address is non-ISDN.	Setup
8	In-band information or appropriate pattern is now available.	Alert, progress, connect

When the interworking is between ISDN and non-ISDN networks, the originating gateway reacts as follows:

- If the originating switch does not include a PI in setup messages, the originating gateway assumes that the originating switch is ISDN and expects the switch to generate the ringback tone. Determine which device generates the ringback tone by using the **progress_ind** dial-peer configuration command:
  - To enable the terminating switch to generate the ringback tone, set the PI to 8 in the alert messages on the terminating gateway. The progress indicator is configured in the POTS dial peer.
  - To enable the originating gateway to generate the ringback tone, set the PI to 3 in setup messages on the originating gateway. The PI is configured in the VoIP dial peer.

Note If the terminating gateway sends an alert message with no PI value, the originating gateway generates the ringback tone. But if the terminating gateway sends an alert message that has a PI of 1, 2, or 8, the originating gateway does not generate the ringback tone.

- The originating gateway cuts through the voice path in the backward direction when it receives a progress or alert message that has a PI of 1, 2, or 8.

Note Pure ISDN calls may use different protocols at the originating and terminating ends. For example, a call may originate on ETSI and terminate on NI2. If the two protocols are not compatible end to end, the gateway drops all IEs from messages, including the progress indicator. Because a progress indicator is required in all progress messages, the originating gateway inserts a PI of 1 in the progress message. To avoid dropping IEs, use the **isdn gateway-max-internetworking** global configuration command to prevent the gateway from checking protocol compatibility.

End-to-End Alerting

Early alerting is prevented in these ways:

- For calls that terminate at an ISDN switch—The terminating gateway sends an alert message to the originating gateway only after it receives an alert message from the terminating switch.
- For calls that terminate at a CAS switch—The terminating gateway sends a progress message, rather than an alert message, to the originating gateway after it receives a setup message.

Cut-Through of Voice Path

When tones and announcements are generated at the destination switch, the backward voice path from the called party to the calling party is cut through before the tones and announcements are played. This allows announcements, such as "The number you have called has been changed," or allows tones for error conditions, such as network congestion, to be forwarded to the calling party. To prevent fraudulent calls, the originating gateway does not perform full cut-through until it receives a connect message from the destination switch. Cut-through is performed as follows:

- For calls that terminate at an ISDN switch—The terminating gateway performs backward cut-through when it receives an alert or progress message and full cut-through (both directions) when it receives a connect message. The originating gateway performs backward cut-through when it receives a call proceeding message and full cut-through when it receives a connect message.
- For calls that terminate at a CAS switch—The terminating gateway performs backward cut-through after it sends a progress message and full cut-through (both directions) when it receives an off-hook signal. The originating gateway performs backward cut-through when it receives a progress message and full cut-through when it receives a connect message.

Note If the originating or terminating gateway sends a call proceeding message and then receives a call proceeding message with a progress indicator of 1, 2, or 8, the gateway converts this call proceeding message into a progress message with a corresponding PI.

H.245 Initiation

To avoid speech clipping, H.245 capabilities are now initiated at the originating gateway at the earliest possible moment, when the originating gateway receives a call proceeding message from the terminating gateway. Previously, call proceeding messages were not passed end to end across the VoIP network; H.245 was initiated only after the originating gateway received an alert message.

Overlap Dialing

To enhance overlap dialing, the call proceeding message is now passed transparently from the terminating switch to the originating switch if the originating switch does not include the sending complete information element in the setup message. The call proceeding message notifies the originating switch that the terminating switch has collected all dialed digits that are required to route the call. If the originating switch sends a sending complete IE, the originating gateway responds with a call proceeding message, and the session application drops the call proceeding message sent by the terminating switch.

Configurable Timers in H.225.0

When a call is attempted, a TCP connection is made: the TCP socket connection is made for the signaling that the H.225.0 protocol carries. When the timer expires, the call is timed out and attempted using another dial peer, if one has been defined. Cisco configurable timers in H.225.0 software allow users to configure the H.225.0 TCP connection timeout value for all outgoing call attempts (on a per-VoIP dial peer basis).

In previous releases of Cisco IOS software, the call attempt timeout was 15 seconds and could not be changed. In some cases, however, users might need a shorter timeout value to facilitate a faster failover. In other cases, they might need a greater timeout value.

Configurable timers in H.225 address those needs by allowing the user to override the default of 15 seconds and configure the timeout value.

