CIPT1

Cisco Voice over IP

Volume 3

Version 6.0

Student Guide

Editorial, Production, and Web Services: 02.15.08

cisco.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED “AS IS.” CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

Table of Contents

Volume 3

Module 5

H.323 Gatekeepers

Overview

Gatekeepers are a major part of medium to large H.323 VoIP network solutions. When used, these components allow for dial-plan scalability and reduce the need to manage global dial plans locally. In this module, you will learn the functions of a gatekeeper and directory gatekeeper. Additionally, you will learn how to configure gatekeepers to interoperate with gateways and how to provide gatekeeper redundancy in medium to large VoIP networks.

Module Objectives

Upon completing this module, you will be able to implement gatekeepers and directory gatekeepers, and identify redundancy options for gatekeepers. This ability includes being able to meet these objectives:

- Describe Cisco gatekeeper functionality
- Configure gatekeepers for device registration, address resolution, and call routing
- Implement gatekeeper-based Call Admission Control (CAC)

Lesson 1

Introducing Gatekeepers

Overview

This lesson reviews the functions and roles of gatekeepers and directory gatekeepers and the protocol used between gateways and gatekeepers. This lesson discusses in depth the Registration, Admission, and Status (RAS) signaling sequencing between gateways and gatekeepers, and discusses the use of the Gatekeeper Transaction Message Protocol (GKTMP).

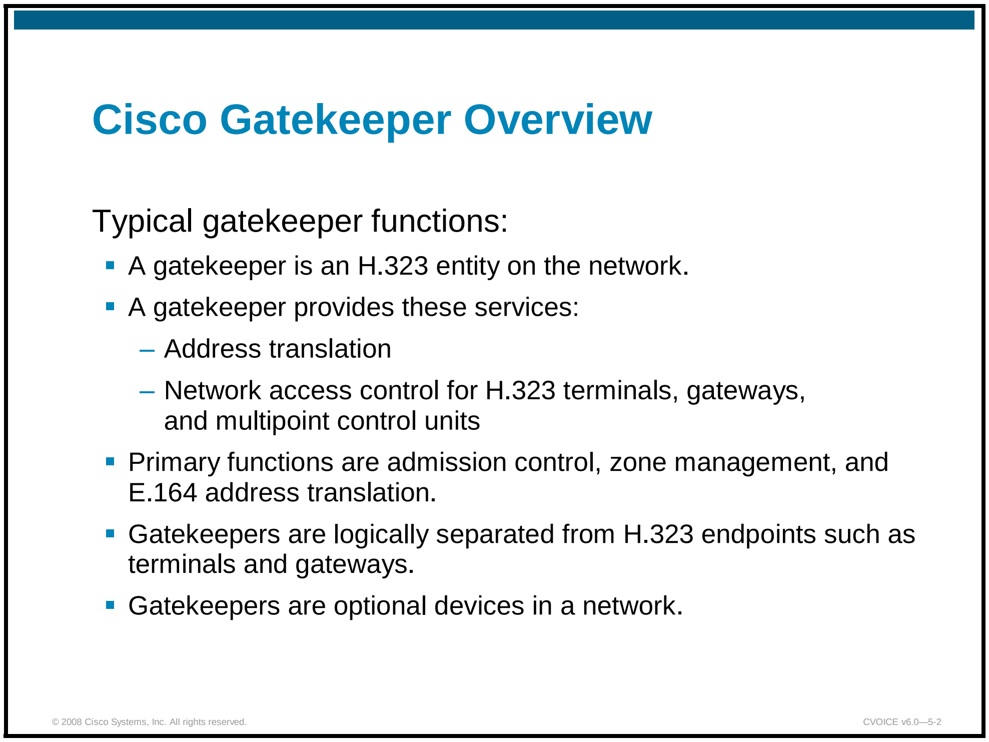
Objectives

Upon completing this lesson, you will be able to describe Cisco gatekeeper functionality. This ability includes being able to meet these objectives:

- Describe the functionality of gatekeepers in an H.323 environment
- Define the hardware and software requirements for gatekeeper functionality
- Describe the signaling between gateways and gatekeepers
- Describe how directory gatekeepers enhance the scalability of a network
- Describe how gatekeeper zone prefixes are used for call routing
- Describe how gatekeeper technology prefixes are used for call routing
- Describe how gatekeepers perform address resolution and call routing in different scenarios
- Describe how GKTMP works
- Describe some commands that are used to verify H.323 gatekeeper operation

Gatekeeper Overview

This topic describes the functionality of gatekeepers in an H.323 environment.



Cisco Gatekeeper Overview

Typical gatekeeper functions:

- A gatekeeper is an H.323 entity on the network.
- A gatekeeper provides these services:
  - Address translation
  - Network access control for H.323 terminals, gateways, and multipoint control units
- Primary functions are admission control, zone management, and E.164 address translation.
- Gatekeepers are logically separated from H.323 endpoints such as terminals and gateways.
- Gatekeepers are optional devices in a network.

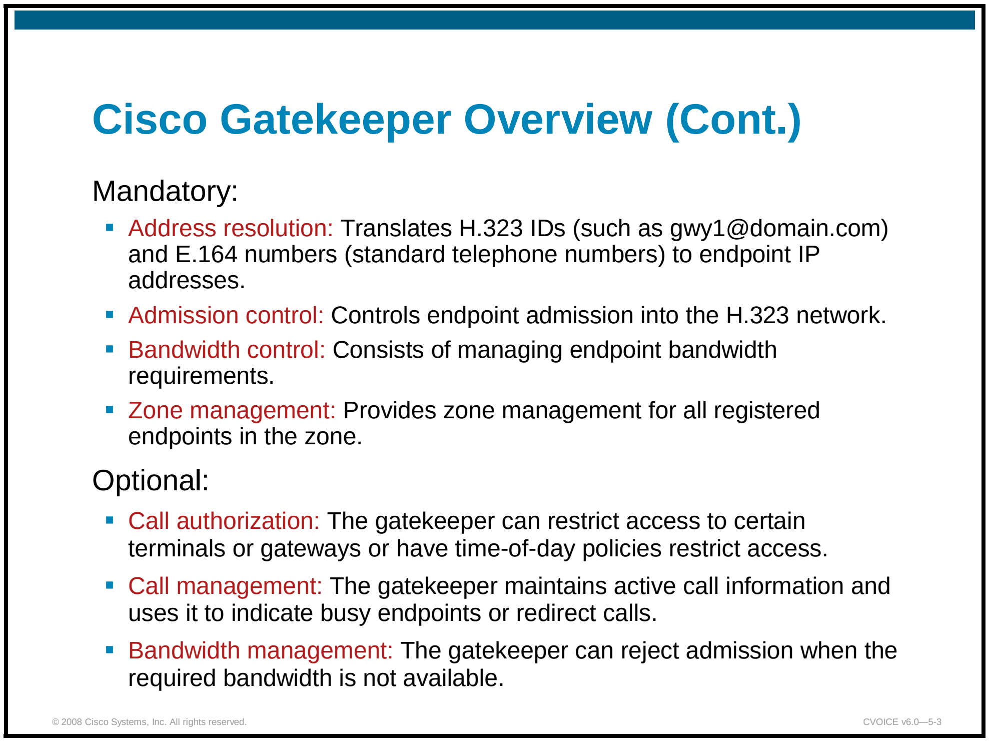
© 2008 Cisco Systems, Inc. All rights reserved.

CVOICE v6.0—5-2

A gatekeeper is an H.323 entity on the network that provides services such as address translation and network access control for H.323 terminals, gateways, and multipoint control units. The primary functions of a gatekeeper are admission control, zone management, and E.164 address translation. Gatekeepers are logically separated from H.323 endpoints and optional devices in an H.323 network environment.

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

Note	The ITU-T specifies that although a gatekeeper is an optional device in H.323 networks, if a network does include a gatekeeper, all H.323 endpoints should use it.



Cisco Gatekeeper Overview (Cont.)

Mandatory:

- Address resolution: Translates H.323 IDs (such as gwy1@domain.com) and E.164 numbers (standard telephone numbers) to endpoint IP addresses.
- Admission control: Controls endpoint admission into the H.323 network.
- Bandwidth control: Consists of managing endpoint bandwidth requirements.
- Zone management: Provides zone management for all registered endpoints in the zone.

Optional:

- Call authorization: The gatekeeper can restrict access to certain terminals or gateways or have time-of-day policies restrict access.
- Call management: The gatekeeper maintains active call information and uses it to indicate busy endpoints or redirect calls.
- Bandwidth management: The gatekeeper can reject admission when the required bandwidth is not available.

CVOICE v6.0—5-3

Gatekeepers have mandatory and optional responsibilities.

The mandatory responsibilities are these tasks, which occur simply because the device is in the network and has been configured:

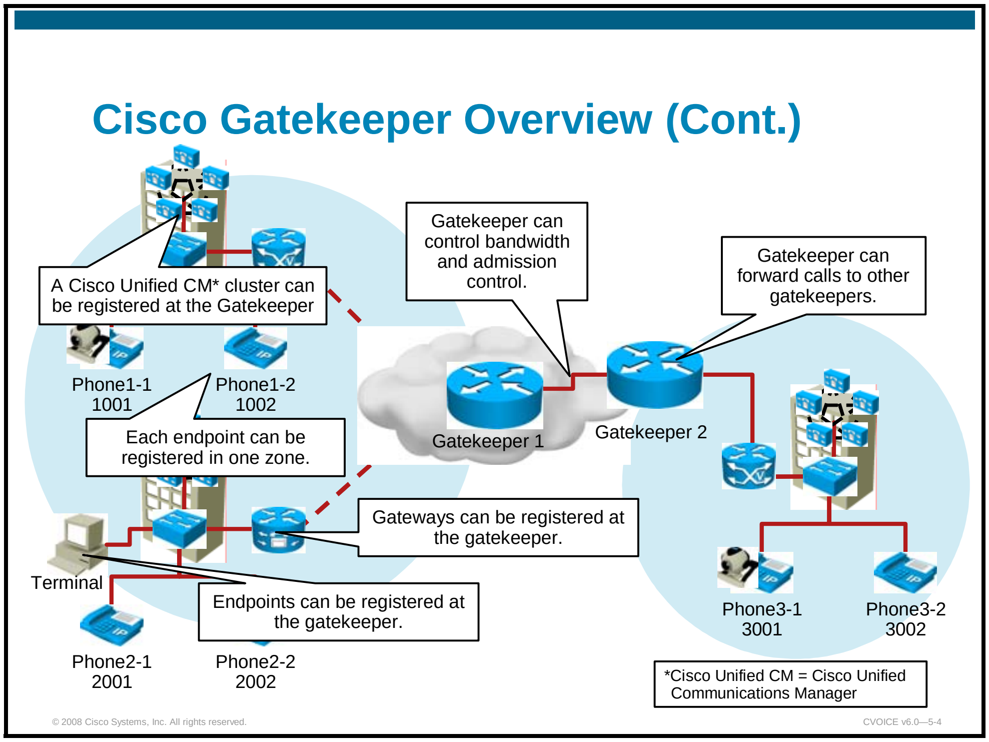
- **Address resolution:** Calls originating within an H.323 network may use an alias to address the destination terminal. Calls originating outside the H.323 network and received by a gateway may use an E.164 telephone number to address the destination terminal. The gatekeeper must be able to resolve the alias or the E.164 telephone number into the network address for the destination terminal. The destination endpoint can be reached using the network address on the H.323 network. The translation is done using a translation table that is updated with registration messages.
- **Admission control:** The gatekeeper can control the admission of the endpoints into the H.323 network. It uses these RAS messages to achieve this: Admission Request (ARQ), Admission Confirmation (ACF), and Admission Reject (ARJ). Admissions control may also be a null function that admits all requests.
- **Bandwidth control:** The gatekeeper manages endpoint bandwidth requirements. When registering with a gatekeeper, an endpoint will specify its preferred codec. During H.245 negotiation, a different codec may be required. These RAS messages are used to control this codec negotiation: Bandwidth Request (BRQ), Bandwidth Confirmation (BCF), and Bandwidth Reject (BRJ).
- **Zone management:** A gatekeeper is required to provide address translation, admission control, and bandwidth control for terminals, gateways, and multipoint control units located within its zone of control.

All of these gatekeeper-required roles are configurable.

The following are optional responsibilities the gatekeeper can provide:

- **Call authorization:** With this option, the gatekeeper can restrict access to certain endpoints or gateways based on policies such as time-of-day.

- **Call management:** With this option, the gatekeeper maintains active call information and uses it to indicate busy endpoints or redirect calls.
- **Bandwidth management:** With this option, the gatekeeper can reject admission when the required bandwidth is not available.



Cisco Gatekeeper Overview (Cont.)

A Cisco Unified CM* cluster can be registered at the Gatekeeper

Gatekeeper can control bandwidth and admission control.

Gatekeeper can forward calls to other gatekeepers.

Each endpoint can be registered in one zone.

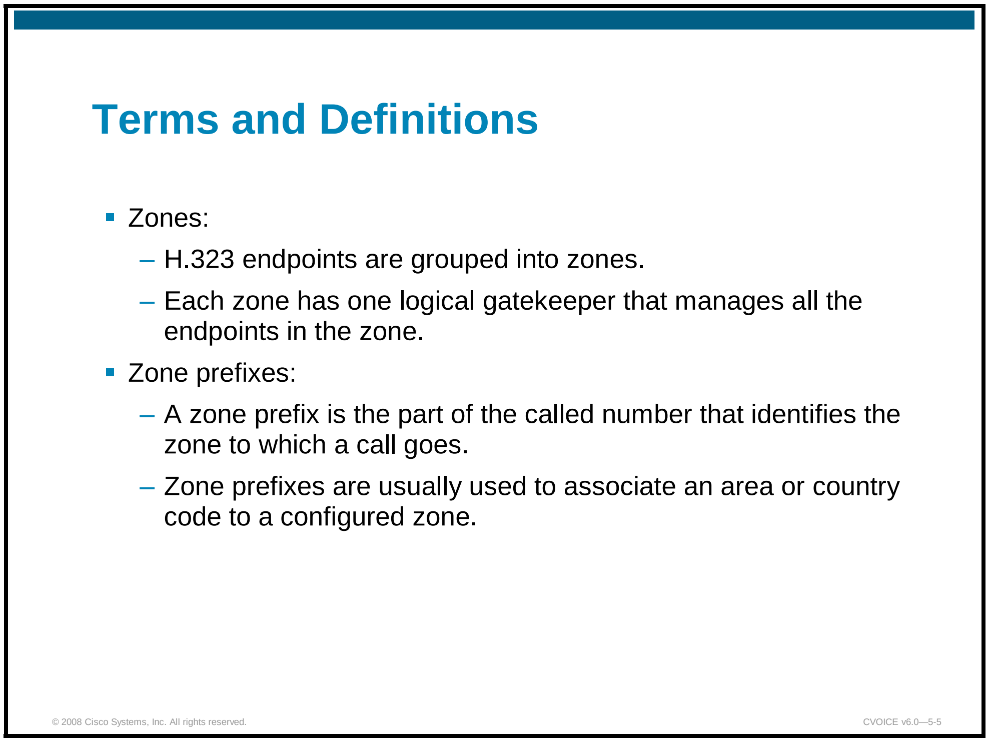
Gateways can be registered at the gatekeeper.

Endpoints can be registered at the gatekeeper.

*Cisco Unified CM = Cisco Unified Communications Manager

CVOICE v6.0—5-4

Endpoints attempt to register with a gatekeeper on startup. When they want to communicate with another endpoint, they request admission to initiate a call using a symbolic alias for the destination endpoint, such as an E.164 address or an e-mail address. If the gatekeeper determines 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. The Cisco gatekeeper provides H.323 call management, including admission control, bandwidth management, and routing services for calls in the network.



Terms and Definitions

- Zones:
  - H.323 endpoints are grouped into zones.
  - Each zone has one logical gatekeeper that manages all the endpoints in the zone.
- Zone prefixes:
  - A zone prefix is the part of the called number that identifies the zone to which a call goes.
  - Zone prefixes are usually used to associate an area or country code to a configured zone.

CVOICE v6.0—5-5

This figure describes the characteristic of zones and zone prefixes.

Zones

A zone is defined as the set of H.323 nodes controlled by a single logical gatekeeper. Gatekeepers that coexist on a network may be configured so that they register endpoints from different subnets. There can only be one active gatekeeper per zone. These zones can overlay subnets, and one gatekeeper can manage gateways in one or more of these subnets.

Endpoints attempt to discover a gatekeeper and consequently the zone of which they are members by using the RAS message protocol. The protocol supports a discovery message that may be sent multicast or unicast.

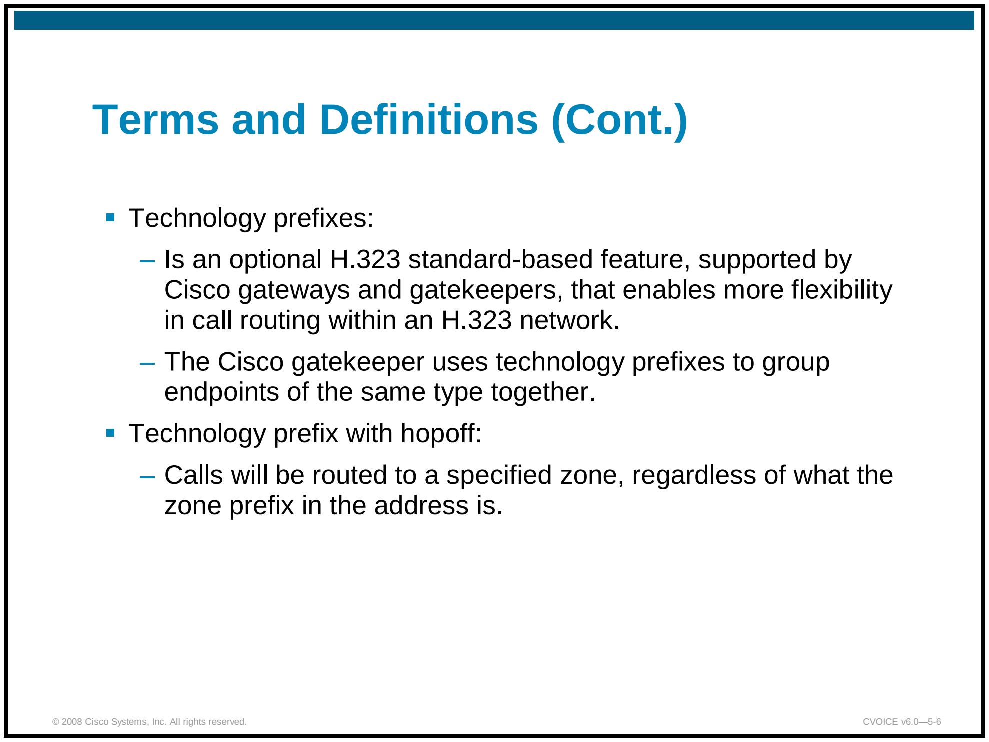
If the message is sent multicast, the endpoint registers nondeterministically with the first gatekeeper that responds to the message. To enforce predictable behavior, where endpoints on certain subnets are assigned to specific gatekeepers, the zone subnet command can be used to define the subnets that constitute a given gatekeeper zone. Any endpoint on a subnet that is not enabled for the gatekeeper is not accepted as a member of that gatekeeper zone. If the gatekeeper receives a discovery message from such an endpoint, it sends an explicit reject message.

Zone Prefixes

A zone prefix determines to which zone calls are sent. For a zone, which is controlled by a gatekeeper, the zone prefixes help route the call to the appropriate endpoint. The zone prefixes (typically area codes) serve the same purpose as the domain names in the H.323 ID (such as gwy1@domain.com) address space. For example, a local gatekeeper might be configured with the knowledge that zone prefix 212xxxxxxx (that is, any address beginning with 212 and followed by seven arbitrary digits) is handled by gatekeeper GK1, like this:

```
router(config-gk)# zone prefix GK1 212.......
```

Then when the local gatekeeper is asked to admit a call to destination address 2125551111, it knows to send the location request to GK1.



Terms and Definitions (Cont.)

- Technology prefixes:
  - Is an optional H.323 standard-based feature, supported by Cisco gateways and gatekeepers, that enables more flexibility in call routing within an H.323 network.
  - The Cisco gatekeeper uses technology prefixes to group endpoints of the same type together.
- Technology prefix with hopoff:
  - Calls will be routed to a specified zone, regardless of what the zone prefix in the address is.

This figure describes the characteristic of technology prefixes and tech-prefixes with the **hopoff** command.