See the “H.323 Configuration Task List” section for information on how to configure timers in H.225.0.

Answer Supervision Reporting

Answer supervision reporting is an enhancement to the information request (IRR) Registration, Admission, and Status (RAS) protocol message that enables gatekeepers to maintain call accounting information by reporting the call connection time of connected calls to the gatekeeper.

In H.323 configurations, the endpoint (gateway) uses direct call-routed signaling. Gatekeepers do not have real-time knowledge or control over the state of a call and are dependent on the endpoints to provide them with necessary real-time information, such as call connect time, call termination time, and call termination reason.

When a call ends, the gateway sends a DRQ message with the BillingInformationToken (which contains the duration of the call) to the gatekeeper. If for some reason the gatekeeper does not receive the DRQ message, the gatekeeper will not have the information about when the call started or the duration of the call, which is necessary to maintain accounting information.

Answer supervision reporting allows the call connection time to be reported to the gatekeeper upon the connection of a call and at periodic intervals thereafter. Answer supervision reporting adds a proprietary Cisco parameter, the call connection time, to the perCallInfo parameter in the nonStandardData field, which is located in the IRR message. When a connect message is received, the originating gateway sends the unsolicited IRR message to its gatekeeper. On sending a connect message, the terminating gateway sends the unsolicited IRR message to its gatekeeper. If the ACF message has a nonzero value for the IRR frequency parameter, the gateway sends the unsolicited IRR message to its gatekeeper at periodic intervals, which are determined by the value in the IRRfrequency parameter.

With the exception of containing the call connection time in the perCallInfo parameter, the IRR message and its functionality remain the same.

Gateway-to-Gatekeeper Billing Redundancy

Gateway-to-gatekeeper billing enhances the accounting capabilities of the Cisco H.323 gateway and provides support for VocalTec™ gatekeepers. Gateway-to-gatekeeper billing redundancy provides for redundant billing information to be sent to an alternate gatekeeper if the primary gatekeeper to which a gateway is registered becomes unavailable.

During the process of establishing a call, the primary gatekeeper sends an ACF message to the registered gateway. The ACF message includes the billing information of the user and an access token. To provide the billing information to an alternate gatekeeper if the primary gatekeeper is unavailable when the call session ends, the access token information sent in the ACF message is also included in the DRQ message that is sent to the alternate gatekeeper.

This features enables the alternate gatekeeper to obtain the billing information required to successfully complete the transaction.

For further information on configuring gateway-to-gatekeeper billing redundancy, refer to *Cisco H.235 Accounting and Security Enhancements for Cisco Gateways, Cisco H.323 Gateway Security and Accounting Enhancements,* and *Gateway Support for Alternate Gatekeeper.*

Ecosystem Gatekeeper Interoperability

Ecosystem gatekeeper interoperability adds support for the alternate gatekeeper field (altGKInfo) in the gatekeeper rejection (GRJ), registration rejection (RRJ), and admission rejection (ARJ) messages. This allows a gateway to move between gatekeepers during the GRQ, RRQ, and ARQ phases. There is no need for gateway reconfiguration or for a gatekeeper failover in the gateway.

Gateways can be configured to switch from their primary gatekeeper to an alternate gatekeeper if a failure or outage occurs. If an outage occurs and gateways move from one gatekeeper to another, there may be an imbalance in the number of gateways registered to each gatekeeper. The ecosystem gatekeeper interoperability feature helps to restore the balance (when the outage has been corrected) by allowing some of the gateways to be moved back to their proper gatekeepers.

The altGKInfo consists of two subfields: the alternateGatekeeper and the altGKisPermanent flag. The alternateGatekeeper is the list of alternate gatekeepers. The altGKisPermanent is a flag that indicates whether the gatekeepers in the associated alternateGatekeeper field are permanent or temporary.

- If the current state of the altGKisPermanent flag is TRUE, the new altGKInfo of any RAS message received from one of the alternate gatekeepers is accepted and the new list will replace the existing list.
- If the current state of the altGKisPermanent flag is FALSE, the altGKInfo of any RAS message received from one of the alternate gatekeepers will be ignored.

If the current permanent gatekeeper becomes nonresponsive and the altGKisPermanent flag is set to FALSE, the gateway sets the internal state of the altGKisPermanent flag to TRUE. This allows the gateway to accept the alternate gatekeeper list from one of the gatekeepers in the existing alternate gatekeeper list.

The handling of the altGKInfo field varies depending on whether it is included in a GRJ or an RRJ message.

For further information on configuring ecosystem gatekeeper interoperability, refer to *Gateway Support for Alternate Gatekeepers, Configuring H.323 VoIP Gateway for Cisco Access Platforms*, and *Ecosystem Gatekeeper Interoperability Enhancements*.

AltGKInfo in GRJ Messages

When the gateway accepts the alternate gatekeeper list from the GRJ, the gateway sends a GRQ message to a gatekeeper on the list. The selection is based on priority of the alternate gatekeepers. Each alternate gatekeeper is tried until a GCF message is received.

If the gateway receives a GRJ message without the AltGKInfo field, it accepts the rejection. Because this is the first phase for the gateway to contact a gatekeeper, the gateway is considered lost without a gatekeeper.

During the GRQ phase, the gateway ignores the value of the altGKisPermanent flag in any RAS message and sets the value internally to TRUE.

AltGKInfo in RRJ Messages

When the gateway accepts the alternate gatekeeper list from the first RRJ message, the gateway retransmits an RRQ message to a gatekeeper on the alternate gatekeeper list. The selection is based on priority of the alternate gatekeepers.

The retransmission of the RRQ message depends on the type of RRQ (full or lightweight), the current state of the altGKisPermanent flag, and the current state of the needToRegister flag of each alternate gatekeeper as follows:

- If the state of the altGKisPermanent flag is TRUE and the state of the needToRegister flag is NO, the gateway will retransmit the full RRQ to an alternate gatekeeper for full RRQs and a lightweight RRQ for lightweight RRQs.
- If the state of the altGKisPermanent flag is TRUE and the state of the needToRegister flag is YES, the gateway will retransmit the full RRQ to an alternate gatekeeper for full RRQs and lightweight RRQs.
- If the state of the altGKisPermanent flag is FALSE and the state of the needToRegister flag is NO, the gateway will retransmit a lightweight RRQ for lightweight RRQs and nothing for full RRQs.
- If the state of the altGKisPermanent flag is TRUE and the state of the needToRegister flag is YES, the gateway will not retransmit the RRQ.

If the gateway receives an RRJ message without the AltGKInfo field, it accepts the rejection and returns to the GRQ phase. If the state of the altGKisPermanent flag is FALSE, the gateway sends the GRQ message to the original gatekeeper that sent the first RRJ. If the state of the altGKisPermanent flag is TRUE, the gateway sends the GRQ to the current gatekeeper.

If the current state of the altGKisPermanent flag is TRUE, then the next RAS message is sent to the new gatekeeper. Otherwise, the next RAS message is sent to the original gatekeeper.

If the gateway exhausts the list of alternate gatekeepers without receiving any response from an alternate gatekeeper, the gateway returns to the GRQ phase.

For more information regarding the Cisco ecosystem gatekeeper interoperability feature, see the "Alternate Gatekeepers" section in the "Configuring H.323 Gateways and Proxies" chapter.

H.323 Restrictions

The following sections contain the restrictions that apply to the Cisco H.323-compliant features:

H.323 Version 2 Feature Restrictions

The following restrictions apply to the Cisco H.323 Version 2 features:

- All systems must be running either Cisco IOS Release 11.3(9)NA and later releases or Cisco IOS Release 12.0(3)T and later releases to interoperate with the Cisco H.323 Version 2 features. Earlier releases contain H.323 Version 1 software that does not support protocol messages that have an H.323 Version 2 protocol identifier. The earlier releases will not interoperate with Cisco H.323 Version 2 Phase 2 features.
- To use H.450 services (call transfer or call deflection), use Cisco IOS Release 12.1(1)T of the gatekeeper: H.450 on the gateways is incompatible with previous releases of the Cisco gatekeeper.
- If a Cisco AS5300 universal access server is used, the software requires the appropriate version of VCWare.
- The H.323 Version 2 fast connect feature is not explicitly configurable. It is assumed that the gateway is capable of sending and receiving fast connect procedures unless its corresponding dial peer has been configured for RSVP (in other words, the req-qos is set to a value other than the default of best-effort). If the dial peer has been configured for RSVP, traditional “slow” connect procedures will be followed, and the endpoint will neither attempt to initiate fast connect nor respond to a fast connect request from its peer.