Technology Prefixes

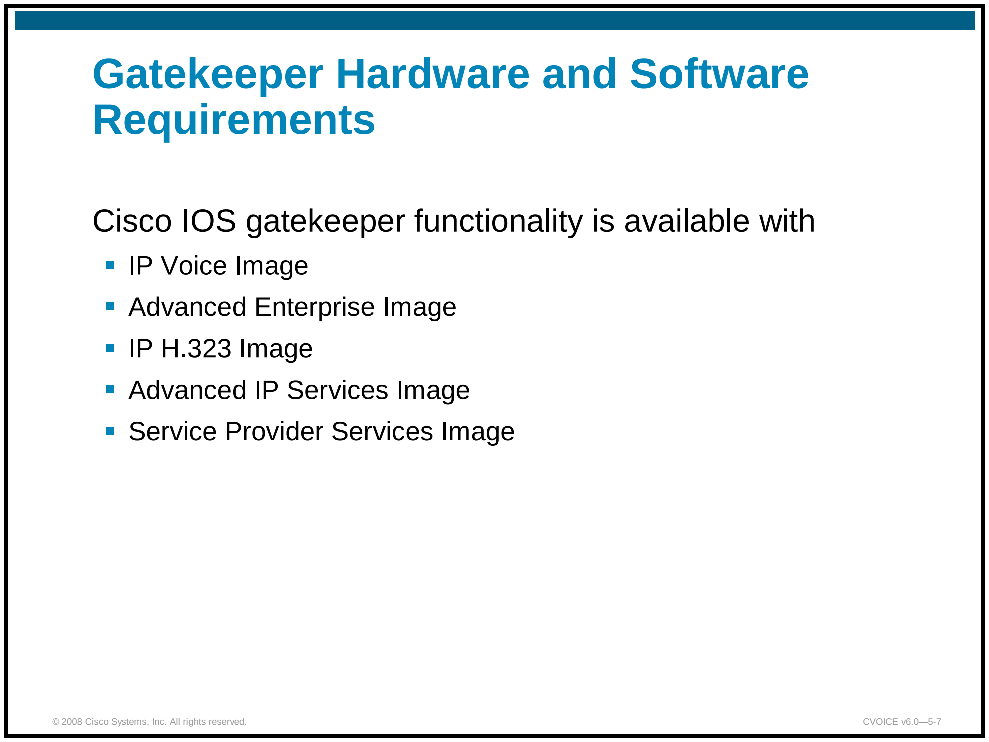
The network administrator selects technology prefixes to denote different types or classes of gateways. The gateways are then configured to register with their gatekeepers with these prefixes. For example, voice gateways might register with technology prefix 1#, H.320 gateways with 2#, voice-mail gateways with 3#, and so on. More than one gateway may register with the same type prefix. When that happens, the gatekeeper makes a random selection among gateways of the same type. The caller, who knows the type of device they are trying to reach, can now prepend a technology prefix to the destination address to indicate the type of gateway to use to get to the destination.

Technology Prefix with Hopoff

The other gateway-type feature is the ability to force a hopoff to a particular zone. Normally, when an endpoint or gateway makes a call admission request to its gatekeeper, the gatekeeper resolves the destination address by first looking for the technology prefix. When that is matched, the remaining string is compared against known zone prefixes. If the address resolves to a remote zone, the entire address, including both technology and zone prefixes, is sent to the remote gatekeeper in a Location Request (LRQ). That remote gatekeeper then uses the technology prefix to decide which of its gateways to hop off. The zone prefix determines the routing to a zone, and the technology prefix determines the gateway in that zone. This behavior can be overridden by associating a forced hopoff zone with a particular technology prefix. This forces the call to the specified zone, regardless of what the zone prefix is in the address.

Gatekeeper Hardware and Software Requirements

This topic defines the hardware and software required to support gatekeeper functionality.



Gatekeeper Hardware and Software Requirements

Cisco IOS gatekeeper functionality is available with

- IP Voice Image
- Advanced Enterprise Image
- IP H.323 Image
- Advanced IP Services Image
- Service Provider Services Image

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—5-7

To determine the latest Cisco IOS software version that is needed for the various router platforms, you will need to use the Feature Navigator tool to search for it. For example, you may want to search for which Cisco IOS version would be best to support a high-performance gatekeeper. You can find the platform and Cisco IOS version for the gatekeeper by using the Feature Navigator tool on Cisco.com at http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp. To start the search, follow these steps:

Step 1 Click the **Search by Feature** link.

Step 2 Select **High Performance Gatekeeper** in the **Available Features** list.

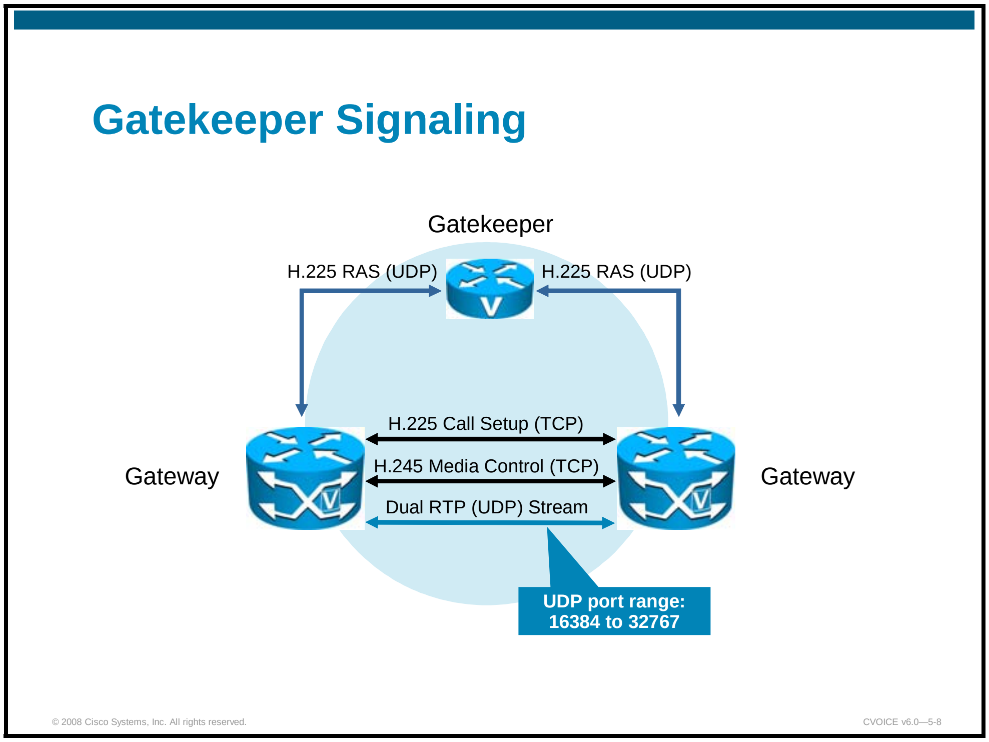
Step 3 Click the **Add** button to place the feature in the **Selected Features** box.

Step 4 Click the **Continue** button.

The Feature Navigator will return all the versions of Cisco IOS that support this feature. This includes General Deployment (GD), Limited Deployment (LD), and Early Deployment (ED) releases as well as the release numbers, platform types, feature sets, image names, and DRAM and Flash requirements.

Gatekeeper Signaling

This topic describes the signaling between gateways and gatekeepers.



Gatekeeper Signaling

CVOICE v6.0—5-8

Cisco gatekeepers use H.323 RAS, the Gatekeeper Update Protocol (GUP), and GKTMP as signaling methods when providing call services.

RAS is a subset of the H.225 signaling protocol. This signaling is based on User Data Protocol (UDP). Signaling messages between gateways are H.225 call control, setup, or signaling messages.

H.225 call control signaling is used to set up connections between H.323 endpoints. The ITU H.225 recommendation specifies the use and support of Q.931 signaling messages. If no gatekeeper is present, H.225 messages are exchanged directly between the endpoints.

After call signaling is set up between the gateways, H.245 is negotiated. H.245, a control signaling protocol in the H.323 multimedia communication architecture, is for the exchange of end-to-end H.245 messages between communicating H.323 endpoints. The H.245 control messages are carried over H.245 control channels. The H.245 control channel is the logical channel 0 and is permanently open, unlike the media channels. The messages carried include messages to exchange capabilities of terminals and to open and close logical channels.

After a connection has been set up via the call signaling procedure, the call cannot be established until the H.245 call control protocol is used to resolve the call media type and establish the media flow. The H.245 call control protocol also manages the call after it has been established.

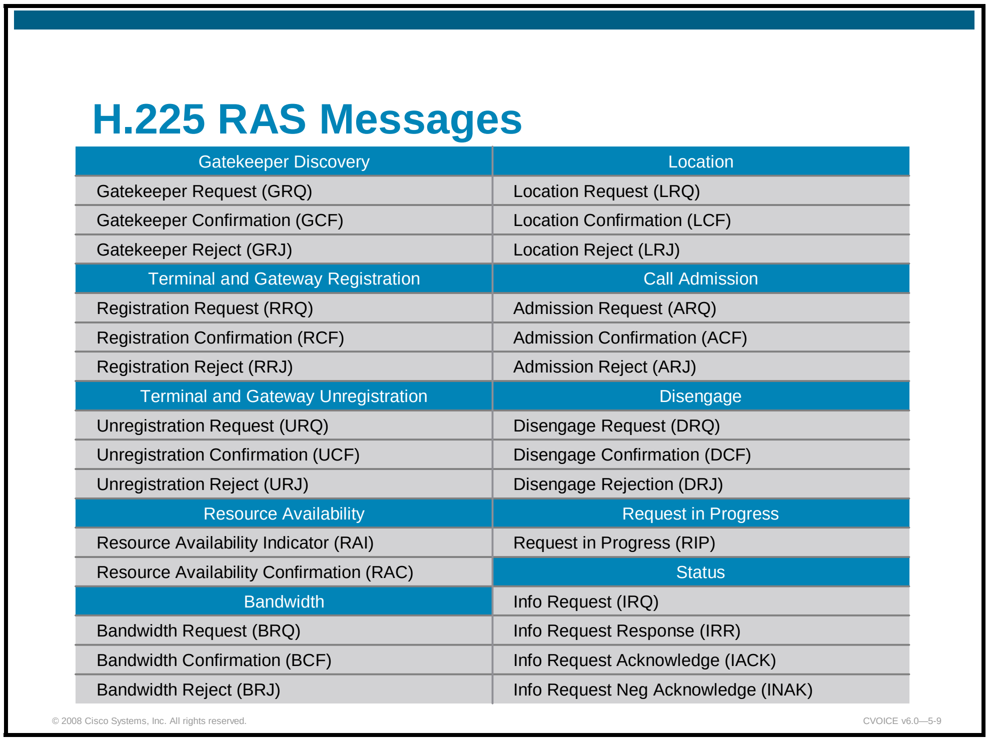
As the call is set up between gateways, all other port assignments are dynamically negotiated, as in these examples:

- Real-Time Transport Protocol (RTP) ports are negotiated from the lowest number.

- The H.245 TCP port is negotiated during H.225 signaling for a standard H.323 connection.
- The RTP UDP port range is 16384 to 32768.

RAS Messages

This subtopic describes RAS signal messages and how gatekeepers communicate through the RAS channel using different types of RAS messages.



H.225 RAS Messages

Gatekeeper Discovery	Location
Gatekeeper Request (GRQ)	Location Request (LRQ)
Gatekeeper Confirmation (GCF)	Location Confirmation (LCF)
Gatekeeper Reject (GRJ)	Location Reject (LRJ)
Terminal and Gateway Registration	Call Admission
Registration Request (RRQ)	Admission Request (ARQ)
Registration Confirmation (RCF)	Admission Confirmation (ACF)
Registration Reject (RRJ)	Admission Reject (ARJ)
Terminal and Gateway Unregistration	Disengage
Unregistration Request (URQ)	Disengage Request (DRQ)
Unregistration Confirmation (UCF)	Disengage Confirmation (DCF)
Unregistration Reject (URJ)	Disengage Rejection (DRJ)
Resource Availability	Request in Progress
Resource Availability Indicator (RAI)	Request in Progress (RIP)
Resource Availability Confirmation (RAC)	Status
Bandwidth	Info Request (IRQ)
Bandwidth Request (BRQ)	Info Request Response (IRR)
Bandwidth Confirmation (BCF)	Info Request Acknowledge (IACK)
Bandwidth Reject (BRJ)	Info Request Neg Acknowledge (INAK)

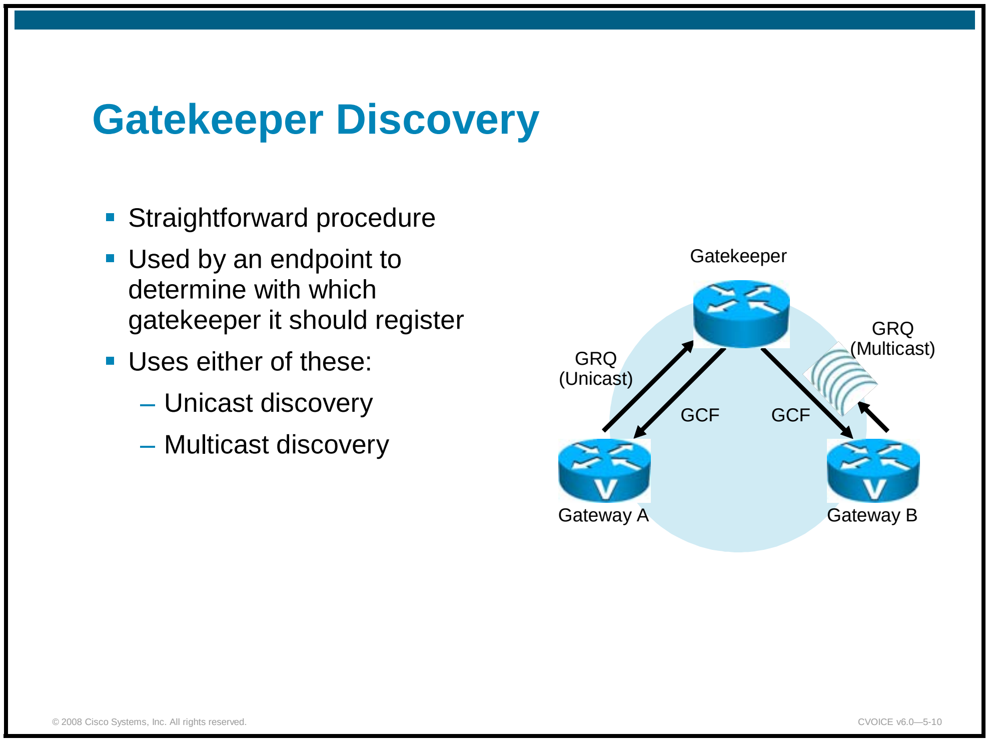
The figure shows common RAS signal messages, which are initiated by a gateway and gatekeeper. RAS message types include those listed here:

- **Gatekeeper discovery messages:** An endpoint multicasts a gatekeeper discovery request. The Gatekeeper Request (GRQ) message requests that any gatekeeper receiving it respond with a Gatekeeper Confirmation (GCF) message granting it permission to register. The Gatekeeper Reject (GRJ) message is a rejection of this request, indicating that the requesting endpoint should seek another gatekeeper.
  - **GRQ:** Message sent by an endpoint to a gatekeeper.
  - **GCF:** Reply from a gatekeeper to an endpoint indicating the transport address of the gatekeeper RAS channel.
  - **GRJ:** Reply from a gatekeeper to an endpoint rejecting the request from the endpoint for registration. The GRJ message usually occurs because of a gateway or gatekeeper configuration error.
- **Terminal and gateway registration messages:** The Registration Request (RRQ) message is a request to register from a terminal to a gatekeeper. If the gatekeeper responds with a Registration Confirmation (RCF) message, the terminal will use the responding gatekeeper for future calls. If the gatekeeper responds with a Registration Reject (RRJ) message, the terminal must seek another gatekeeper with which to register.
  - **RRQ:** Sent from an endpoint to a gatekeeper RAS channel address. Included in this message is the technology prefix, if configured.
  - **RCF:** Reply from the gatekeeper confirming endpoint registration.
  - **RRJ:** Reply from the gatekeeper rejecting endpoint registration.

- **Terminal and gateway unregistration messages:** The Unregistration Request (URQ) message requests that the association between a terminal and a gatekeeper be broken. Note that the URQ request is bidirectional, that is, a gatekeeper can request a terminal to consider itself unregistered, and a terminal can inform a gatekeeper that it is revoking a previous registration.
  - **URQ:** Sent from an endpoint or a gatekeeper to cancel registration.
  - **Unregistration Confirmation (UCF):** Sent from an endpoint or a gatekeeper to confirm an unregistration.
  - **Unregistration Reject (URJ):** Indicates that an endpoint was not preregistered with the gatekeeper.
- **Resource availability messages:** The Resource Availability Indication (RAI) message is a notification from a gateway to a gatekeeper of its current call capacity for each H-series protocol and data rate for that protocol. Upon receiving an RAI message, the gatekeeper responds with a Resource Availability Confirmation (RAC) message to acknowledge its reception.
  - **RAI:** Used by gateways to inform the gatekeeper whether resources are available in the gateway to take on additional calls.
  - **RAC:** Notification from the gatekeeper to the gateway acknowledging receipt of the RAI message.
- **Bandwidth messages:** An endpoint sends a bandwidth change request (BRQ) to its gatekeeper to request an adjustment in call bandwidth. The gatekeeper either grants the request with a BCF message or denies it with a BRJ message.
  - **BRQ:** Sent by the endpoint to the gatekeeper requesting an increase or decrease in call bandwidth.
  - **BCF:** Sent by the gatekeeper confirming acceptance of the bandwidth request.
  - **BRJ:** Sent by the gatekeeper rejecting the bandwidth request.
- **Location messages:** These are commonly used between interzone gatekeepers to get the IP addresses of different zone endpoints.
  - **LRQ:** Sent by a gatekeeper to the directory gatekeeper to request the contact information for one or more E.164 addresses. An LRQ is sent directly to a gatekeeper if one is known, or it is multicast to the gatekeeper discovery multicast address.
  - **Location Confirmation (LCF):** Sent by a responding gatekeeper and contains the call signaling channel or RAS channel address (IP address) of itself or the requested endpoint. It uses the requested endpoint address when directed endpoint call signaling is used.
  - **Location Reject (LRJ):** Sent by gatekeepers that received an LRQ for a requested endpoint that is not registered or that has unavailable resources.
- **Call admission messages:** The ARQ message requests that an endpoint be allowed access to the packet-based network by the gatekeeper. The request identifies the terminating endpoint and the bandwidth required. The gatekeeper either grants the request with an ACF message or denies it with an ARJ message.
  - **ARQ:** An attempt by an endpoint to initiate a call.

- **ACF:** An authorization by the gatekeeper to admit the call. This message contains the IP address of the terminating gateway or gatekeeper and enables the originating gateway to initiate call control signaling procedures.
- **ARJ:** Denies the request from the endpoint to gain access to the network for this particular call if the endpoint is unknown or inadequate bandwidth is available.

- **Disengage messages:** When a call is disconnected, the endpoint sends a disengage request (DRQ) to the gatekeeper. The gatekeeper confirms (disengage confirmation [DCF]) or rejects (disengage rejection [DRJ]) the request. If sent from an endpoint to a gatekeeper, the DRQ message informs the gatekeeper that an endpoint is being dropped. If sent from a gatekeeper to an endpoint, the DRQ message forces a call to be dropped—such a request will not be refused. The DRQ message is not sent directly between endpoints.
  - **DRQ:** Sent from the endpoint to a gatekeeper when a call is disconnected.
  - **DCF:** Confirms the disengage request sent by the endpoint.
  - **DRJ:** Rejects the disengage request sent by the gatekeeper.
- **Request in progress (RIP) message:** The gatekeeper sends out an RIP message to an endpoint or gateway to prevent call failures due to RAS message timeouts during gatekeeper call processing. A gateway receiving an RIP message knows to continue to wait for a gatekeeper response.
- **Status messages:** A gatekeeper uses an interrupt request (IRQ) to determine the status of an endpoint. In its information request (IRR), the endpoint indicates whether it is on line or off line. The endpoint may also reply that it understands the information request (information request acknowledge [IACK]) or that it does not understand the request (information request neg acknowledge [INAK]).
  - **IRQ:** Sent from a gatekeeper to an endpoint requesting status.
  - **ICF:** Sent from an endpoint to a gatekeeper to confirm the status.
  - **IRR:** Sent from an endpoint to a gatekeeper in response to an IRQ. This message is also sent from an endpoint to a gatekeeper if the gatekeeper requests periodic status updates. Gateways use the IRR to inform the gatekeeper about the active calls.
  - **IACK:** Used by the gatekeeper to respond to IRR messages.
  - **INACK:** Used by the gatekeeper to respond to IRR messages.



Gatekeeper Discovery

- Straightforward procedure
- Used by an endpoint to determine with which gatekeeper it should register
- Uses either of these:
  - Unicast discovery
  - Multicast discovery

CVOICE v6.0—5-10

Endpoints attempt to discover a gatekeeper and, consequently, the zone of which they are members by using the RAS message protocol. The protocol supports a discovery message that may be sent via multicast or unicast. The initial signaling from a gateway to a gatekeeper is done through H.225 RAS. Gateways can discover their gatekeepers through one of these two processes:

- **Unicast discovery**
  - Uses UDP port 1718.
  - In this process, endpoints are configured with the gatekeeper IP address and can attempt registration immediately.
  - The gatekeeper replies with a GCF or GRJ message.
- **Multicast discovery**
  - Uses UDP multicast address 224.0.1.41.
  - Auto discovery enables an endpoint to discover its gatekeeper through a multicast message. Because endpoints do not have to be statically configured for gatekeepers, this method has less administrative overhead.
  - A gatekeeper replies with a GCF message or GRJ message.