H.323 Signaling Enhancement Feature Restrictions

The following restrictions apply to the H.323 signaling enhancement feature:

- Supplementary voice services are not supported with ISDN and CAS over an H.323 network—except on the NET5 switch.
- Progress messages require a PI value, and only ITU-T standards are supported.
- Progress indicator 2 is not supported in progress messages for the DMS100 switch.
- TCL 2.0 for IVR supports the interworking signaling enhancements only on the Cisco AS5300. For IVR on other Cisco platforms, select TCL 1.0 as the session application. To use standard IVR applications with TCL 1.0, configure the application name as “session.t.old” by using the **call application voice** global configuration command. It is not necessary to do this if customized scripts are used.

- The Cisco AS5300 universal access server sends a connect message to the originating gateway after it receives a setup message only when it is configured for one of the following supported switch types:
  - 5ESS
  - NET5
  - NTT
  - QSIG
  - QSIGP
- For the SS7 interconnect for voice gateways solution, the following behavior applies to suspend and resume messages, which are supported on NET5 and NI2+ ISDN interfaces:
  - If the ISDN interface is NET5, the Cisco AS5300 sends a notify message with the notification indicator (NI) set to user-suspended or user-resumed.
  - If the ISDN interface is NI2+, the Cisco AS5300 sends a suspend or resume message to the Cisco SC2200.
  - If the Cisco SC2200 receives an ISUP suspend or resume message, it sends an NI2+ suspend or resume message to the Cisco AS5300.
  - Both the Cisco AS5300 and SC2200 timers start when a suspend message is received. The Cisco AS5300 timer, T307, is configurable from 30 to 300 seconds. The Cisco SC2200 timer, T6, is not configurable and has a default of 120 seconds if the ISUP variant Q.761 is used.

    When the Cisco AS5300 and the SC2200 receive a resume message, the timers are stopped. If either of the the timers expires, the call is released with a cause code of normal clearing.

Configurable Timers in H.225.0 Restriction

This feature is limited to H.323 dial peers.

Source Call Signal Address and H.245 Empty Capabilities Set Restrictions

The following restrictions apply to source call signal address and H.245 empty capabilities set:

- To use H.450 services (call transfer or call deflection), Cisco IOS Release 12.1(2)T of the gatekeeper must be used. H.450 on the gateways is incompatible with previous releases of the Cisco gatekeeper.
- If a Cisco AS5300 universal access server is used, the system requires the appropriate version of VCWare.

Ecosystem Gatekeeper Interoperability Restrictions

The following restrictions apply to ecosystem gatekeeper interoperability:

- The maximum number of alternate gatekeepers is eight (including static gatekeepers).
- During the retransmission of the GRQ or RRQ messages, the gateway responds only to the current gatekeeper (regardless of the state of the altGKisPermanent flag).
- The process of retransmission to an alternate gatekeeper can be time-consuming.

H.323 Prerequisite Tasks

To use the Cisco H.323 signaling enhancements, first do the following:

- Establish a working IP network. For more information about configuring IP, refer to the *Cisco IOS IP Configuration Guide*.
- Install the appropriate voice network module and voice interface card for the Cisco router. For more information about the physical characteristics of the voice network module or on how to install it, refer to the *Voice Network Module and Voice Interface Card Configuration Note* that came with the voice network module.
- Configure your H.323 gateways, gatekeepers, and proxies. For more information about configuring VoIP for your access platform, see the "Configuring H.323 Gateways," "Configuring H.323 Gatekeepers and Proxies," and "Voice over IP Overview" chapters in this configuration guide.
- To ensure network security, configure a RADIUS authentication, authorization, and accounting (AAA) server.

  In addition to the configuration, make sure that the following information is configured in your CiscoSecure AAA server:

  In the /etc/raddb/clients file, ensure that the following information is provided:

```
#Client Name            Key
#-----------       ------------------
gk215.cisco.com         testing123
```

  Where:

  gk215.cisco.com is resolved to the IP address of the gatekeeper requesting authentication

  In the /etc/raddb/users file, ensure that the following information is provided:

```
taeduk@cisco.com  Password = "thiswouldbethepassword"
User-Service-Type = Framed-User,
Login-Service = Telnet
```

  Where:

  taeduk@cisco.com is the h323-id of the gateway authenticating to gatekeeper gk215.cisco.com.
- Configure an NTP server for your network.

Additional requirements and tasks for the individual features follow:

- The configurable timers in the H.225.0 feature require the Cisco H.323 VoIP Gateway for Cisco Access Platforms feature.
- Answer supervision reporting requires a Cisco H.323 gatekeeper.
- Gateway-to-gatekeeper billing redundancy requires a Cisco H.323 gatekeeper and the Gateway Support for Alternate Gatekeepers feature.
- Ecosystem gatekeeper interoperability requires a Cisco H.323 gatekeeper.
- For H.323 Version 2 features, configure an NTP server for the network.

H.323 Configuration Task List

To configure the H.323 features in this chapter, perform the tasks described in the following sections:

Configuring Timers in H.225.0

To use the configurable timers in H.225.0, first create an H.323 voice class and then specify the timeout value associated with that class. To configure the H.225.0 TCP timeout value, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 4	`Router(config)# voice class h323 number`	Enters voice class mode to create or modify an H.323 voice class. The *number* argument identifies the H.323 voice class. There is no default value.
Step 5	`Router(voice-class)# h225 timeout tcp establish value`	Sets the H.225.0 TCP timeout value for the specified voice class. The *value* argument indicates the timeout value, in seconds. There is no default value.
Step 6	`Router(voice-class)# exit`	Exits voice class mode.

Next, associate the H.323 voice class with each VoIP dial peer that should use the specified timeout. To associate the H.323 voice class with a dial peer, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# dial-peer voice tag voip`	Enters dial-peer configuration mode and defines a remote VoIP dial peer. The keywords and arguments are as follows: • The *tag* argument is one or more digits identifying the dial peer.Valid entries are from 1 to 2,147,483,647. • The **voip** keyword indicates a VoIP peer using voice encapsulation on the IP network.
Step 2	`Router(config-dial-peer)# voice-class h323 number`	Associates the specified H.323 voice class (and all of its related attributes) with the dial peer. The *number* argument identifies the H.323 voice class. There are no default values.

Verifying the H.225.0 TCP Timeout Value

To verify that the timeout value is defined for a dial peer, enter the **show running-config** command. The output shows the current configuration of the voice class and the dial peer.

```
Router# show running-config

Building configuration...

Current configuration:
!
voice class h323 1
 h225 timeout tcp etablish 10

dial-peer voice 919 voip
 application session
 destination-pattern 919555....
 voice-class codec 1
 voice-class h323 1
 session target ras
```

Configuring H.245 Tunneling of DTMF Relay in Conjunction with Fast Connect

The **dtmf-relay** command configured on the outgoing VoIP dial peer initiates H.245 tunneling procedures from a fast connect call. Note that H.245 tunneling will be activated only if the **dtmf-relay**, **h245-alphanumeric**, or **h245-signal** (but *not* **cisco-rtp**) commands are configured on the VoIP dial peer.

Configuring H.450

A Cisco gateway for H.450 is configured in one of the following ways, depending on what the gateway needs to do:

- By redirecting an unanswered call (call deflection).
- By transferring an answered call to a new DN (call transfer without consultation).

Although there are no new CLI commands for configuring H.450 services, the services are enabled only when a TCL/IVR Session Application is configured. Therefore, to use H.450 services, you must configure a TCL/IVR-based "application" on each applicable incoming dial peer for each Cisco gateway that will be involved in call transfer or call deflection. If no special TCL/IVR behavior is required, you can use the standard TCL/IVR application "session." This is not to be confused with application "SESSION," which is not TCL/IVR-based and does not support H.450 services.

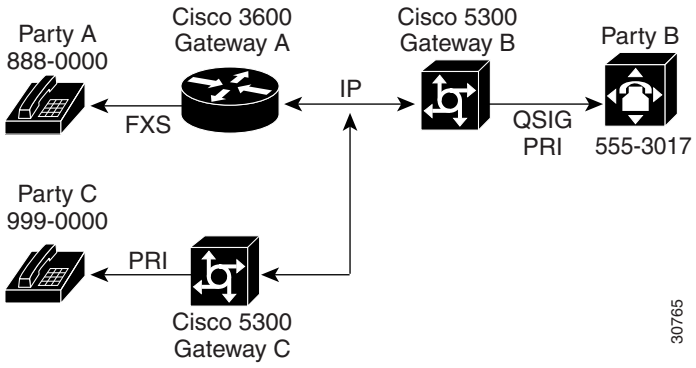
In addition, if call deflection is to be initiated from a QSIG PRI, you must configure the PRI using the **isdn switch-type primary-qsig** and **isdn alert end-to-end** commands.

Note For general information on configuring dial peer application and the meaning of incoming dial peer, refer to *Voice over IP for the Cisco AS5300*.

Configuring Call Deflection

A sample call deflection configuration is shown in Figure 53.