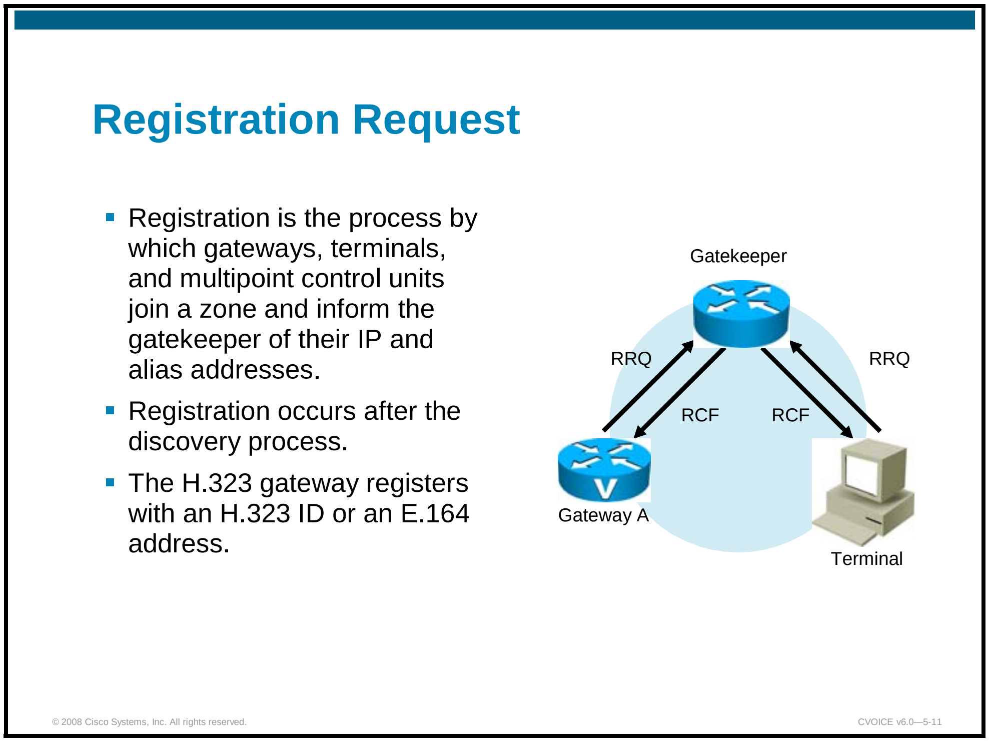
Note A Cisco IOS gatekeeper always replies to a GRQ with a GCF or GRJ message. It never remains silent.

  - A gatekeeper can be configured to respond to specific subnets.

If the message is sent via multicast, the endpoint registers nondeterministically with the first gatekeeper that responds to the message. To enforce predictable behavior, where endpoints on certain subnets are assigned to specific gatekeepers, the **zone subnet** command can be used to define the subnets that constitute a given gatekeeper zone. Any endpoint on a subnet that is not enabled for the gatekeeper is not accepted as a member of that gatekeeper zone. If the gatekeeper receives a discovery message from such an endpoint, it sends an explicit rejection message.

The GRQ message requests that any gatekeeper receiving it respond with a GCF message granting it permission to register. The GRJ message is a rejection of this request, indicating that the requesting endpoint should seek another gatekeeper.

If a gateway requests an explicit gatekeeper name, only that gatekeeper will respond. If not, the first gatekeeper to respond will become the gatekeeper of that gateway. If a gatekeeper is not available, the gateway will periodically attempt to rediscover another gatekeeper. If a gateway-discovered gatekeeper has gone off line, the gateway will stop accepting new calls and will attempt to rediscover another gatekeeper. Active calls are not affected by this process, because the RTP streams are directly between the phones.



Registration Request

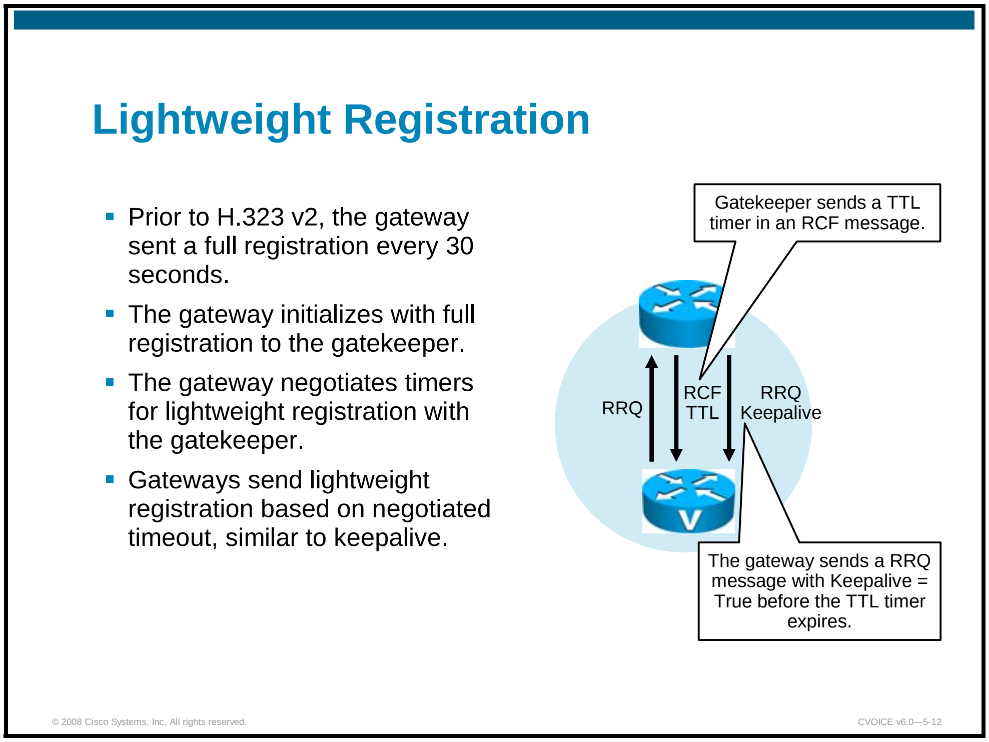
- Registration is the process by which gateways, terminals, and multipoint control units join a zone and inform the gatekeeper of their IP and alias addresses.
- Registration occurs after the discovery process.
- The H.323 gateway registers with an H.323 ID or an E.164 address.

The RRQ message is a registration request from a terminal to a gatekeeper. If the gatekeeper responds with an RCF message, the terminal will use the responding gatekeeper for future calls. If the gatekeeper responds with an RRJ message, the terminal must seek another gatekeeper with which to register.

An H.323 gateway learns of a gatekeeper by using either a static configuration or dynamic discovery. Static configuration simply means configuring the gatekeeper IP address on an Ethernet interface used for H.323 signaling.

Use this information to register an H.323 ID or an E.164 address:

- **H323 ID:** gatewayname@domain.com
- **E.164 address:** 4085551212



Lightweight Registration

- Prior to H.323 v2, the gateway sent a full registration every 30 seconds.
- The gateway initializes with full registration to the gatekeeper.
- The gateway negotiates timers for lightweight registration with the gatekeeper.
- Gateways send lightweight registration based on negotiated timeout, similar to keepalive.

Gatekeeper sends a TTL timer in an RCF message.

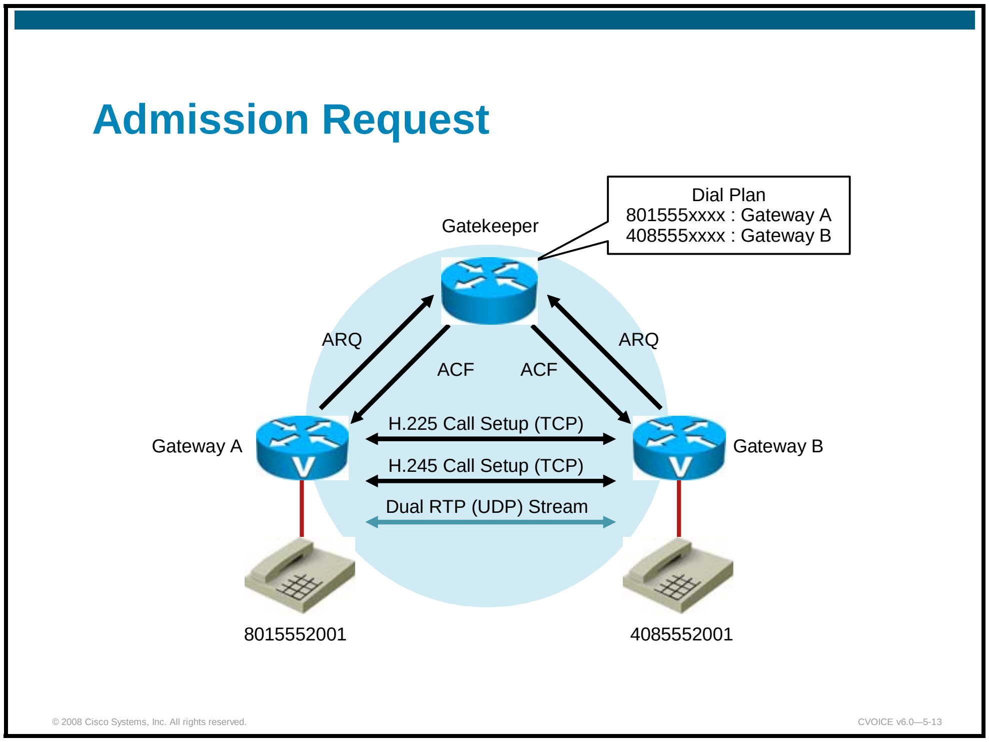
The gateway sends a RRQ message with Keepalive = True before the TTL timer expires.

CVOICE v6.0—5-12

Prior to H.323 version 2, 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. This behavior generated considerable overhead at the gatekeeper. H.323 version 2 defines a lightweight registration procedure that still requires the full registration process for initial registration, but 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 RRQ message. When a gatekeeper receives an RRQ message with a TTL value, it returns an updated TTL timer value in an 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.

An H.323 version 2 endpoint is not required to 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 are ignored other than the endpoint identifier, gatekeeper identifier, tokens, and TTL. With H.323 version 1, endpoints cannot process the TTL field in the RCF; the gatekeeper probes the endpoint with IRQs for a predetermined grace period to learn if the endpoint is still alive.



Admission Request

Dial Plan
801555xxxx : Gateway A
408555xxxx : Gateway B

Gatekeeper

ARQ

ACF

ACF

ARQ

Gateway A

H.225 Call Setup (TCP)

H.245 Call Setup (TCP)

Dual RTP (UDP) Stream

Gateway B

8015552001

4085552001

CVOICE v6.0—5-13

This example shows an admission request. Before the call is set up, Gateway A sends an ARQ request to the gatekeeper. The gatekeeper checks the status of called party and sends either an ACF message or an ARJ message. In this case, the gatekeeper sends an ACF message. The H.225 call setup will be directly between the two gateways.

Admission messages between endpoints and gatekeepers provide the basis for call admissions and bandwidth control. Gatekeepers authorize access to H.323 networks by confirming or rejecting an admission request.

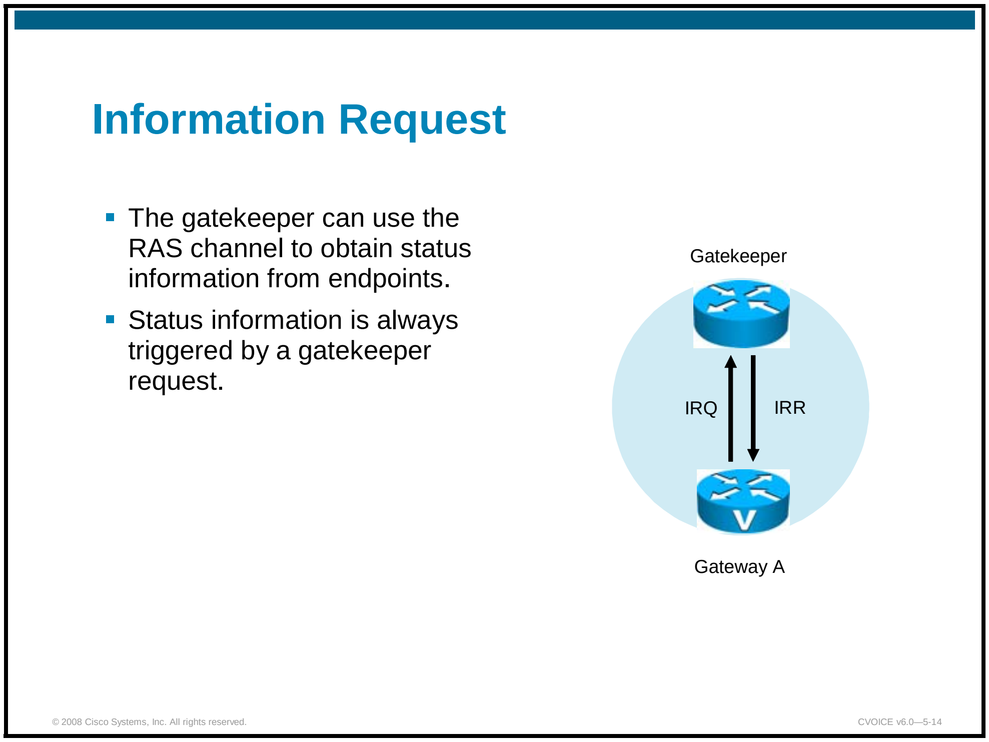
ARQ Message Failures

It may not be clear from the RAS ARJ message why the message was rejected. Here are some basic ARJ messages that may be returned and the reasons why these messages occur:

- **calledPartyNotRegistered:** This message is returned because the called party either was never registered or has not renewed its registration with a keepalive RRQ.
- **invalidPermission:** The call violates some proprietary policy within the gatekeeper that is typically set by the administrator of the network or by the gatekeeper. For example, only certain categories of endpoints may be allowed to use gateway services.
- **requestDenied:** The gatekeeper performs zone bandwidth management, and the bandwidth required for this call would exceed the bandwidth limit of the zone.
- **callerNotRegistered:** The endpoint asking for permission to be admitted to the call is not registered with the gatekeeper from whom it is asking permission.
- **routeCallToGatekeeper:** The registered endpoint has been sent a setup message from an unregistered endpoint, and the gatekeeper wishes to route the call signaling channel.
- **invalidEndpointIdentifier:** The endpoint identifier in the ARQ is not the one the gatekeeper assigned to this endpoint in the preceding RCF.
- **resourceUnavailable:** This message indicates that the gatekeeper does not have the resources, such as memory or administrated capacity, to permit the call. It could possibly

also be used in reference to the remote endpoint, meaning that the endpoint is unavailable. However, another reason may be more appropriate, such as the call capacity has been exceeded, which would return a callCapacityExceeded message.

- **securityDenial:** This message refers to the Tokens or CryptoTokens fields. For example, failed authentication, lack of authorization (permission), failed integrity, or the received crypto parameters are not acceptable or understood. This message might also be used when the password or shared secret is invalid or not available, the endpoint is not allowed to use a service, a replay was detected, an integrity violation was detected, the digital signature was incorrect, or the certificate expired.
- **qosControlNotSupported:** The endpoint specified a transport quality of service (QoS) of gatekeeperControlled in its ARQ, but the gatekeeper cannot or will not provide QoS for this call.
- **incompleteAddress:** This is used for what is referred to as “overlapped sending.” If there is insufficient addressing information in the ARQ, the gatekeeper responds with this message. This message indicates that the endpoint should send another ARQ when more addressing information is available.
- **routeCallToSCN:** This message means that the endpoint is to redirect the call to a specified telephone number on the Switched Circuit Network (SCN) or public switched telephone network (PSTN). This is only used if the ARQ was from an ingress gateway.
- **aliasesInconsistent:** The ARQdestinationInfo contained multiple aliases that identify different registered endpoints. This is distinct from destinationInfo containing one or more aliases identifying the same endpoint plus additional aliases that the gatekeeper cannot resolve.
- **exceedsCallCapacity:** This message was formerly callCapacityExceeded. It signifies that the destination endpoint does not have the capacity to accept the call. This is primarily intended for use with gateways that are version 4 or later that report their call capacity to the gatekeeper.
- **undefinedReason:** This message is used only if none of the other reasons are appropriate.



Information Request

- The gatekeeper can use the RAS channel to obtain status information from endpoints.
- Status information is always triggered by a gatekeeper request.

CVOICE v6.0—5-14

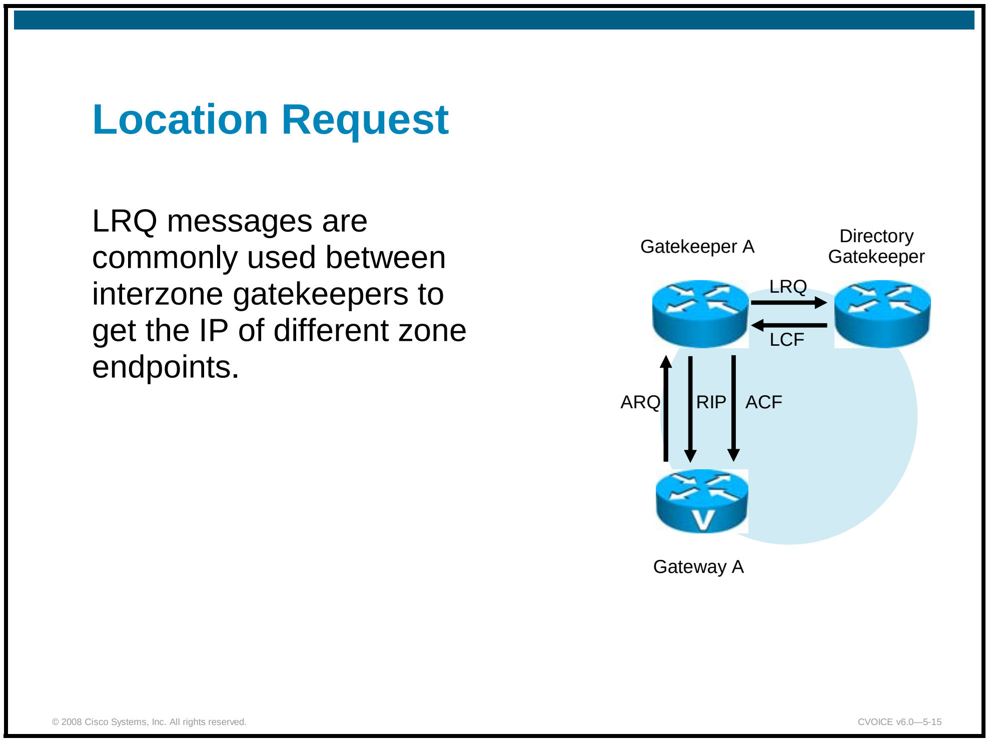
The gatekeeper periodically sends an IRQ to each registered endpoint to verify that it still exists. To limit traffic, the IRQ is sent only if the endpoint does not send some other RAS traffic within a certain interval. If an IRR is not received after an IRQ is sent, the registration is aged out of the system.

Note In addition, during calls, endpoints are instructed to send periodic unsolicited IRRs to report their call state. Cisco endpoints (proxies and gateways) send IRRs whenever there is a state transition, so that accounting information is accurate.

Whenever an IRR is sent, the age tags on the registration information for the endpoint are refreshed. In addition, if the IRR contains Cisco accounting information in its nonStandardData field, this information is used to generate authentication, authorization, and accounting (AAA) transactions.

To ensure that accounting is as accurate and simple as possible, the gatekeeper will confirm IRRs from Cisco gateways and proxies by sending an ICF. If the gateway or proxy does not receive the ICF, the IRR should be resent.

RAS status information messages include IRQ, IRR, IACK, and INACK.

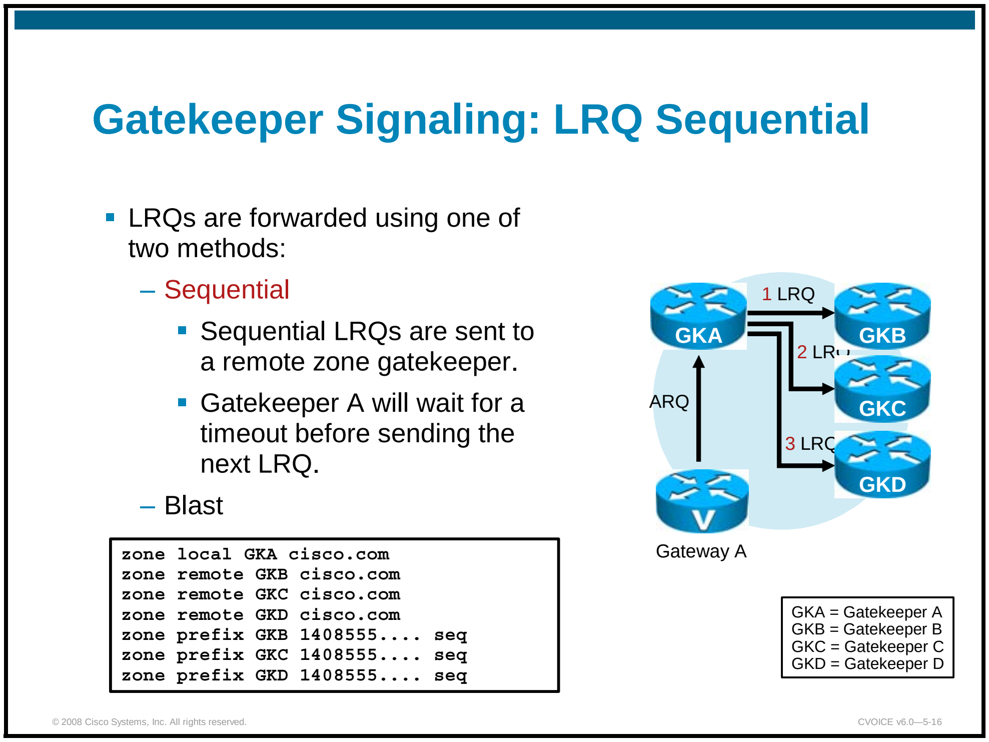


Location Request

LRQ messages are commonly used between interzone gatekeepers to get the IP of different zone endpoints.

An H.323 LRQ message is sent by a gatekeeper to another gatekeeper to request a terminating endpoint. The second gatekeeper determines the appropriate endpoint on the basis of the information contained in the LRQ message. However, sometimes all the terminating endpoints are busy servicing other calls and none are available. If you configure the **lrq reject-resource-low** command, the second gatekeeper will reject the LRQ request if no terminating endpoints are available. If the command is not configured, the second gatekeeper will allocate and return a terminating endpoint address to the sending gatekeeper even if all the terminating endpoints are busy.

Note The gatekeeper sends out an RIP message to an endpoint or gateway to prevent call failures due to RAS message timeouts during gatekeeper call processing. A gateway receiving a RIP message will continue to wait for a gatekeeper response.



Gatekeeper Signaling: LRQ Sequential

- LRQs are forwarded using one of two methods:
  - Sequential
    - Sequential LRQs are sent to a remote zone gatekeeper.
    - Gatekeeper A will wait for a timeout before sending the next LRQ.
  - Blast

```
zone local GKA cisco.com
zone remote GKB cisco.com
zone remote GKC cisco.com
zone remote GKD cisco.com
zone prefix GKB 1408555.... seq
zone prefix GKC 1408555.... seq
zone prefix GKD 1408555.... seq
```

GKA = Gatekeeper A
GKB = Gatekeeper B
GKC = Gatekeeper C
GKD = Gatekeeper D

For gatekeeper redundancy and load sharing features, you can configure multiple gatekeepers to service the same zone or technology prefix by sending LRQs to two or more gatekeepers. The LRQs are sent either sequentially to the gatekeepers or to all gatekeepers at the same time (blast).

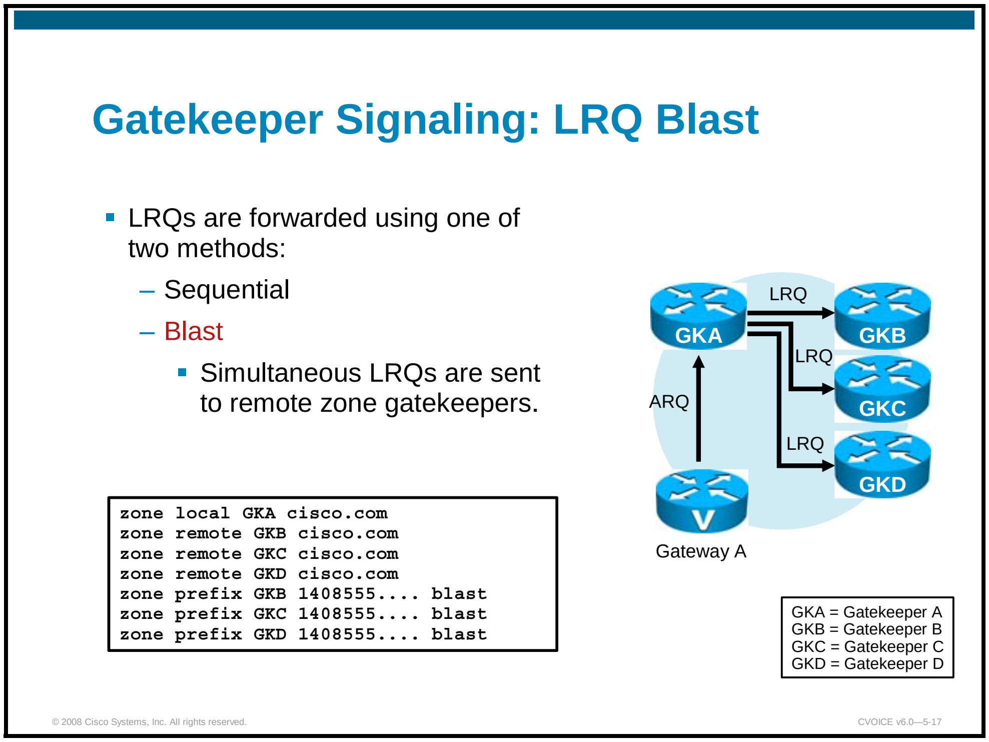
Sequential forwarding of LRQs is the default forwarding mode. With sequential LRQ forwarding, the originating gatekeeper will forward an LRQ to the first gatekeeper in the matching list. The originating gatekeeper will then wait for a response before sending an LRQ to the next gatekeeper on the list. If the originating gatekeeper receives an LCF while it is waiting, it will terminate the LRQ forwarding process.

If you have multiple matching prefix zones, you may want to consider using sequential LRQ forwarding as opposed to blast LRQ forwarding. With sequential forwarding, you can configure which routes are primary, secondary, and tertiary.

There are three gatekeepers shown in the figure. Gatekeeper A will send an LRQ first to Gatekeeper B. Gatekeeper B will send a reply as either an LCF or an LRJ to Gatekeeper A. If Gatekeeper B returns an LCF to Gatekeeper A, the LRQ forwarding process will be terminated. If Gatekeeper B returns an LRJ to Gatekeeper A, then Gatekeeper A will send an LRQ to Gatekeeper C. Gatekeeper C will return either an LCF or LRJ to Gatekeeper A. Then, Gatekeeper A will either terminate the LRQ forwarding process or start the LRQ process again with Gateway D.

Notice the zone prefix commands at the bottom of the router output. Because sequence is the default method for LRQ forwarding, the option **seq** can be included, and sequential LRQ forwarding will take place.

Note	With sequential LRQs, there is a fixed timer when LRQs are sent. Even if Gatekeeper A gets an LRJ back immediately from Gatekeeper B, it will wait a fixed amount of time before sending the next LRQ to Gatekeeper C and Gatekeeper D. You can speed up this process by using the **lrq lrj immediate-advance** timer command.



Gatekeeper Signaling: LRQ Blast

- LRQs are forwarded using one of two methods:
  - Sequential
  - Blast
    - Simultaneous LRQs are sent to remote zone gatekeepers.

```
zone local GKA cisco.com
zone remote GKB cisco.com
zone remote GKC cisco.com
zone remote GKD cisco.com
zone prefix GKB 1408555.... blast
zone prefix GKC 1408555.... blast
zone prefix GKD 1408555.... blast
```

GKA
LRQ
GKB
LRQ
GKC
ARQ
LRQ
GKD
V
Gateway A

GKA = Gatekeeper A
GKB = Gatekeeper B
GKC = Gatekeeper C
GKD = Gatekeeper D

CVOICE v6.0—5-17

In the figure, when blast LRQ is used, Gatekeeper A will send LRQs to all three gatekeepers that match the zone prefix. If they all three reply with a positive confirmation (for example, an LCF), Gatekeeper A chooses which one to use. Gatekeeper A can tailor the choice by using the **cost** and **priority** keywords at the end of the zone remote statement like this:

```
zone remote GKB cisco.com cost 50 priority 50

zone remote GKC cisco.com cost 51 priority 49

zone remote GKD Cisco.com cost 52 priority 48
```

The **cost** and **priority** command options need to be examined carefully for correct priority operation. The default cost is 50 in a range from 1 to 100. In the example, you see the three gatekeepers have costs of 50, 51, and 52. This means that Gatekeeper B has a lower cost than Gatekeeper C, and Gatekeeper C has a lower cost than Gatekeeper D. Therefore, Gatekeeper B will be selected first, and then Gatekeeper C, and finally Gatekeeper D.

The priority also can be set. The default for this option is also 50 in a range from 1 to 100. In the example, the gatekeepers with a higher cost also have a lower priority. When each of the gatekeepers returns an LCF to Gatekeeper A, a decision about which gatekeeper the call should be forwarded to can be made based on either cost or priority.

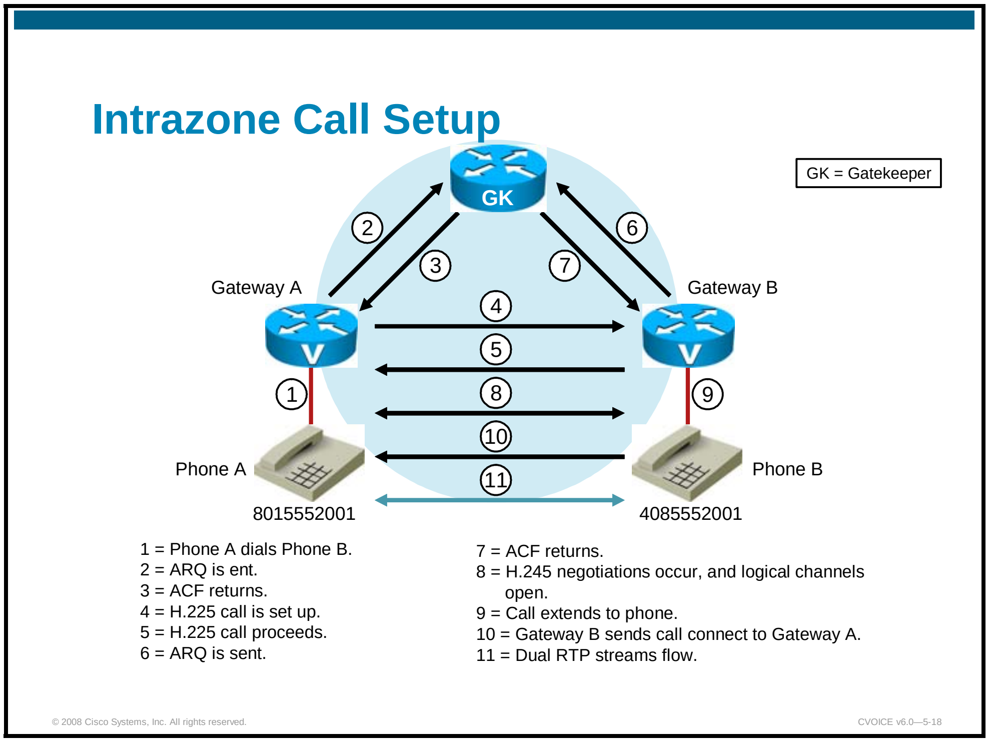
You can assign cost and priority values independently of each other. You may choose to assign only a cost or a priority to a specific gatekeeper. If the values you assign to a specific gatekeeper are higher or lower than the default values, and there are other gatekeepers that are using default values for cost and priority, call routing may take these unexpected paths:

```
zone prefix GKB 1408555.... blast

zone prefix GKC 1408555.... blast

zone prefix GKD 1408555.... blast
```

In this example, the blast option has been added to the zone prefix commands. This option is an important part of the configuration that is often overlooked. The blast option allows Gatekeeper

A to simultaneously send LRQs to Gatekeeper B, Gatekeeper C, and Gatekeeper D. If the blast command option is omitted, the gatekeeper will use the default method, which is to choose a gatekeeper based on sequence.

To summarize, Gatekeeper A receives an ARQ from a gateway for 1408555xxxx. Gatekeeper A then blasts LRQs to all gatekeepers, which in this case are Gatekeeper B, Gatekeeper C, and Gatekeeper D. Gatekeeper A will use the cost and priority values to evaluate the received LCFs to determine where the call should be forwarded. In this case, if all of the downstream gatekeepers respond with LCFs, Gatekeeper A will use the priority and cost values and choose to forward the call to Gatekeeper B.

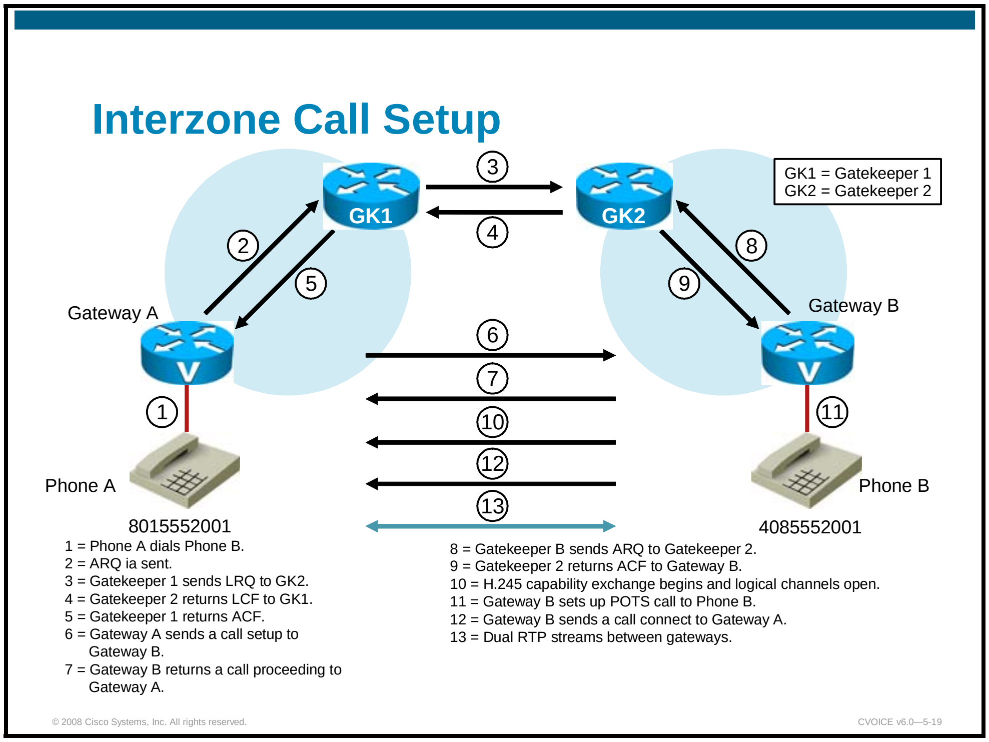


Intrazone Call Setup

1 = Phone A dials Phone B.
2 = ARQ is ent.
3 = ACF returns.
4 = H.225 call is set up.
5 = H.225 call proceeds.
6 = ARQ is sent.
7 = ACF returns.
8 = H.245 negotiations occur, and logical channels open.
9 = Call extends to phone.
10 = Gateway B sends call connect to Gateway A.
11 = Dual RTP streams flow.

This figure shows the sequence of the signaling events and the basic signaling that takes place between a gateway and gatekeeper:

1. Phone A dials the phone number 4085552001 for Phone B.
2. Gateway A sends an ARQ to the gatekeeper, asking permission to call Phone B.
3. The gatekeeper does a lookup and finds Phone B registered to Gateway B and returns an ACF with the IP address of Gateway B.
4. Gateway A sends an H.225 call setup message to Gateway B with the phone number of Phone B.
5. Gateway B sends an H.255 call proceeding message to Gateway A.
6. Gateway B sends an ARQ to the gateway, asking permission to answer Gateway A’s call.
7. The gateway returns an ACF with the IP address of Gateway A.
8. Gateway B and Gateway A initiate an H.245 capability exchange and open logical channels.
9. Gateway B sets up a plain old telephone service (POTS) call to Phone B at 4085552001.
10. When Phone B answers, Gateway B sends an H.245 call connect message to Gateway A.
11. Dual RTP streams flow between gateways.



Interzone Call Setup

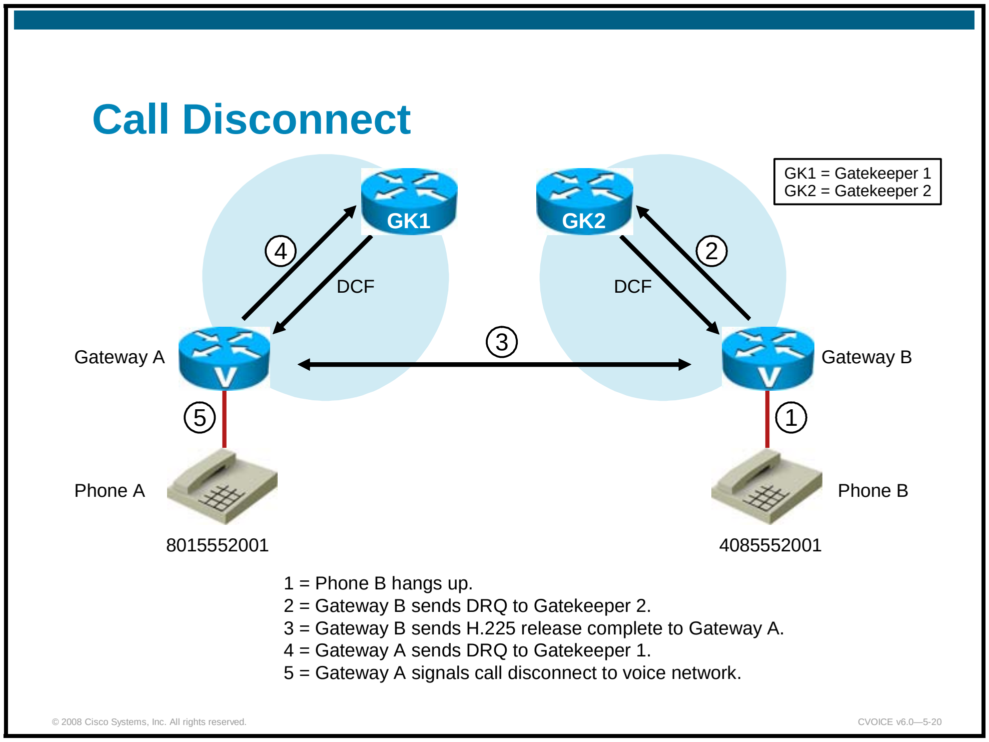
1 = Phone A dials Phone B.
2 = ARQ ia sent.
3 = Gatekeeper 1 sends LRQ to GK2.
4 = Gatekeeper 2 returns LCF to GK1.
5 = Gatekeeper 1 returns ACF.
6 = Gateway A sends a call setup to Gateway B.
7 = Gateway B returns a call proceeding to Gateway A.
8 = Gatekeeper B sends ARQ to Gatekeeper 2.
9 = Gatekeeper 2 returns ACF to Gateway B.
10 = H.245 capability exchange begins and logical channels open.
11 = Gateway B sets up POTS call to Phone B.
12 = Gateway B sends a call connect to Gateway A.
13 = Dual RTP streams between gateways.

CVOICE v6.0—5-19

This figure shows how gatekeepers signal each other in a multizone gatekeeper network. It shows the sequence of RAS signaling events between gatekeepers, the LRQ RAS messages, and how LRQ is used.

This is the basic gateway-to-gatekeeper signaling that occurs between zones:

1. Phone A dials the phone number 4085552001 for Phone B.
2. Gateway A sends Gatekeeper 1 an ARQ, asking permission to call Phone B.
3. Gatekeeper 1 does a lookup and does not find Phone B registered. Gatekeeper 1 does a prefix lookup and finds a match with Gatekeeper 2. Gatekeeper 1 sends an LRQ to Gatekeeper 2 and a RIP to Gateway A.
4. Gatekeeper 2 does a look-up, finds Phone B registered, and returns an LCF to Gatekeeper 1 with the IP address of Gateway B.
5. Gatekeeper 1 returns an ACF with the IP address of Gateway B.
6. Gateway A sends an H.225 call setup message to Gateway B with the phone number of Phone B.
7. Gateway B sends an H.225 call proceeding message to Gateway A.
8. Gateway B sends Gatekeeper 2 an ARQ asking permission to answer the call from Gateway A.
9. Gatekeeper 2 returns an ACF with the IP address of Gateway A.
10. Gateway B and Gateway A initiate an H.245 capability exchange and open logical channels.
11. Gateway B sets up a POTS call to Phone B at 4085552001.
12. Gateway B sends a call connect to Gateway A.
13. Dual RTP streams flow between gateways.



Call Disconnect

1 = Phone B hangs up.
2 = Gateway B sends DRQ to Gatekeeper 2.
3 = Gateway B sends H.225 release complete to Gateway A.
4 = Gateway A sends DRQ to Gatekeeper 1.
5 = Gateway A signals call disconnect to voice network.

CVOICE v6.0—5-20

This figure shows basic call disconnect signaling between a gateway and a gatekeeper. The RAS signaling messages used in this figure are DRQ and DCF.

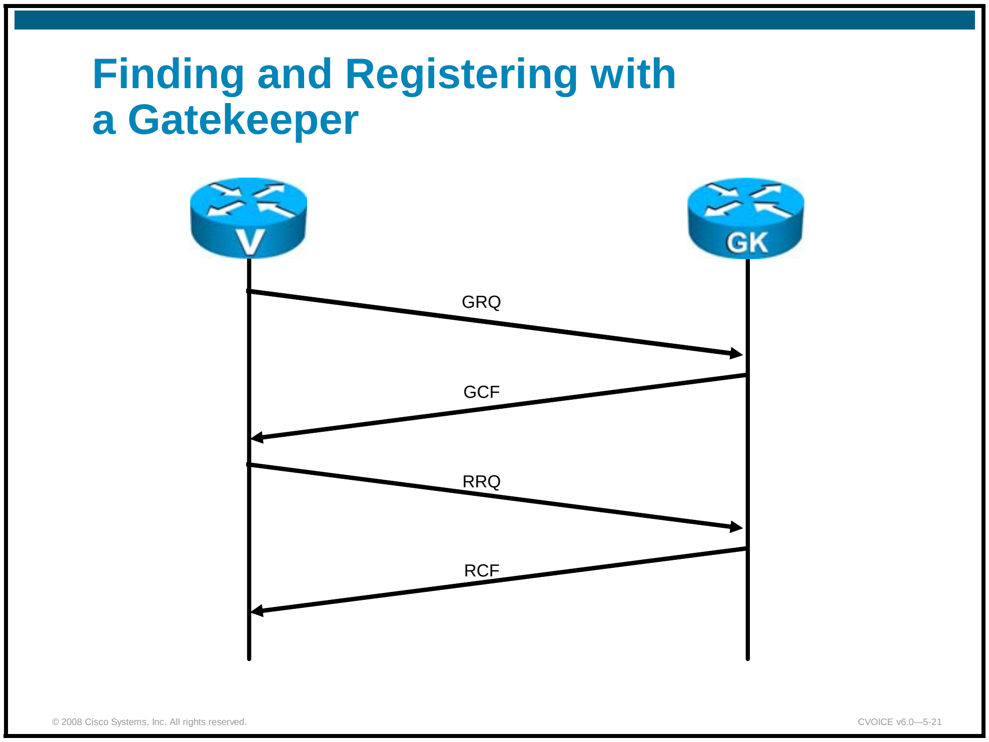
Phones A and B are in a conversation, and this is the RAS signaling that occurs:

1. Phone B hangs up.
2. Gateway B sends a DRQ to Gatekeeper 2, disconnecting the call between Phones A and B. A DCF is received some time later.
3. Gateway B sends a Q.931 release complete message to Gateway A.
4. Gateway A sends a DRQ to Gatekeeper 1, disconnecting the call between Phones A and B. A DCF is received some time later.
5. Gateway A signals a call disconnect to the voice network.