Figure 53 H.450 Configuration to Redirect Unanswered Calls



In this example, three gateways are configured to redirect unanswered calls, so that when Party A calls Party B, Party B can invoke deflection to pass the call to Party C. For this to work, "application session" or another TCL/IVR-based application must be configured on each applicable incoming dial peer as follows:

- On Gateway A, the POTS dial peer for destination pattern 8880000.
- On Gateway B, the VoIP dial peer for destination pattern 8880000.
- On Gateway C, the VoIP dial peer for destination pattern 8880000.

To configure the Gateway A POTS dial peer, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# dial-peer voice` *tag* `pots`	Enters dial-peer configuration mode. The *tag* argument is a digit that defines a particular dial peer. Valid entries are from 1 to 2,147,483,647.
Step 2	`Router(dial-peer)# application` *name*	Specifies the application that will be invoked for this dial peer. Only TCL-based applications are able to support H.450 services. The *name* argument indicates the name of the predefined TCL/IVR application. Incoming calls using this POTS dial peer will be handed off to this application.

Command	Purpose
Step 3 `Router(dial-peer)# destination-pattern [+]string[T]`	Specifies either the prefix or the full E.164 telephone number (depending on the dial plan) to be used for a dial peer. The keywords and arguments are as follows: • [+]—(Optional) Specifies a character indicating an E.164 standard number. The plus sign (+) is not supported on the Cisco MC3810 multiservice concentrator. • *string*—Specifies a series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: – The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. – Comma (,)—Inserts a pause between digits. – Period (.)—Matches any entered digit (this character is used as a wildcard). – Percent sign (%)—Indicates that the previous digit/pattern occurred zero or multiple times, similar to the wildcard usage in the regular expression. – Plus sign (+)—Matches a sequence of one or more matches of the character/pattern. **Note** The plus sign used as part of the digit string is different from the plus sign that can be used in front of the digit string to indicate that the string is an E.164 standard number. – Circumflex (^)—Indicates a match to the beginning of the string. – Dollar sign ($)—Matches the null string at the end of the input string. – Backslash symbol (\)—Is followed by a single character matching that character or used with a single character having no other significance (matching that character). – Question mark (?)— Indicates that the previous digit occurred zero or one time. – Brackets ([])—Indicates a range of digits. A range is a sequence of characters enclosed in the brackets, and only numeric characters from “0” to “9” are allowed in the range. This is similar to a regular expression rule.

	Command	Purpose
		– Parentheses (())—Indicate a pattern and is the same as the regular expression rule—for example, 408(555). Parentheses are used in conjunction with symbols ?, %, or +. For more information on applying wildcard symbols to destination patterns and the dial strings that result, see the "Configuring Dial Plans, Dial Peers, and Digit Manipulation" chapter. • **T**—(Optional) Control character indicating that the **destination-pattern** value is a variable-length dial string.
Step 4	`Router(dial-peer)# exit`	Exits dial-peer configuration mode.
Step 5	**2600 and 3600 Series Routers** `Router(config)# port {slot-number/subunit-number/port} | {slot/port:ds0-group-no}`	Specifies the voice slot number, subunit number, and port through which incoming VoIP calls will be received. The keywords and arguments are as follows: • *slot-number*—Specifies the slot number in the Cisco router in which the voice interface card is installed. Valid entries are from 0 to 3, depending on the slot in which it has been installed. • *subunit-number*—Specifies the subunit on the voice interface card in which the voice port is located. Valid entries are 0 or 1. • *port*—Specifies the voice interface card location. Valid entries are 0 or 3. • *slot*—Specifies the router location in which the voice port adapter is installed. Valid entries are from 0 to 3. • *port*—Specifies the voice interface card location. Valid entries are 0 or 3. • *ds0-group-no*—Indicates the defined DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows individual DS0s to be defined on the digital T1/E1 card. **Note** The slashes must be entered along with the arguments shown within the braces in the Command column.

To configure the VoIP dial peers on Gateways B and C, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# dial-peer voice number voip`	Enters dial-peer configuration mode. The *number* argument defines a particular dial peer. Valid entries are 1 to 2,147,483,647.
Step 2	`Router(dial-peer)# application name`	Specifies the application that will be invoked for this dial peer. Only Tool Command Language- (TCL-) based applications are able to support H.450 services. The *name* argument indicates the name of the predefined TCL/IVR application. Incoming calls using this VoIP dial peer will be handed off to this application.
Step 3	`Router(dial-peer)# destination-pattern [+]string[T]`	Specifies either the prefix or the full E.164 telephone number (depending on the dial plan) to be used for a dial peer. For a description of the keywords and arguments for this command, see Step 3 in the first configuration task table (showing how to configure the Gateway A POTS dial peer) in the "Configuring Call Deflection" section on page 240.