The mechanism to disconnect the call differs depending on the trunk used on Gateway A. If the phone is set to Foreign Exchange Station (FXS), then there is no mechanism to signal the call disconnect.

Call Flows with a Gatekeeper

This topic describes call setup scenarios with a gatekeeper.



Finding and Registering with a Gatekeeper

© 2008 Cisco Systems, Inc. All rights reserved.

CVOICE v6.0—5-21

The figure illustrates how an endpoint locates and registers with a gatekeeper. A gatekeeper adds scalability to H.323. Without a gatekeeper, an endpoint must recognize or have the ability to resolve the IP address of the destination endpoint.

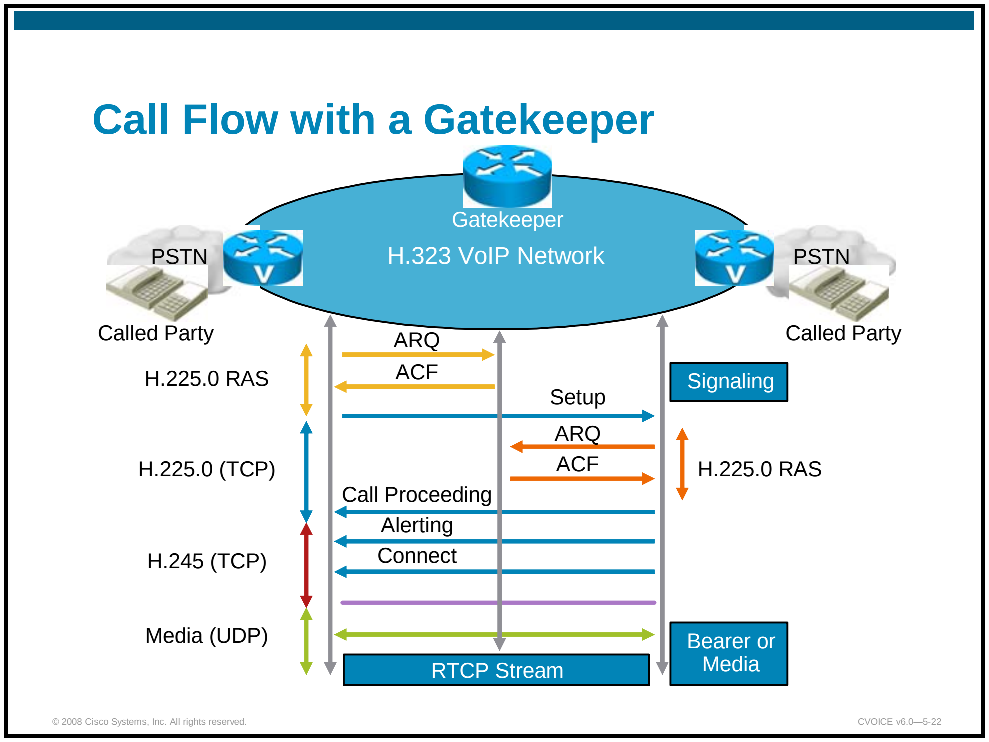
Before an endpoint can use a gatekeeper, it must register with the gatekeeper. To register, an endpoint must recognize the IP address of the gatekeeper.

One of these two methods is used to determine the address of the gatekeeper:

- An endpoint can be preconfigured to recognize the domain name or IP address of its gatekeeper. If configured to recognize the name, an endpoint must have a means to resolve the name to an IP address. A common address resolution technique is the Domain Name System (DNS).
- An endpoint can issue a multicast GRQ to the gatekeeper discovery address (224.0.1.41) to discover the IP address of its gatekeeper. If the endpoint receives a GCF for the request, it uses the IP address to proceed with registration.

To initiate registration, an endpoint sends an RRQ to the gatekeeper. In the RRQ, the endpoint identifies itself with its ID and provides its IP address. Optionally, the endpoint lists the prefixes (for example, telephone numbers) that it supports. These prefixes are gleaned from the plain old telephone service (POTS) dial-peer destination patterns associated with any FXS port.

With this procedure, a gatekeeper determines the location and identity of endpoints and the identities of SCN endpoints from gateway registrations.



Call Flow with a Gatekeeper

Gatekeeper

H.323 VoIP Network

PSTN

PSTN

Called Party

Called Party

H.225.0 RAS

ARQ

ACF

Setup

Signaling

H.225.0 (TCP)

ARQ

ACF

H.225.0 RAS

Call Proceeding

Alerting

Connect

H.245 (TCP)

Media (UDP)

RTCP Stream

Bearer or Media

CVOICE v6.0—5-22

In this example, both endpoints have registered with the same gatekeeper. Call flow with a gatekeeper proceeds as follows:

1. The gateway sends an ARQ to the gatekeeper to initiate the procedure. The gateway is configured with the domain or address of the gatekeeper.

2. The gatekeeper responds to the ARQ with an ACF. In the confirmation, the gatekeeper provides the IP address of the remote endpoint.

3. When the originating endpoint identifies the terminating endpoint, it initiates a basic call setup.

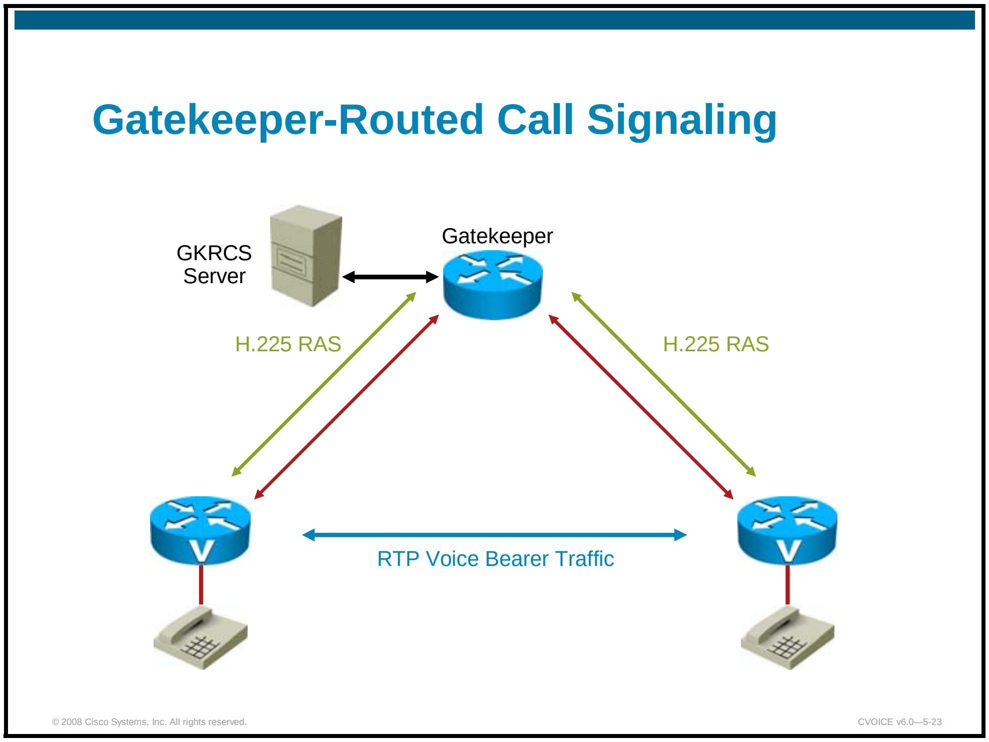
4. Before the terminating endpoint accepts the incoming call, it sends an ARQ to the gatekeeper to gain permission.

5. The gatekeeper responds affirmatively, and the terminating endpoint proceeds with the call setup procedure.

During this procedure, if the gatekeeper responds to either endpoint with an ARJ to the ARQ, the endpoint that receives the rejection terminates the procedure.

Gatekeeper-Routed Call Signaling

The figure shows an example of gatekeeper-routed call signaling.



Gatekeeper-Routed Call Signaling

© 2008 Cisco Systems, Inc. All rights reserved.

CVOICE v6.0—5-23

In the previous examples, the call-signaling channel is created from endpoint to endpoint. In some cases, it is desirable to have the gatekeeper represent the other endpoint for signaling purposes. This method is called gatekeeper-routed call signaling. The process for gatekeeper-routed call signaling is as follows:

1. The gatekeeper responds to an ARQ and advises the endpoint to perform the call setup procedure with the gatekeeper, not with the terminating endpoint.

2. The endpoint initiates the setup request with the gatekeeper.

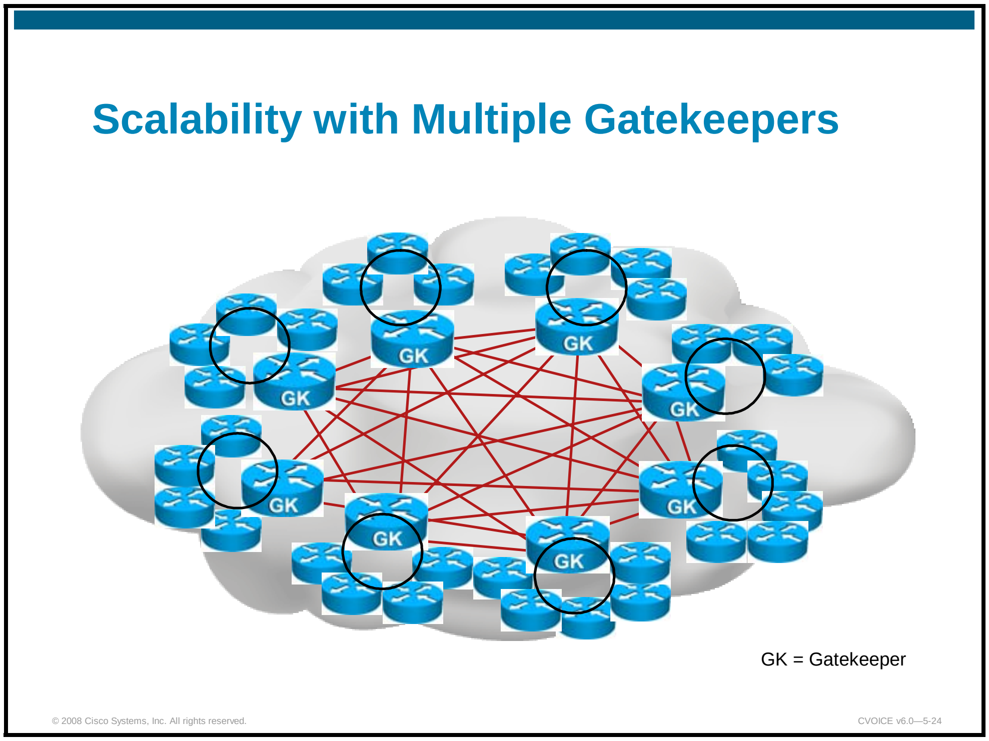
3. The gatekeeper sends its own request to the terminating endpoint and incorporates some of the details acquired from the originating request.

4. When a connect message is received from the terminating endpoint, the gatekeeper sends a connect message to the originating endpoint.

5. The two endpoints establish an H.245 control channel between them. The call procedure continues normally from this point.

Call Flows with Multiple Gatekeepers

This subtopic describes the use of multiple gatekeepers for scalability and illustrates call flow in a multiple gatekeeper environment.



Scalability with Multiple Gatekeepers

GK = Gatekeeper

CVOICE v6.0—5-24

By simplifying configuration of the endpoints, gatekeepers aid in building large-scale VoIP networks. As the VoIP network grows, incorporating additional gatekeepers enhances the network scalability.

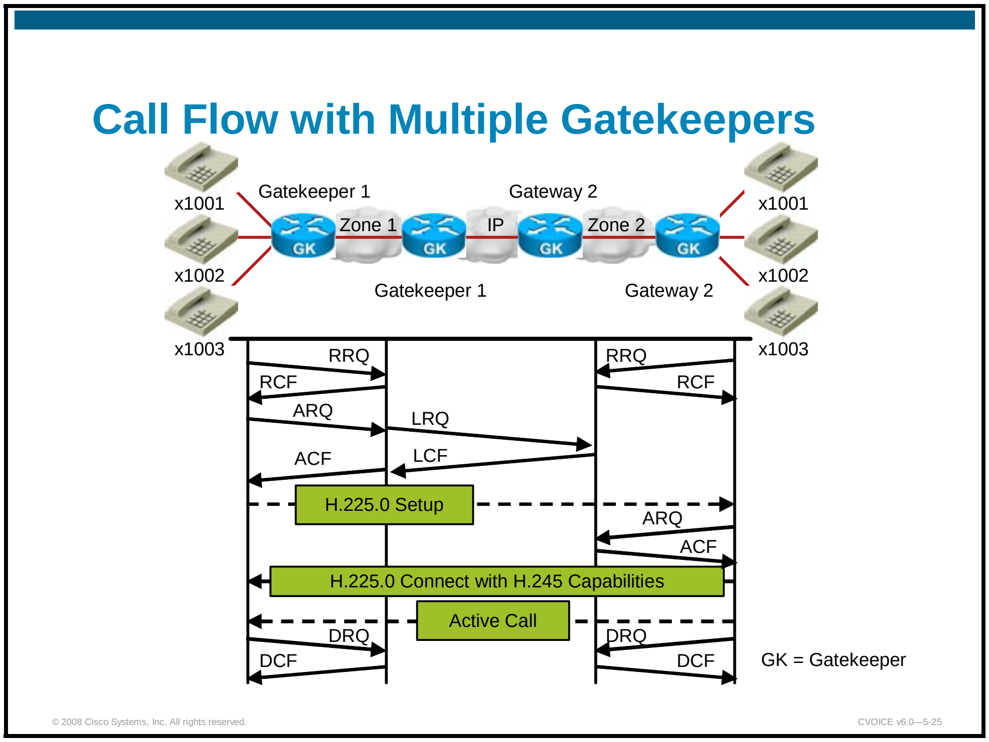
Without a gatekeeper, endpoints must find each other by any means available. This limits the growth potential of the VoIP network. Through the registration and address resolution services of a gatekeeper, growth potential improves significantly.

A single gatekeeper design may not be appropriate for several reasons. A single gatekeeper can become overloaded, or it can have an inconvenient network location, resulting in a long and expensive round trip to it.

Deploying multiple gatekeepers offers a more scalable and robust environment.

Call Setup with Multiple Gatekeepers Example

The example shows a call setup involving two gatekeepers.



Call Flow with Multiple Gatekeepers

© 2008 Cisco Systems, Inc. All rights reserved.

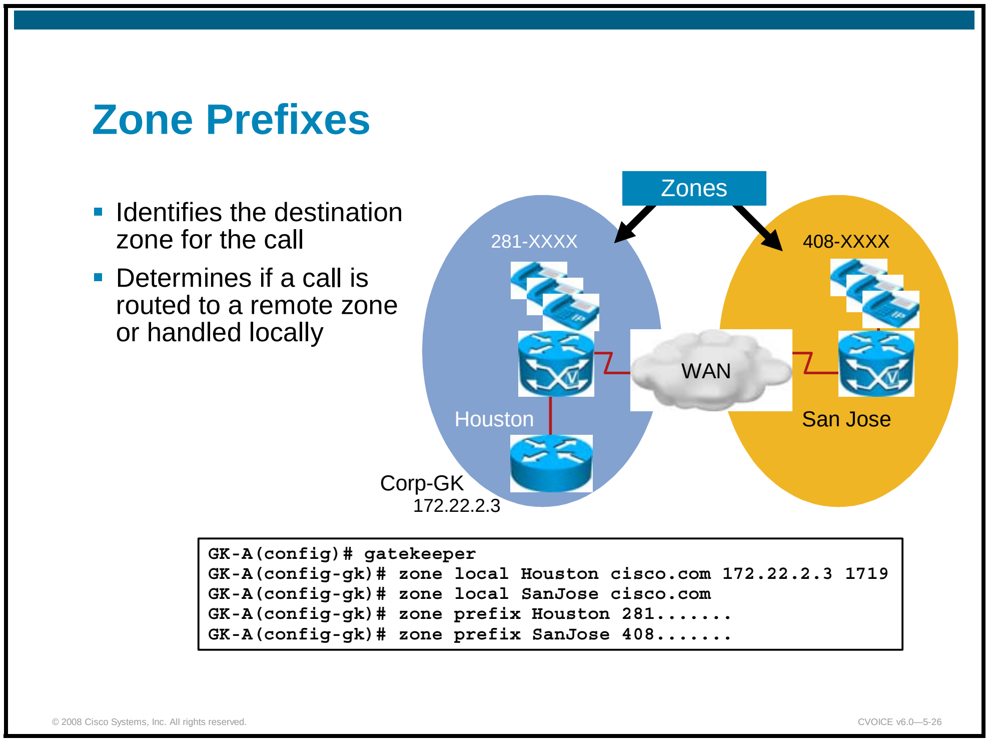
CVOICE v6.0—5-25

In this example, each endpoint is registered with a different gatekeeper. Notice the changes in the following call setup procedure:

1. The originating endpoint sends an ARQ to its gatekeeper requesting permission to proceed and asking for the session parameters for the terminating endpoint.
2. The gatekeeper for the originating endpoint (Gatekeeper 1) determines from its configuration or from a directory resource that the terminating endpoint is potentially associated with gatekeeper 2. Gatekeeper 1 sends an LRQ to Gatekeeper 2.
3. Gatekeeper 2 recognizes the address and sends back an LCF. In the confirmation, Gatekeeper 2 provides the IP address of the terminating endpoint.
4. If Gatekeeper 1 considers the call acceptable for security and bandwidth reasons, it maps the LCF to an ARQ and sends the confirmation back to the originating endpoint.
5. The endpoint initiates a call setup to the remote endpoint.
6. Before accepting the incoming call, the remote endpoint sends an ARQ to Gatekeeper 2 requesting permission to accept the incoming call.
7. Gatekeeper 2 performs admission control on the request and responds with a confirmation.
8. The endpoint responds to the call setup request.
9. The call setup progresses through the H.225.0 call function and H.245 control function procedures until the RTP sessions are initiated.
10. At the conclusion of the call, each endpoint sends a disconnect request to its gatekeeper to advise the gatekeeper that the call is complete.
11. The gatekeeper responds with a confirmation

Zone Prefixes

This topic describes how gatekeeper zone prefixes are used for call routing.



Zone Prefixes

- Identifies the destination zone for the call
- Determines if a call is routed to a remote zone or handled locally

```
GK-A(config)# gatekeeper
GK-A(config-gk)# zone local Houston cisco.com 172.22.2.3 1719
GK-A(config-gk)# zone local SanJose cisco.com
GK-A(config-gk)# zone prefix Houston 281.......
GK-A(config-gk)# zone prefix SanJose 408.......
```

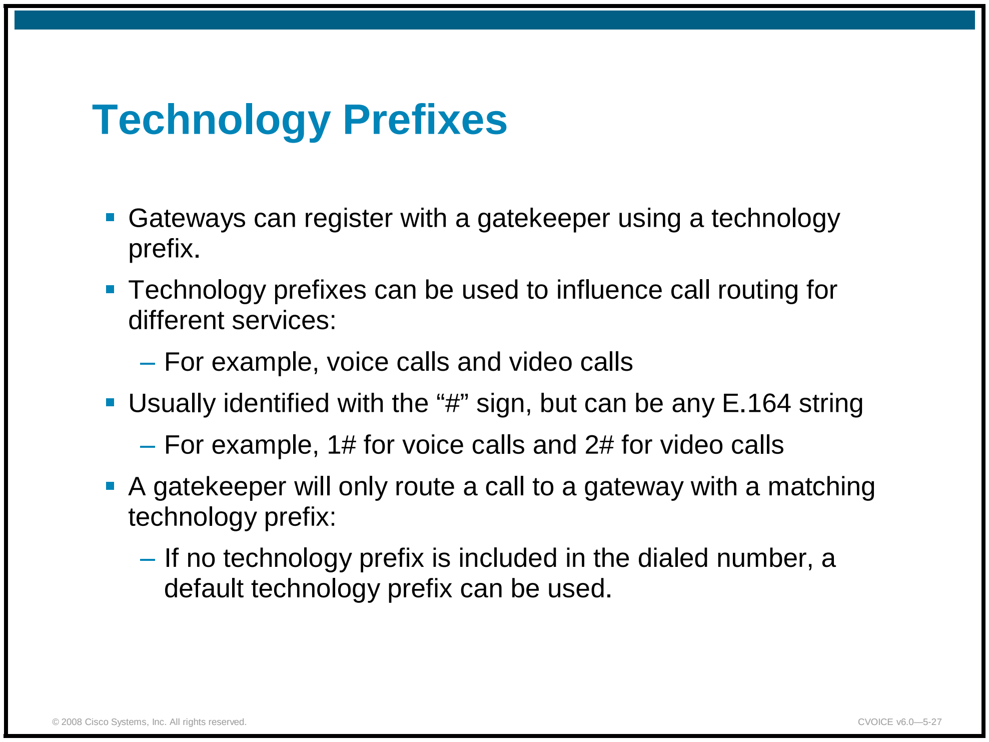
A zone prefix is the part of the called number that identifies the destination zone for a call. Zone prefixes are usually used to associate an area code to a configured zone and they serve the same purpose as the domain names in the H.323 ID address space.

The Cisco gatekeeper determines if a call is routed to a remote zone or handled locally. For example, according to this configuration excerpt, gatekeeper Corp-GK in Houston forwards 408....... calls to the San Jose gateway. Calls to area code (281) are handled locally.

When the San Jose gateway receives the request, the gatekeeper must resolve the address so that the call can be sent to its final destination. There may be an H.323 endpoint with that E.164 address that has registered with the San Jose gateway, in which case the San Jose gateway returns the IP address for that endpoint. However, it is possible that the E.164 address belongs to a device that is not H.323 (for example, a telephone or an H.320 terminal). Because devices that are not H.323 do not register with gatekeepers, the San Jose gateway cannot resolve the address. The gatekeeper must be able to select a gateway that can be used to reach such devices. This is where the technology prefixes (also called “gateway-type”) become useful.

Technology Prefixes

This topic describes gatekeeper technology prefixes.

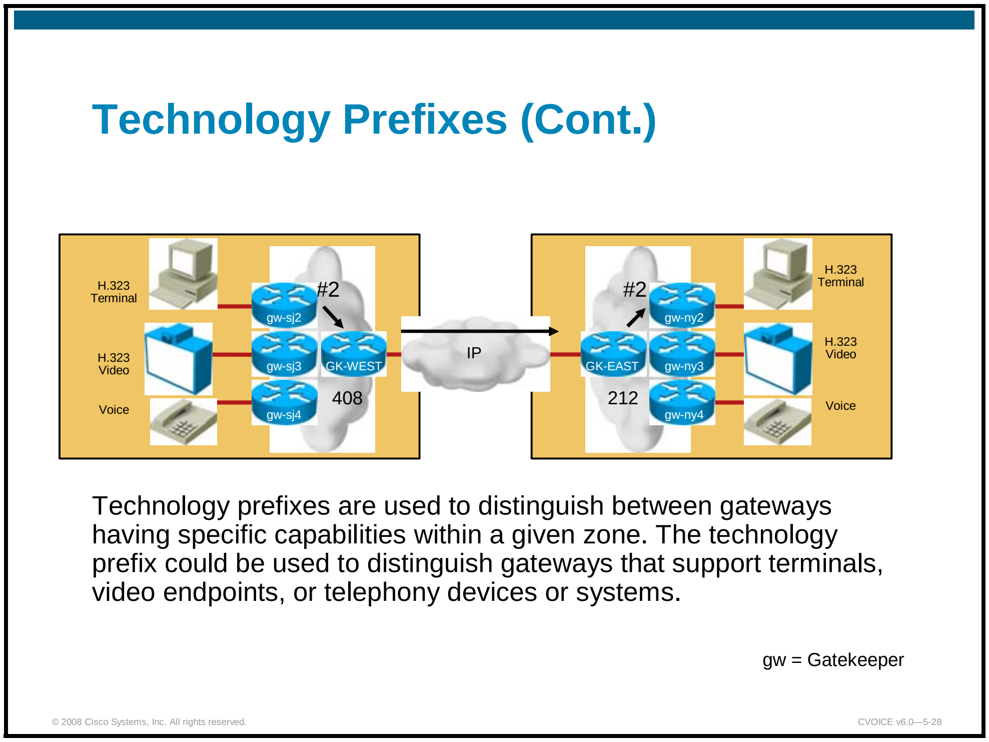


Technology Prefixes

- Gateways can register with a gatekeeper using a technology prefix.
- Technology prefixes can be used to influence call routing for different services:
  - For example, voice calls and video calls
- Usually identified with the “#” sign, but can be any E.164 string
  - For example, 1# for voice calls and 2# for video calls
- A gatekeeper will only route a call to a gateway with a matching technology prefix:
  - If no technology prefix is included in the dialed number, a default technology prefix can be used.

CVOICE v6.0—5-27

A technology prefix is an optional H.323 standards-based feature that is supported by Cisco gateways and gatekeepers that enables more flexibility in call routing within an H.323 VoIP network. Technology prefixes are used to group gateways by type (such as voice or video) or class or to define a pool of gateways.



Technology Prefixes (Cont.)

Technology prefixes are used to distinguish between gateways having specific capabilities within a given zone. The technology prefix could be used to distinguish gateways that support terminals, video endpoints, or telephony devices or systems.

gw = Gatekeeper

CVOICE v6.0—5-28

Technology prefixes are used to separately identify gateways that support different types of services, such as video calls versus voice calls, where the gatekeeper can use this information to correspondingly route traffic to the appropriate gateways.

The network administrator selects technology prefixes (tech-prefixes) to denote different types or classes of gateways. The gateways are then configured to register with their gatekeepers with these prefixes. For example, voice gateways can register with tech-prefix 1#, H.320 gateways with tech-prefix 2#, and voicemail gateways with tech-prefix 3#. More than one gateway can register with the same type of prefix. When this happens, the gatekeeper makes a random selection among gateways of the same type.

If the callers know the type of device that they are trying to reach, they can include the tech-prefix in the destination address to indicate the type of gateway to use to get to the destination. For example, if a caller knows that address 2125551111 belongs to a regular telephone, the destination address of 1#2125551111 can be used, where 1# indicates that the address should be resolved by a voice gateway. When the voice gateway receives the call for 1#2125551111, it strips off the tech-prefix and bridges the next leg of the call to the telephone at 2125551111.

Cisco gatekeepers use tech-prefixes to route calls when there is no E.164 addresses registered (by a gateway) that matches the called number. In fact, this is a common scenario, because most Cisco IOS gateways can either register their H.323 ID or destination patterns. Cisco Unified Communications Manager Express and Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) can register the DNS of their Ethernet phone-dn (ephone-directory number) at the gatekeeper. Without E.164 addresses registered, the Cisco gatekeeper relies on these two options to make the call routing decision:

- **Technology prefix matches option:** The Cisco gatekeeper uses the tech-prefix appended in the called number to select the destination gateway or zone.
- **Default technology prefixes option:** The Cisco gatekeeper assigns a default gateway or gateways for routing unresolved call addresses. This assignment is based on the registered tech-prefix of the gateways.

The gatekeeper uses a default tech-prefix for routing all calls that do not have a tech-prefix or for gateways that do not have a tech-prefix defined. That remote gatekeeper then matches the tech-prefix to decide which of its gateways to hop off. The zone prefix determines the routing to a zone just as the tech-prefix determines the gateway in that zone.

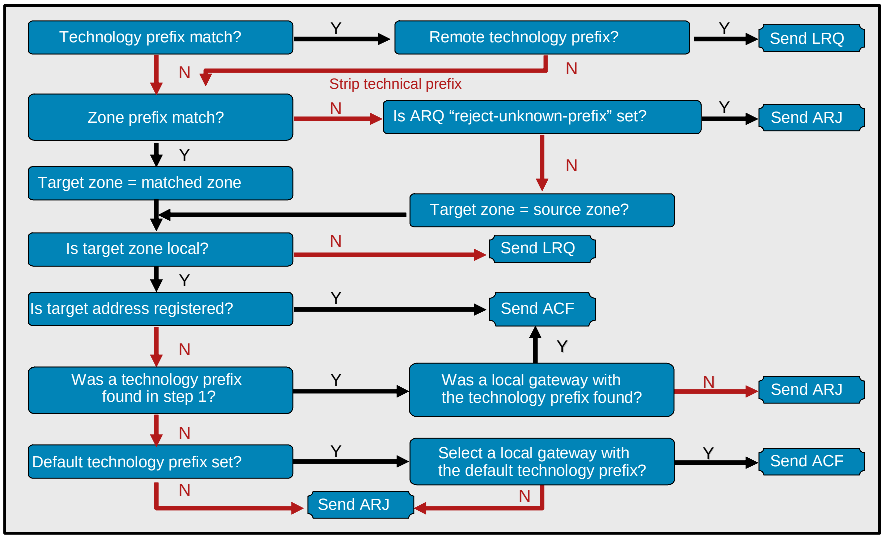
If the majority of calls hop off on a particular type of gateway, the gatekeeper can be configured to use that type of gateway as the default type, so that callers no longer have to prepend a tech-prefix on the address. For example, if you use mostly voice gateways in your network, and you have configured all your voice gateways to register with tech-prefix 1, you can configure your gatekeeper to use "1xx gateways" as the default:

```
router(config-gk)# gw-type-prefix 1# default-technology
```

Gatekeeper Call Routing

This topic describes the gatekeeper call routing process.

Gatekeeper Address Resolution



Technology prefix match?
Y
Remote technology prefix?
Y
Send LRQ
N
N
Strip technical prefix
Zone prefix match?
N
Is ARQ "reject-unknown-prefix" set?
Y
Send ARJ
Y
N
Target zone = matched zone
Target zone = source zone?
Is target zone local?
N
Send LRQ
Y
Is target address registered?
Y
Send ACF
N
Y
Was a technology prefix found in step 1?
Y
Was a local gateway with the technology prefix found?
N
Send ARJ
N
Default technology prefix set?
Y
Select a local gateway with the default technology prefix?
Y
Send ACF
N
Send ARJ
N

CVOICE v6.0—5-29

When a gatekeeper receives an ARQ message from a gateway, it reacts like this:

- If there is a tech-prefix specified in the admission request and it is a hopoff tech-prefix, the gatekeeper sends an LRQ message.
- If there is no tech-prefix or the tech-prefix is not a hopoff tech-prefix, the gatekeeper uses the exact E.164 alias in the ARQ message, including the zone prefix, if there is one, to search its E.164 alias table. It then proceeds according to the result of the search and the configuration:
  - — If no match is found and the **arq reject-unknown prefix** command is set, the gatekeeper sends an ARJ message.
  - — If a match is found and the destination zone is not local, the gatekeeper sends an LRQ message to the remote zone.
  - — If the destination zone is local and the destination address is registered, the gatekeeper sends an ACF message.
  - — If the destination zone is local and the destination address is not registered, but the local gateway is found with the specified tech-prefix or the default tech-prefix, the gatekeeper sends an ACF. If no local gateway with the specified tech-prefix is found, the gatekeeper sends an ARJ message.
- If there is no matching tech-prefix and no default tech-prefix is set, the gatekeeper sends an ARJ message.

When a gatekeeper receives an LRQ message from a gateway, it performs one of these procedures:

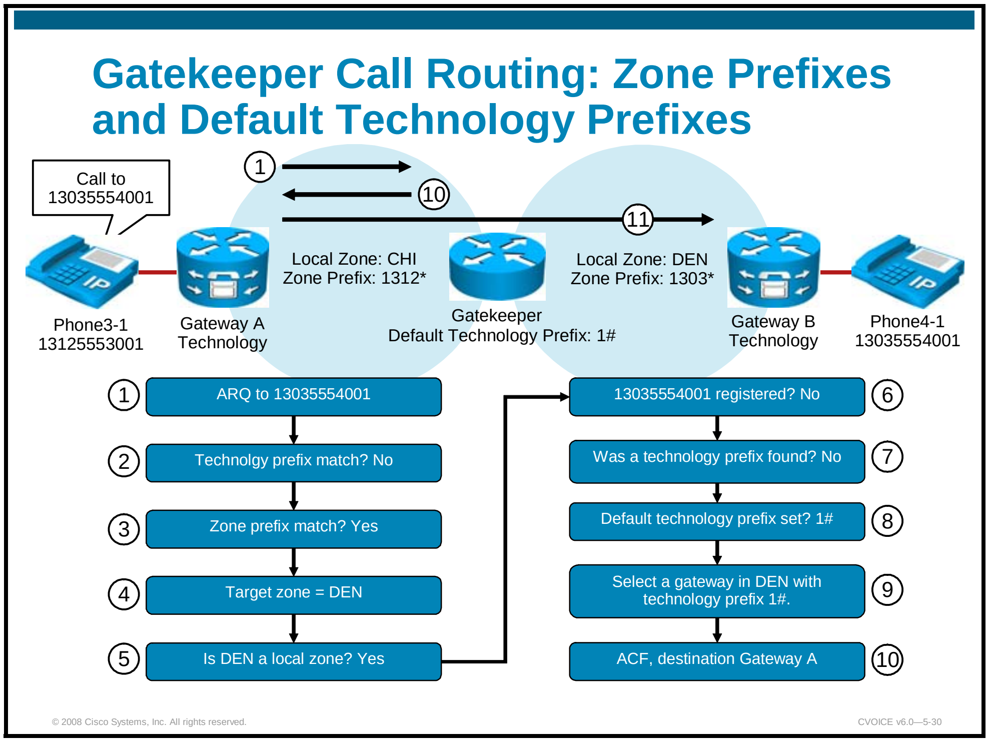
- If there is a hopoff tech-prefix specified in the admission request, the destination zone is not local, and the **lrq forward-queries** command is set, the gatekeeper sends an LRQ message.

- If there is no tech-prefix or the tech-prefix is not a hop off technology prefix, the gatekeeper uses the exact E.164 alias in the LRQ message to search its E.164 alias table. Then, depending on the results of the search, it proceeds accordingly:
  - If no match is found and the **lrq reject-unknown prefix** command is set, the gatekeeper sends an LRJ message.
  - If a match is found and the destination zone is the matched zone, the gatekeeper sends an LRQ message to the destination zone.
  - If the destination zone is local and the destination address is registered, the gatekeeper sends an LCF message.
  - If the destination zone is local and the destination address is not registered, but the local gateway is found with the specified technology prefix or the default tech-prefix, the gatekeeper sends an LCF message. If no local gateway with the specified tech-prefix is found, the gatekeeper sends an LRJ message.

If the destination zone is local, the destination address is not registered, there is no matching tech-prefix, and no default tech-prefix is set, the gatekeeper sends an LRJ message.

Gatekeeper Call Routing Examples

These examples show some different gatekeeper call routing scenarios.



Gatekeeper Call Routing: Zone Prefixes and Default Technology Prefixes

1. ARQ to 13035554001
2. Technolgy prefix match? No
3. Zone prefix match? Yes
4. Target zone = DEN
5. Is DEN a local zone? Yes
6. 13035554001 registered? No
7. Was a technology prefix found? No
8. Default technology prefix set? 1#
9. Select a gateway in DEN with technology prefix 1#.
10. ACF, destination Gateway A

CVOICE v6.0—5-30

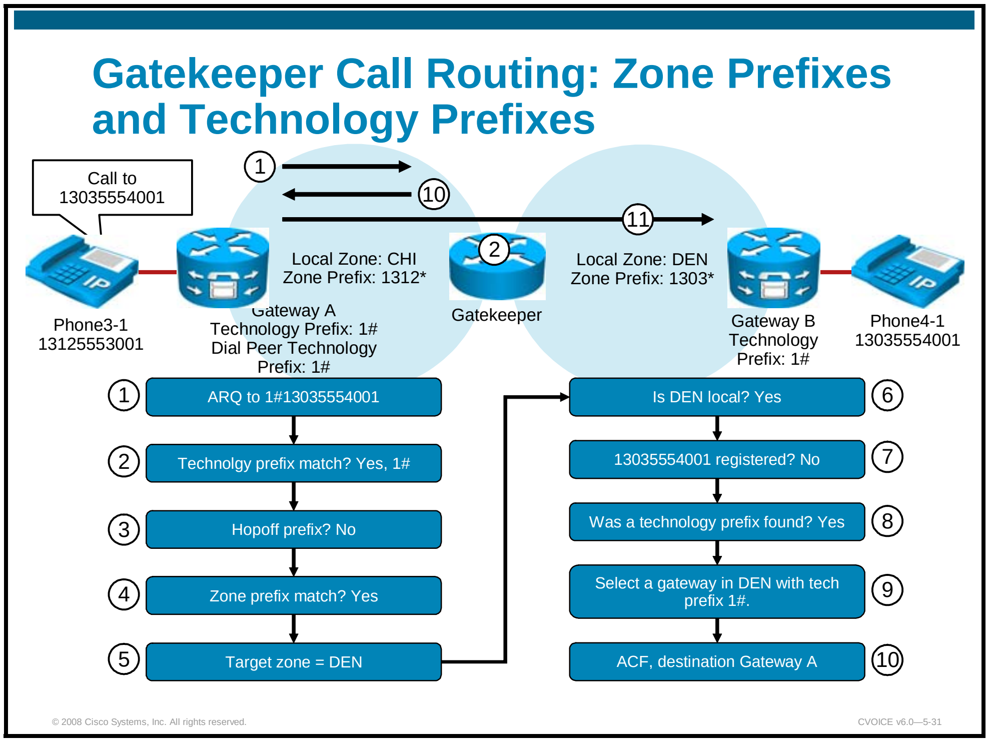
This figure shows a gatekeeper call routing configuration with zone prefixes and default technology prefixes:

- Gatekeeper:
  - Local Zone: Chicago (CHI); Zone Prefix: 1312*
  - Local Zone: Denver (DEN); Zone Prefix: 1303*
  - Default tech-prefix: 1#
- Gateway A tech-prefix: 1#
- Gateway B tech-prefix: 1#

These steps describe the gatekeeper call routing process:

1. Phone 3-1 dials 13035554001 to reach Phone 4-1, and Gateway A sends an ARQ message to the gatekeeper.
2. The gatekeeper checks whether the dialed number includes a tech-prefix. No tech-prefix is matched.
3. The zone prefix 1303 is matched.
4. Due to the zone prefix, the gatekeeper knows where to route the call. In this case, the call is routed to the DEN zone.
5. There is a local configured zone on the gatekeeper for the DEN zone.
6. The dialed number, 13035554001, is not registered locally.

7. No tech-prefix is found in the dialed number.
8. A default tech-prefix is found in the gatekeeper configuration.
9. Gateway B is registered with a tech-prefix of 1# at the gatekeeper, which is also the default tech-prefix at the gatekeeper. The gatekeeper selects the gateway in the DEN zone (Gateway B) with the tech-prefix 1# for call routing.
10. The gatekeeper sends an ACF message with the Gateway B-to-Gateway A destination.
11. The call takes place.



Gatekeeper Call Routing: Zone Prefixes and Technology Prefixes

Call to 13035554001
Phone3-1 13125553001
Gateway A Technology Prefix: 1# Dial Peer Technology Prefix: 1#
Local Zone: CHI Zone Prefix: 1312*
Gatekeeper
Local Zone: DEN Zone Prefix: 1303*
Gateway B Technology Prefix: 1#
Phone4-1 13035554001
1
10
11
2

1. ARQ to 1#13035554001
2. Technolgy prefix match? Yes, 1#
3. Hopoff prefix? No
4. Zone prefix match? Yes
5. Target zone = DEN
6. Is DEN local? Yes
7. 13035554001 registered? No
8. Was a technology prefix found? Yes
9. Select a gateway in DEN with tech prefix 1#.
10. ACF, destination Gateway A

This figure shows a gatekeeper call routing configuration with zone and tech-prefixes:

- Gatekeeper:
  - Local Zone: CHI; Zone Prefix: 1312*
  - Local Zone: DEN; Zone Prefix: 1303*
- Gateway A:
  - Tech-prefix: 1#
  - Dial peer configured with a tech-prefix: 1#
- Gateway B tech-prefix: 1#

This is the gatekeeper call routing process:

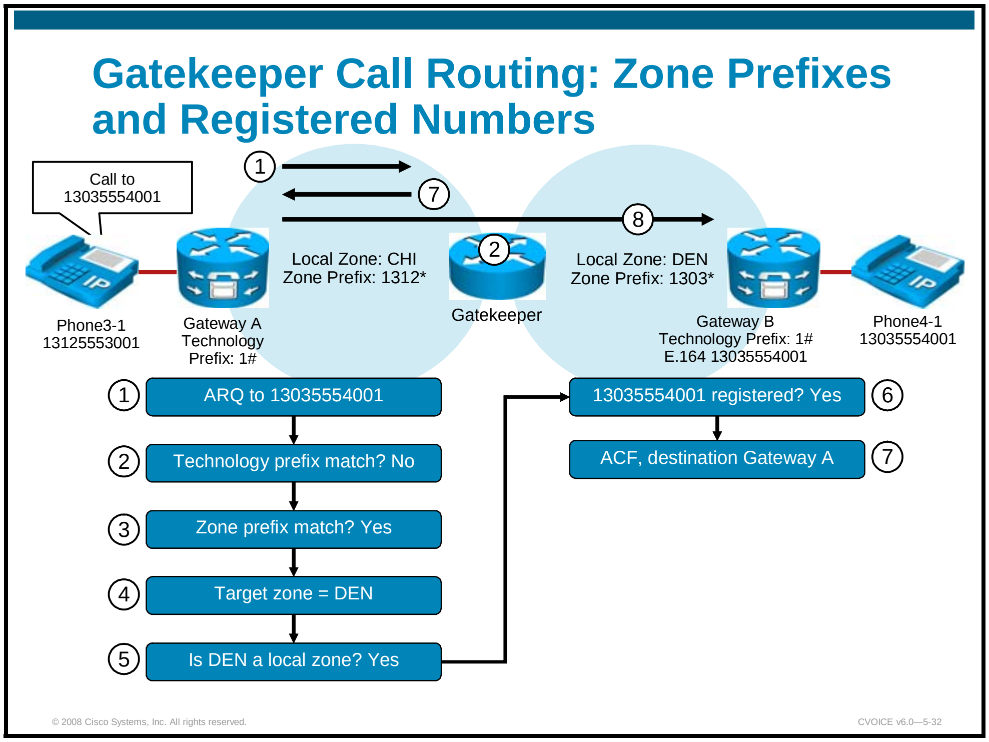
1. Phone 3-1 dials 13035554001 to reach Phone 4-1. Gateway A prefixes 1# to the dialed number and sends an ARQ message to the gatekeeper.
2. The gatekeeper checks if the dialed number includes a tech-prefix. Tech-prefix 1# is matched.
3. The gatekeeper checks whether the tech-prefix is a hopoff prefix. In this example, no hopoff is configured.
4. The zone prefix 1303 is matched.
5. Due to the zone prefix, the gatekeeper knows where to route the call. In this case, the call is routed to the DEN zone.
6. For this configuration, the DEN zone is a local configured zone on the gatekeeper, so the gatekeeper checks if the number is registered at the gatekeeper.
7. The dialed number, 13035554001, is not registered locally.