	Command	Purpose
Step 4	**2600 and 3600 Series VoIP Dial Peers** `Router(dial-peer)#` **`session target`** {**`ipv4:`***`destination-address`* | **`dns:`**[**`$s$.`** | **`$d$.`** | **`$e$.`** | **`$u$.`**]*`host-name`* | **`loopback:rtp`** | **`loopback:compressed`** | **`loopback:uncompressed`**}	Specifies the network-specific address for a specified dial peer. The keywords and arguments are as follows: • **ipv4:***destination-address*—Specifies the IP address of the dial peer. • **dns:***host-name*—Indicates that the Domain Name System (DNS) will be used to resolve the name of the IP address. Valid entries for this parameter are characters that represent the name of the host device. One of the following four optional wildcards can be used with this keyword when defining the session target for VoIP peers: – **s**—Indicates that the source destination pattern will be used as part of the domain name. – **d**—Indicates that the destination number will be used as part of the domain name. – **e**—Indicates that the digits in the called number will be reversed, that periods will be added in between each digit of the called number, and that this string will be used as part of the domain name. – **u**—Indicates that the unmatched portion of the destination pattern (such as a defined extension number) will be used as part of the domain name.
		• loopback:rtp—Indicates that all voice data will be looped back to the originating source. This is applicable for VoIP peers. • loopback:compressed—Indicates that all voice data will be looped back in compressed mode to the originating source. This is applicable for POTS peers. – **loopback:uncompressed**—Indicates that all voice data will be looped back in uncompressed mode to the originating source. This is applicable for POTS peers.

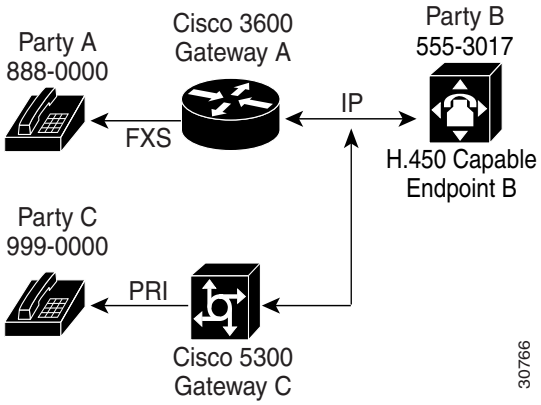
To configure the Gateway B PRI, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	**Cisco 4000 Series Access Servers** `Router(config)# interface serial number:timeslot`	Configures the serial interface. The keywords and arguments are as follows: • *number*—Channelized E1 or T1 controller number. • *time-slot*—For ISDN, the D channel time slot, which is the :23 channel for channelized T1 and the :15 channel for channelized E1. PRI time slots are in the range of 0 to 23 for channelized T1 and in the range of 0 to 30 for channelized E1. – For channel-associated signaling or robbed-bit signaling, *time-slot* is the channel group number. – The colon (:) is required. – On a dual port card, it is possible to run channelized on one port and PRI on the other port.
Step 2	`Router(config-if)# isdn switch-type switch-type`	Configures the ISDN interface as a primary QSIG interface. The *switch-type* argument is the service provider switch type. PRI switch types vary by geographic area. (Refer to the command reference master index, or search online for this information.)

Configuring Call Transfer Without Consultation

A sample configuration is shown in Figure 54.

Figure 54 H.450 Configuration for Calls Transfer Without Consultation



In this example, two gateways are configured to handle call transfers without consultation, so that when Party A calls Party B at 555-3017 at Endpoint B, Endpoint B answers and then invokes call transfer to Party C. To do this, configure the application session or another TCL/IVR-based application on each applicable incoming dial peer as follows:

- On Gateway A, the POTS dial peer for destination pattern 8880000.
- On Gateway C, the VoIP dial peer for destination pattern 8880000.