8. A default tech-prefix is found in the gatekeeper configuration.

9. Gateway B is registered with a tech-prefix of 1# at the gatekeeper, which is also the tech-prefix for the called number 1#13035554001. The gatekeeper selects the gateway in the DEN zone (Gateway B) with the tech-prefix 1# for call routing.

10. The gatekeeper sends an ACF message with the Gateway B-to-Gateway A destination.

11. The call takes place.



Gatekeeper Call Routing: Zone Prefixes and Registered Numbers

1. ARQ to 13035554001
2. Technology prefix match? No
3. Zone prefix match? Yes
4. Target zone = DEN
5. Is DEN a local zone? Yes
6. 13035554001 registered? Yes
7. ACF, destination Gateway A

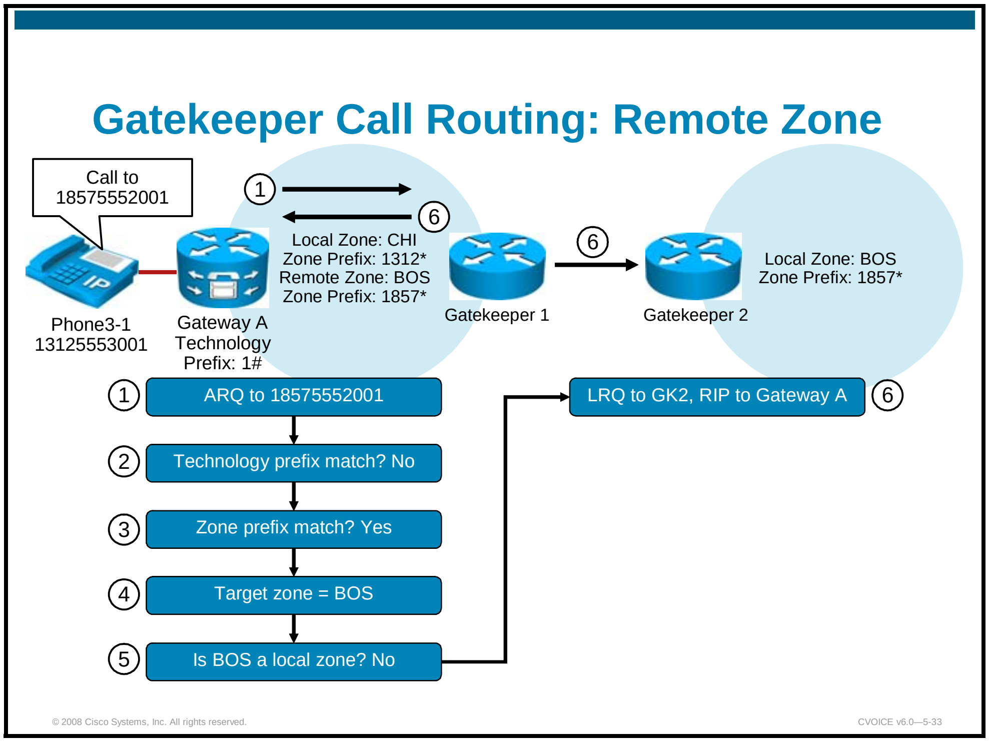
CVOICE v6.0—5-32

This figure shows a gatekeeper call routing configuration with zone prefixes and registered numbers:

- Gatekeeper:
  - Local Zone: CHI; Zone Prefix: 1312*
  - Local Zone: DEN: Zone Prefix: 1303*
- Gateway A tech-prefix 1#
- Gateway B:
  - Tech-prefix: 1#
  - E.164 number registered at the gatekeeper: 13035554001

This is the gatekeeper call routing process:

1. Phone 3-1 dials 13035554001 to reach Phone 4-1. Gateway A sends an ARQ message to the gatekeeper.
2. The gatekeeper checks if the dialed number includes a tech-prefix. No tech-prefix is matched.
3. The zone prefix 1303 is matched.
4. Due to the zone prefix, the gatekeeper where to route the call. In this case, the call is routed to the DEN zone.
5. For this configuration, the DEN zone is a local configured zone on the gatekeeper, so the gatekeeper checks if the number is registered at the gatekeeper. In the example, the number is registered locally on the gatekeeper.
6. The dialed number, 13035554001, is registered locally.
7. The gatekeeper sends an ACF message with the Gateway B-to-Gateway A destination.



Gatekeeper Call Routing: Remote Zone

Call to 18575552001

Phone3-1 13125553001

Gateway A Technology Prefix: 1#

Local Zone: CHI
Zone Prefix: 1312*
Remote Zone: BOS
Zone Prefix: 1857*

Gatekeeper 1

Gatekeeper 2

Local Zone: BOS
Zone Prefix: 1857*

1. ARQ to 18575552001
2. Technology prefix match? No
3. Zone prefix match? Yes
4. Target zone = BOS
5. Is BOS a local zone? No
6. LRQ to GK2, RIP to Gateway A

CVOICE v6.0—5-33

This figure shows a gatekeeper call routing configuration with a remote zone:

- Gatekeeper 1:
  - Local Zone: CHI; Zone Prefix: 1312*
  - Remote Zone: Boston (BOS); Zone Prefix: 1857*
- Gateway A tech-prefix: 1#
- Gatekeeper 2 Local Zone: BOS; Zone Prefix: 1857*

This is the gatekeeper call routing process:

1. Phone 3-1 dials 18575552001 to reach a phone in a remote zone. Gateway A sends an ARQ message to the gatekeeper.

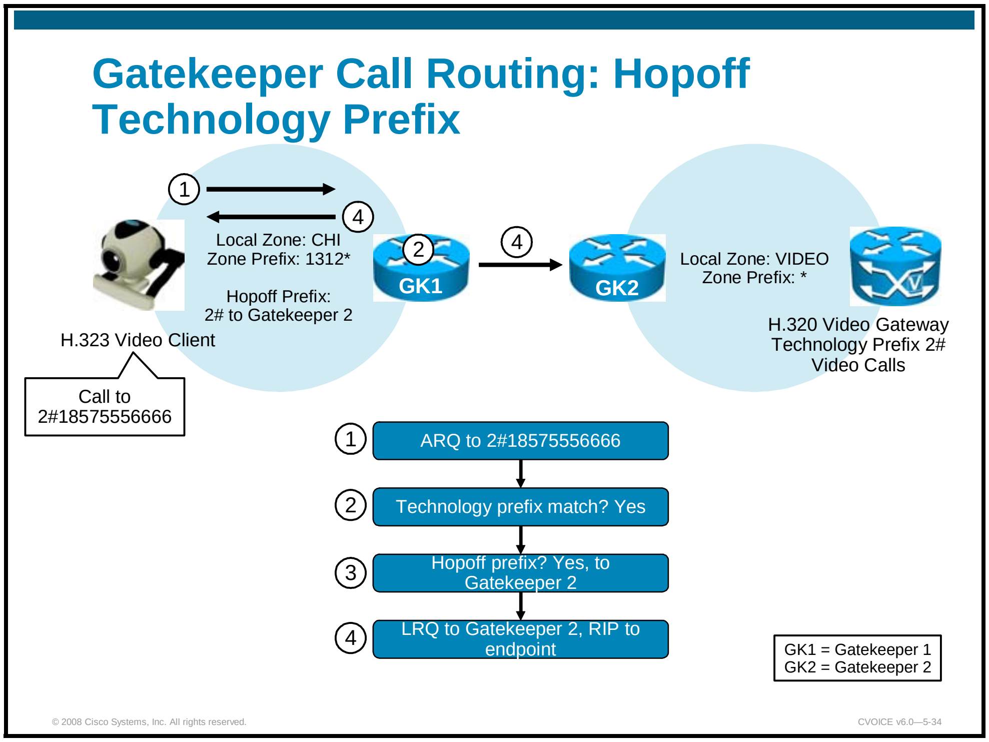
2. The gatekeeper checks if the dialed number includes a tech-prefix. No tech-prefix is matched.

3. The zone prefix 1857 is matched.

4. Due to the zone prefix, the gatekeeper knows where to route the call. In this case, the call is routed to the BOS zone.

5. The BOS zone is configured as a remote zone on the gatekeeper.

6. The gatekeeper sends a LRQ message to Gatekeeper 2 and an RIP message to Gateway A.



Gatekeeper Call Routing: Hopoff Technology Prefix

H.323 Video Client

Call to 2#18575556666

Local Zone: CHI
Zone Prefix: 1312*

Hopoff Prefix:
2# to Gatekeeper 2

GK1

GK2

Local Zone: VIDEO
Zone Prefix: *

H.320 Video Gateway
Technology Prefix 2#
Video Calls

1. ARQ to 2#18575556666
2. Technology prefix match? Yes
3. Hopoff prefix? Yes, to Gatekeeper 2
4. LRQ to Gatekeeper 2, RIP to endpoint

GK1 = Gatekeeper 1
GK2 = Gatekeeper 2

This figure shows a gatekeeper call routing configuration with a hopoff technology prefix:

- Gatekeeper 1:
  - Local Zone: CHI; Zone Prefix: 1312*
  - Hopoff prefix 2# to Gatekeeper 2
- Gatekeeper 2 Local Zone: Video; Zone Prefix: *
- H.320 video gateway tech-prefix: 2#

This is the gatekeeper call routing process:

1. An H.323 video client dials 2#18575556666. The video client is registered at the gatekeeper, so it sends the ARQ message for the number 2#18575556666 to the gatekeeper.

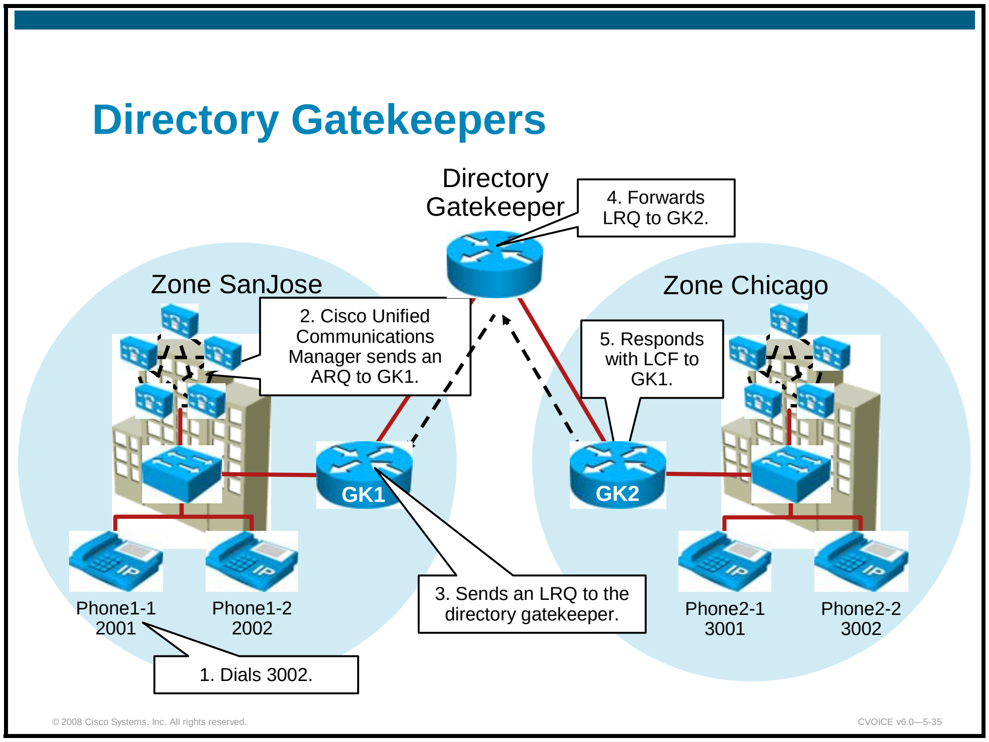
2. The gatekeeper checks if the dialed number includes a tech-prefix. Tech-prefix 2# is matching.

3. The tech-prefix is configured with a hop off prefix, which is pointing to Gatekeeper 2.

4. The gatekeeper sends an LRQ message to Gatekeeper 2 and an RIP message to the endpoint.

Directory Gatekeepers

This topic describes the functions of directory gatekeepers.



Directory Gatekeepers

1. Dials 3002.

2. Cisco Unified Communications Manager sends an ARQ to GK1.

3. Sends an LRQ to the directory gatekeeper.

4. Forwards LRQ to GK2.

5. Responds with LCF to GK1.

In a large network, configuring the prefixes of each zone on all of the gatekeepers can be time-consuming. A directory gatekeeper can be used to reduce the configuration steps on nondirectory gatekeepers in the network. LRQ forwarding allows a gatekeeper to be appointed as the directory gatekeeper or super gatekeeper. With this feature, it is only necessary to configure each gatekeeper with its own local zones and zone prefixes, and a single match-all wildcard prefix for the zone of the directory gatekeeper. Only the directory gatekeeper has to be configured with the full set of all zones and zone prefixes within the network.

A directory gatekeeper is basically a gatekeeper that forwards LRQ messages to other gatekeepers in search of E.164 resolution. These LRQ messages are triggered by other gatekeepers that need to know how to locate an E.164 address to process a call.

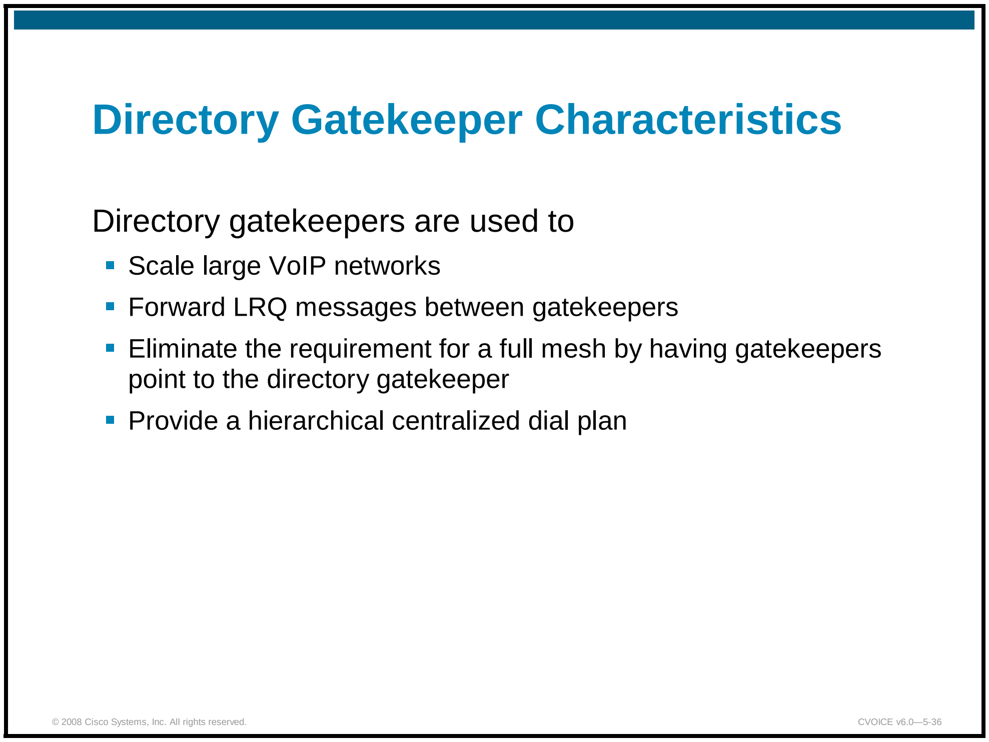
Additional Considerations for Using Directory Gatekeepers

When adding a directory gatekeeper to a network, consider these points:

- Using directory gatekeepers is a network design decision.
- Local zones and LRQ forwarding zones can be mixed.
- An LRQ from a gatekeeper that is not a Cisco gatekeeper cannot be forwarded.

Directory Gatekeeper Characteristics

This subtopic describes directory gatekeeper characteristics.



Directory Gatekeeper Characteristics

Directory gatekeepers are used to

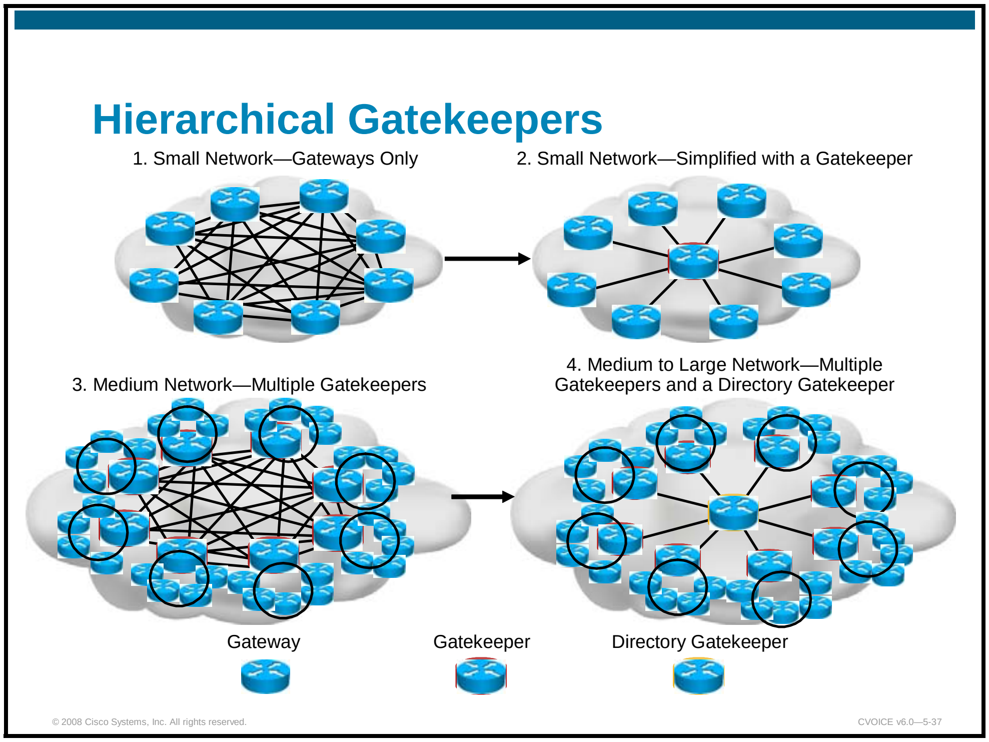
- Scale large VoIP networks
- Forward LRQ messages between gatekeepers
- Eliminate the requirement for a full mesh by having gatekeepers point to the directory gatekeeper
- Provide a hierarchical centralized dial plan

Gatekeepers keep track of other H.323 zones and forward calls appropriately. When many H.323 zones are present, gatekeeper configuration can become intensive in administrative terms. In large VoIP installations, you can use a centralized directory gatekeeper that contains a registry of all the different zones and coordinates LRQ-forwarding processes. In the case of directory gatekeepers, you no longer need a full-mesh configuration between interzone gatekeepers.

A directory gatekeeper is essentially a super gatekeeper that forwards LRQ messages. LRQ messages are RAS messages triggered by an ARQ message from endpoints that are forwarded from gatekeeper to gatekeeper. There is a limit of five hops for an LRQ message, which allows up to a four-tier gatekeeper hierarchy.

By using a directory gatekeeper, you no longer need a full mesh between gatekeepers, which is a major advantage. Directory gatekeepers centralize the dial plan and also serve as a potential interface to other centralized applications. In a large-scale VoIP network, a centralized interface point is required. This interface can interact with other applications and protocol suites, such as the Advanced Intelligent Network (AIN) in Signaling System 7 (SS7), GKTMP route servers, AAA, and so on.

Historically, directory gatekeepers were only used in large service provider wholesale deployments. Nowadays, directory gatekeepers are also used for large-scale enterprise. For example, banks with a large number of Cisco Unified Communications Manager Express sites can use a directory gatekeeper to interconnect the Cisco Unified Communications Manager Express sites with each other.



Hierarchical Gatekeepers

1. Small Network—Gateways Only

2. Small Network—Simplified with a Gatekeeper

3. Medium Network—Multiple Gatekeepers

4. Medium to Large Network—Multiple Gatekeepers and a Directory Gatekeeper

Gateway

Gatekeeper

Directory Gatekeeper

CVOICE v6.0—5-37

Using hierarchical gatekeepers provides a significant advantage in terms of scaling.

This example shows four network deployments:

1. In the case of an H.323 network without gatekeepers, a fully meshed dial plan is required for each gateway. This necessitates a significant amount of administrative work. One solution is to use a gatekeeper as shown in diagram 2.