To configure the Gateway A POTS dial peer, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# dial-peer voice` *tag* `pots`	Enters dial-peer configuration mode. The *tag* argument is a digit that defines a particular dial peer. Valid entries are from 1 to 2,147,483,647.
Step 2	`Router(dial-peer)# application` *name*	Specifies the application that will be invoked for this dial peer. Only Tool Command Language- (TCL-) based applications are able to support H.450 services. The *name* argument indicates the name of the predefined TCL/IVR application. Incoming calls using this POTS dial peer will be handed off to this application.
Step 3	`Router(dial-peer)# destination-pattern [+]`*string*`[T]`	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer (depending on the dial plan) . For a description of the keywords and arguments for this command, see Step 3 in the first configuration task table (showing how to configure the Gateway A POTS dial peer) in the "Configuring Call Deflection" section on page 240.

	Command	Purpose
Step 4	**2600 and 3600 Series POTS Dial Peers** `Router(dial-peer)# session target`	Specifies the IP address of the destination gateway for "outbound" dial peers. Because this is an "incoming" dial peer, the session target is not applicable, so the IP address is ignored.
Step 5	`Router (dial-peer)# port {slot-number/subunit-number/port} | {slot/port:ds0-group-no}`	Specifies the voice slot number, subunit number, and port through which incoming VoIP calls will be received. For a description of the keywords and arguments for this command, see Step 5 in the first configuration task table (showing how to configure the Gateway A POTS dial peer) in the "Configuring Call Deflection" section on page 240.
Step 6	`Router(dial-peer)# exit`	Exits dial-peer configuration mode.

To configure the Gateway C VoIP dial peer, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# dial-peer voice tag voip`	Enters dial-peer configuration mode. The *tag* argument is a digit that defines a particular dial peer. Valid entries are from 1 to 2,147,483,647.
Step 2	`Router(dial-peer)# application name`	Specifies the application that will be invoked for this dial peer. Only Tool Command Language- (TCL-) based applications are able to support H.450 services. The *name* argument indicates the name of the predefined TCL/IVR application. Incoming calls using this VoIP dial peer will be handed off to this application.
Step 3	`Router(dial-peer)# destination-pattern [+]string[T]`	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer (depending on the dial plan) . For a description of the keywords and arguments for this command, see Step 3 in the first configuration task table (showing how to configure the Gateway A POTS dial peer) in the "Configuring Call Deflection" section on page 240.
Step 4	**2600 and 3600 Series VoIP Dial Peers** `Router(dial-peer)# session target {ipv4:destination address | dns: [$s$. | $d$. | $e$.| $u$.]host-name | loopback:rtp | loopback:compressed | loopback:uncompressed}`	Specifies the network-specific address for a specified dial peer. For a description of the keywords and arguments for this command, see Step 4 in the second configuration task table (showing how to configure the VoIP dial peers on Gateways B and C) in the "Configuring Call Deflection" section on page 240.

For more information about POTS dial peers, refer to the Cisco IOS Release 12.0 *Voice, Video, and Home Applications Configuration Guide* or see the "Configuring Dial Plans, Dial Peers, and Digit Manipulation" chapter in this configuration guide.

For more information about any of the commands used to configure VoIP dial peers, refer to the *Cisco IOS Voice, Video, and Fax Command Reference*; the *Cisco IOS Voice, Video, and Home Applications Command Reference*; or see the "Configuring Voice Ports" or the "Configuring Voice over IP" chapters in this configuration guide.

Configuring Voice-Port Descriptions

The voice-port description feature uses the existing **description** subcommand for the voice port. When the voice-port description is being configured, the exact contents of the description field are included in the ARQ message sent from the ingress gateway.

Note Configuring the voice-port description has no effect for calls that are not configured to use RAS.

To configure the description on a voice port, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	**2600 and 3600 Series Routers** `Router(config)# voice-port {slot-number/subunit-number/port} | {slot/port:ds0-group-no}`	Enters voice-port configuration mode for the specified voice port. The arguments are as follows: • *slot-number*—Specifies the slot number in the Cisco router in which the voice interface card (VIC) is installed. Valid entries are from 0 to 3, depending on the slot in which it has been installed. • *subunit-number*—Specifies the subunit on the VIC in which the voice port is located. Valid entries are 0 or 1. • *port*—Specifies the voice port number. Valid entries are 0 or 1. • *slot*—Specifies the router location in which the voice port adapter is installed. Valid entries are from 0 to 3. • *port*—Indicates the voice interface card location. Valid entries are 0 or 3. • *dso-group-no*—Indicates the defines DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.
Step 2	`Router(config-voiceport)# description string`	Defines the description associated with the voice port. The *string* argument is a character string from 1 to 80 characters.