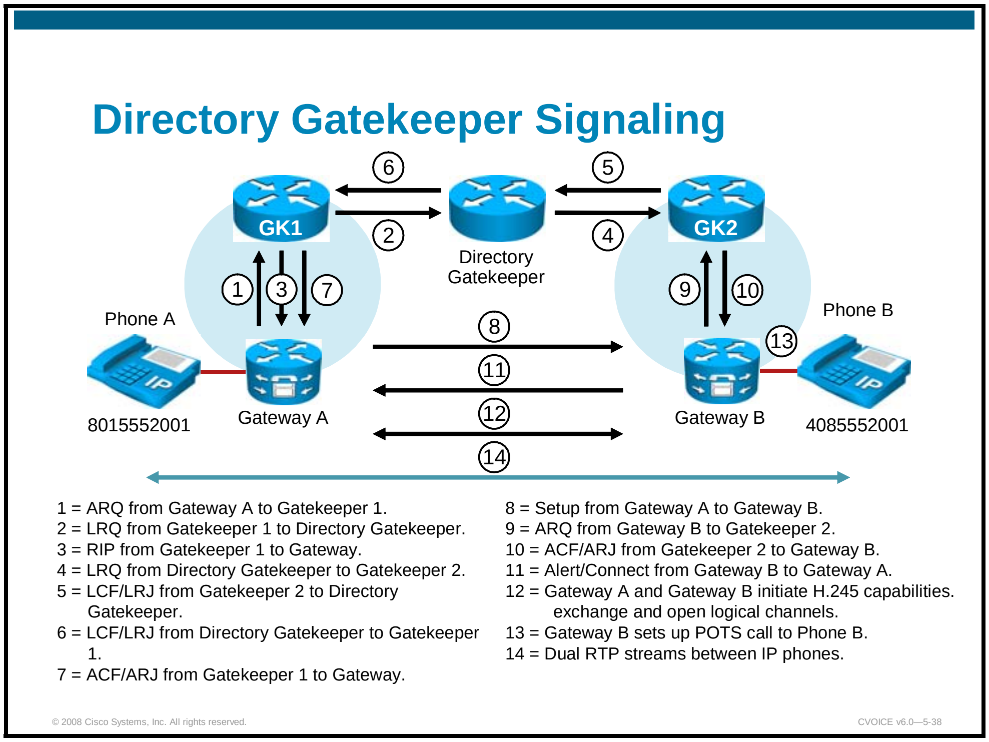
2. Gatekeepers enable a connection with each gateway in the network, thus providing a central location for the dial plan and no longer requiring a full-mesh configuration.

3. In a large network with multiple gatekeepers, a full mesh is again required between the gatekeepers to share dial plan information. When a number of H.323 zones are present, gatekeeper configuration can become administratively intensive.

4. In large VoIP installations, a centralized directory gatekeeper that contains a registry of all zones and coordinates LRQ forwarding can be used. This eliminates the need for a full-mesh configuration.

For example, a large telephone company might use a large number of gateways and may have one gatekeeper responsible for all the gateways in one city. Another level of centralization could use a centralized directory gatekeeper, sometimes called a super gatekeeper, to link multiple cities. This centralized gatekeeper could be an interface to intelligent route engines for dynamic route management, for example.

Redundancy is always an important issue to consider, but it is more important when you’re using a central device like a directory gatekeeper. If the directory gatekeeper shown in diagram 4 fails, the other gatekeepers no longer have access to the dial plan. The best solution is for full redundancy on all levels, including gateways, links, gatekeepers, directory gatekeepers, and all other correlating services. Redundant gatekeepers will be discussed later.



Directory Gatekeeper Signaling

1 = ARQ from Gateway A to Gatekeeper 1.
2 = LRQ from Gatekeeper 1 to Directory Gatekeeper.
3 = RIP from Gatekeeper 1 to Gateway.
4 = LRQ from Directory Gatekeeper to Gatekeeper 2.
5 = LCF/LRJ from Gatekeeper 2 to Directory Gatekeeper.
6 = LCF/LRJ from Directory Gatekeeper to Gatekeeper 1.
7 = ACF/ARJ from Gatekeeper 1 to Gateway.

8 = Setup from Gateway A to Gateway B.
9 = ARQ from Gateway B to Gatekeeper 2.
10 = ACF/ARJ from Gatekeeper 2 to Gateway B.
11 = Alert/Connect from Gateway B to Gateway A.
12 = Gateway A and Gateway B initiate H.245 capabilities. exchange and open logical channels.
13 = Gateway B sets up POTS call to Phone B.
14 = Dual RTP streams between IP phones.

CVOICE v6.0—5-38

The figure shows basic gateway and gatekeeper signaling between zones, but this time with a directory gatekeeper.

Phone A places a call to phone number 4085552001 for Phone B. Then this signaling process occurs:

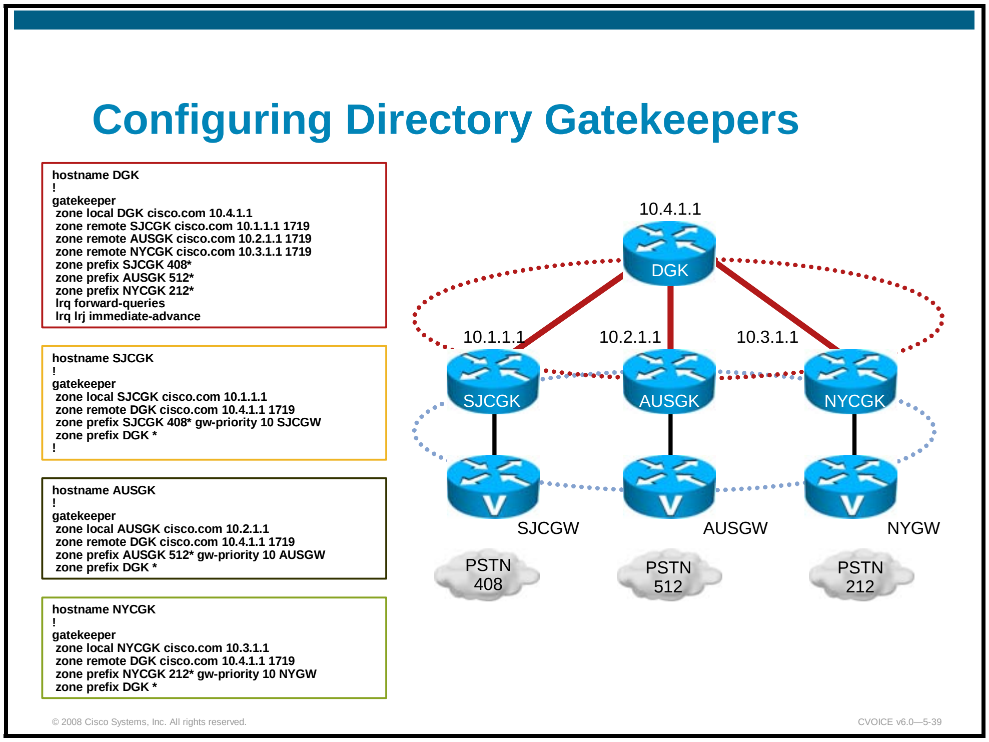
1. Gateway A sends an ARQ to Gatekeeper 1, asking permission to call Phone B.
2. Gatekeeper 1 does a look-up and does not find Phone B registered. Gatekeeper 1 does a prefix lookup and finds a wildcard match with the directory gatekeeper. Gatekeeper 1 sends an LRQ to the directory gatekeeper.
3. Gatekeeper 1 sends an RIP to Gateway A.
4. The directory gatekeeper does a prefix look-up and finds Gatekeeper 2. It forwards the LRQ to Gatekeeper 2.
5. Gatekeeper 2 does a look-up and finds Phone B registered. It returns an LCF with the IP address of Gateway B to the directory gatekeeper.
6. The directory gatekeeper returns an LCF to Gatekeeper 1.
7. Gatekeeper 1 returns an ACF with the IP address of Gateway B.
8. Gateway A sends a H.225 call setup message to Gateway B with the phone number of Phone B.
9. Gateway B sends an ARQ to Gatekeeper 2, asking permission to answer the call from Gateway A.
10. Gatekeeper 2 returns an ACF with the IP address of Gateway A to Gateway B.
11. Gateway B sends an alert and connect message Gateway A.
12. Gateway B and Gateway A initiate H.245 capability exchange and open logical channels.

13. Gateway B sets up a POTS call to Phone B at 4085552001.

14. Dual RTP streams are established between Gateway A and Gateway B.

Configuring Directory Gatekeepers

This topic describes a directory gatekeeper configuration.



Configuring Directory Gatekeepers

```
hostname DGK
!
gatekeeper
 zone local DGK cisco.com 10.4.1.1
 zone remote SJCGK cisco.com 10.1.1.1 1719
 zone remote AUSGK cisco.com 10.2.1.1 1719
 zone remote NYCGK cisco.com 10.3.1.1 1719
 zone prefix SJCGK 408*
 zone prefix AUSGK 512*
 zone prefix NYCGK 212*
 lrq forward-queries
 lrq lrj immediate-advance
```

```
hostname SJCGK
!
gatekeeper
 zone local SJCGK cisco.com 10.1.1.1
 zone remote DGK cisco.com 10.4.1.1 1719
 zone prefix SJCGK 408* gw-priority 10 SJCGW
 zone prefix DGK *
!
```

```
hostname AUSGK
!
gatekeeper
 zone local AUSGK cisco.com 10.2.1.1
 zone remote DGK cisco.com 10.4.1.1 1719
 zone prefix AUSGK 512* gw-priority 10 AUSGW
 zone prefix DGK *
```

```
hostname NYCGK
!
gatekeeper
 zone local NYCGK cisco.com 10.3.1.1
 zone remote DGK cisco.com 10.4.1.1 1719
 zone prefix NYCGK 212* gw-priority 10 NYGW
 zone prefix DGK *
```

CVOICE v6.0—5-39

The configuration of a directory gatekeeper is fairly straightforward. The example above details a typical directory gatekeeper configuration.

Directory Gatekeeper Configuration

Complete the following tasks:

1. Create a single local zone on the directory gatekeeper with a local address.

2. Create remote zones for each gatekeeper controlled by this directory gatekeeper with the addresses of remote gatekeepers.

3. Specify zone prefixes for the remote gatekeepers.

4. Enable forwarding of the location request.

Individual Gatekeeper Configuration

Complete the following tasks:

1. Create a single local zone on the gatekeeper with a local address.

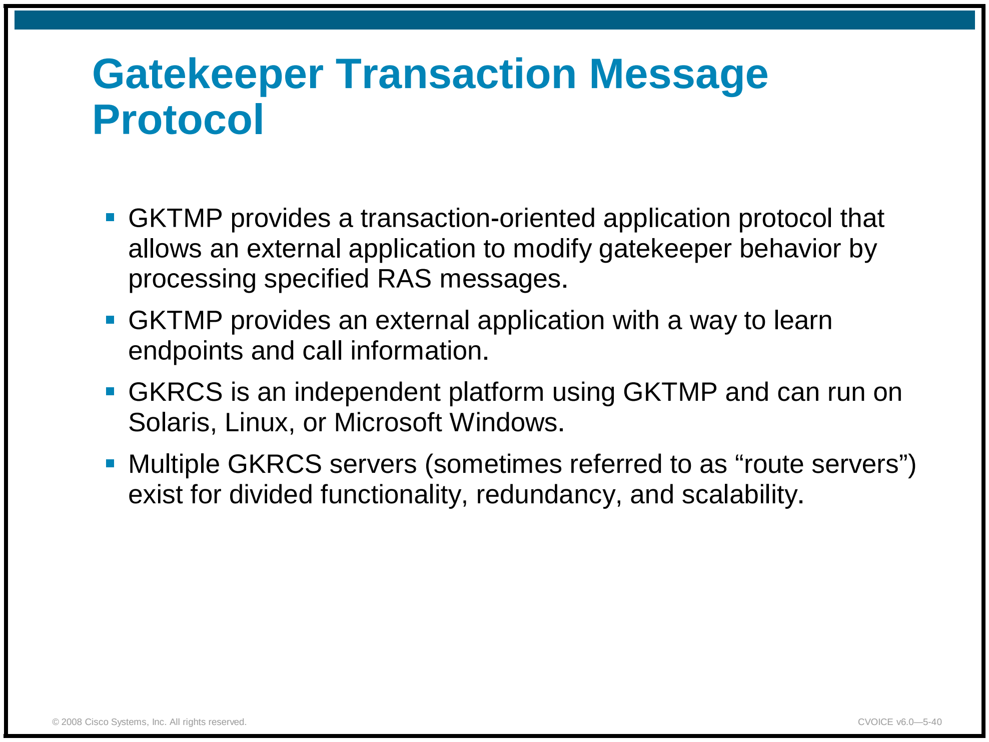
2. Create a remote zone for the directory gatekeeper with the addresses of the directory gatekeeper.

3. Specify a zone prefix to register with the directory gatekeeper.

4. Specify the zone prefix of the directory gatekeeper.

Gatekeeper Transaction Message Protocol

This topic describes the function of the GKTMP.

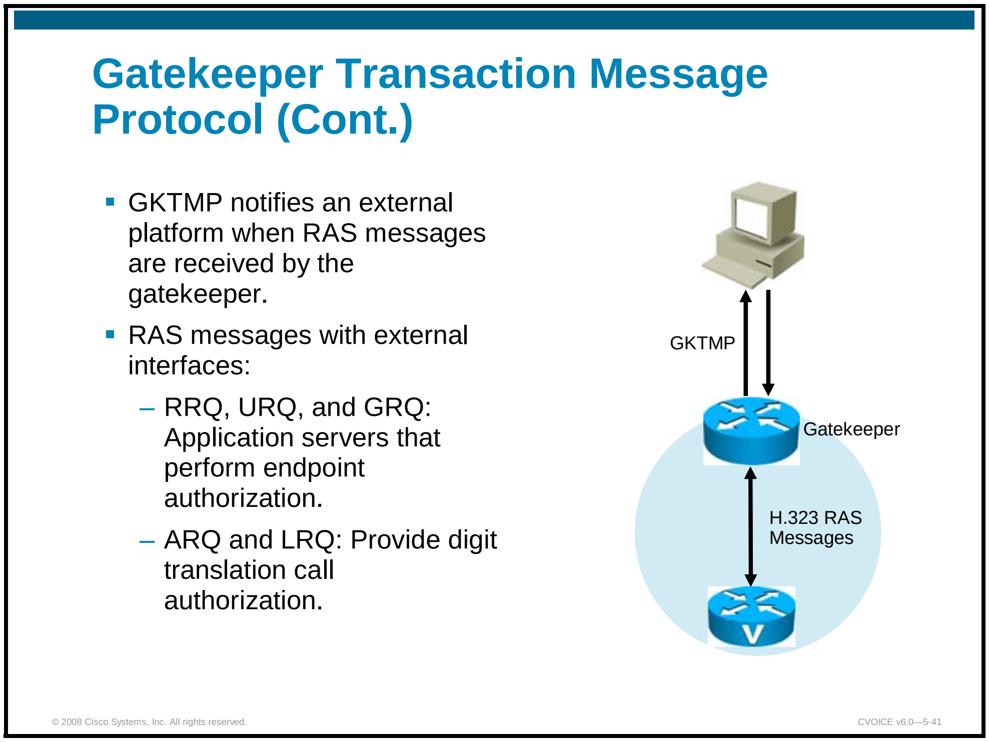


Gatekeeper Transaction Message Protocol

- GKTMP provides a transaction-oriented application protocol that allows an external application to modify gatekeeper behavior by processing specified RAS messages.
- GKTMP provides an external application with a way to learn endpoints and call information.
- GKRCS is an independent platform using GKTMP and can run on Solaris, Linux, or Microsoft Windows.
- Multiple GKRCS servers (sometimes referred to as “route servers”) exist for divided functionality, redundancy, and scalability.

GKTMP can extend the call control intelligence of a gatekeeper by providing an interface to a route application server where advanced routing decisions can be made. It converts incoming RAS messages to text messages and sends them to an off-board server. The server can override default gatekeeper behavior.

Gatekeeper Route Control Server (GKRCS) is an independent platform using GKTMP and can run on Solaris, Linux, or Microsoft Windows NT. An example of the use of GKTMP is where a service provider wants to control the call routing behavior of certain calls during a certain time of the day. The gatekeeper in this case will offload the routing instructions to the route application server and process the request from the server for altered call routing behavior.



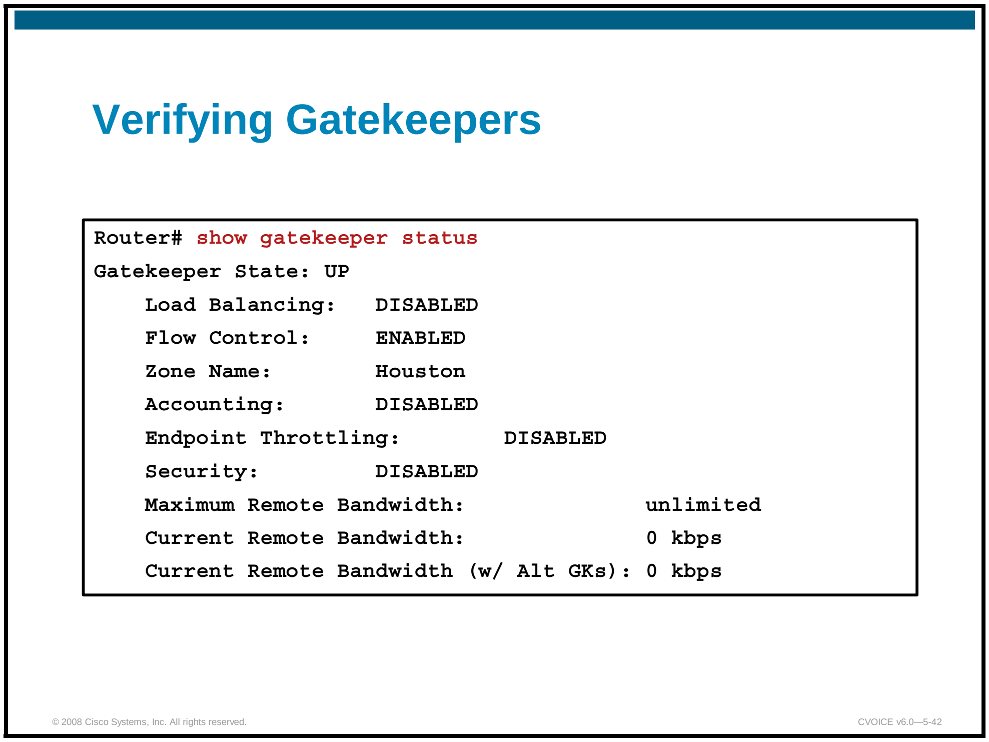
Gatekeeper Transaction Message Protocol (Cont.)

- GKTMP notifies an external platform when RAS messages are received by the gatekeeper.
- RAS messages with external interfaces:
  - RRQ, URQ, and GRQ: Application servers that perform endpoint authorization.
  - ARQ and LRQ: Provide digit translation call authorization.

GKTMP notifies an external platform (Solaris, Linux, or Microsoft) when a gatekeeper receives RAS messages like RRQ, URQ, and GRQ when performing endpoint authorization by an application server, or ARQ and LRQ messages for digit translation and call authorization.

Verifying Gatekeepers

This topic describes how to verify gatekeeper operation.

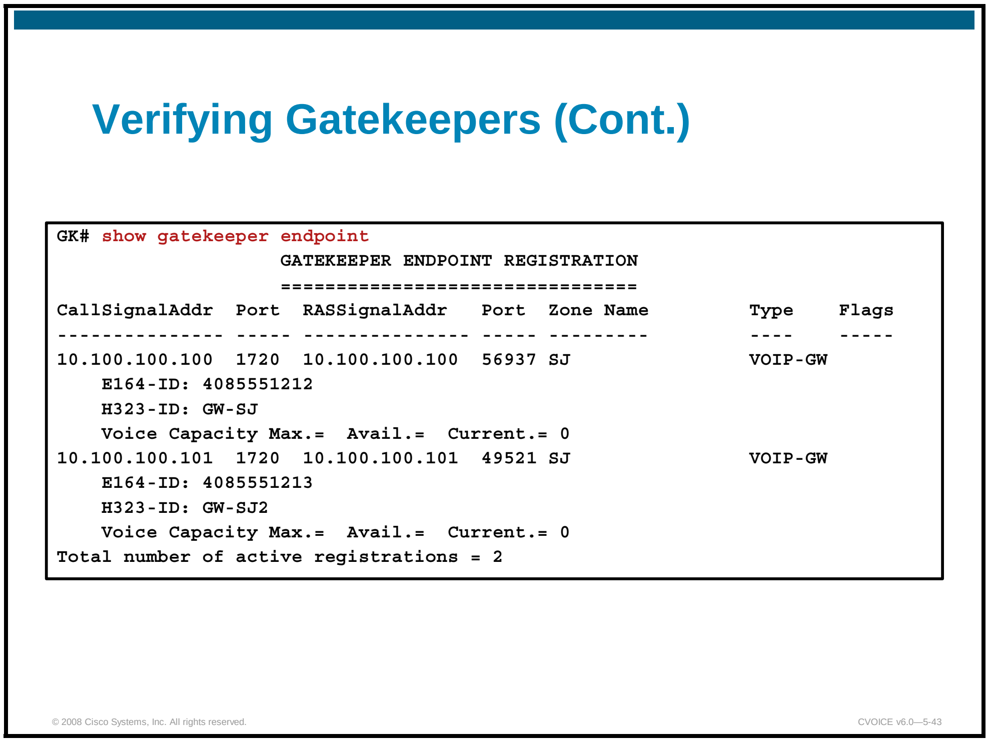


Verifying Gatekeepers

```
Router# show gatekeeper status
Gatekeeper State: UP
    Load Balancing:   DISABLED
    Flow Control:     ENABLED
    Zone Name:        Houston
    Accounting:       DISABLED
    Endpoint Throttling:        DISABLED
    Security:         DISABLED
    Maximum Remote Bandwidth:             unlimited
    Current Remote Bandwidth:             0 kbps
    Current Remote Bandwidth (w/ Alt GKs): 0 kbps
```

CVOICE v6.0—5-42

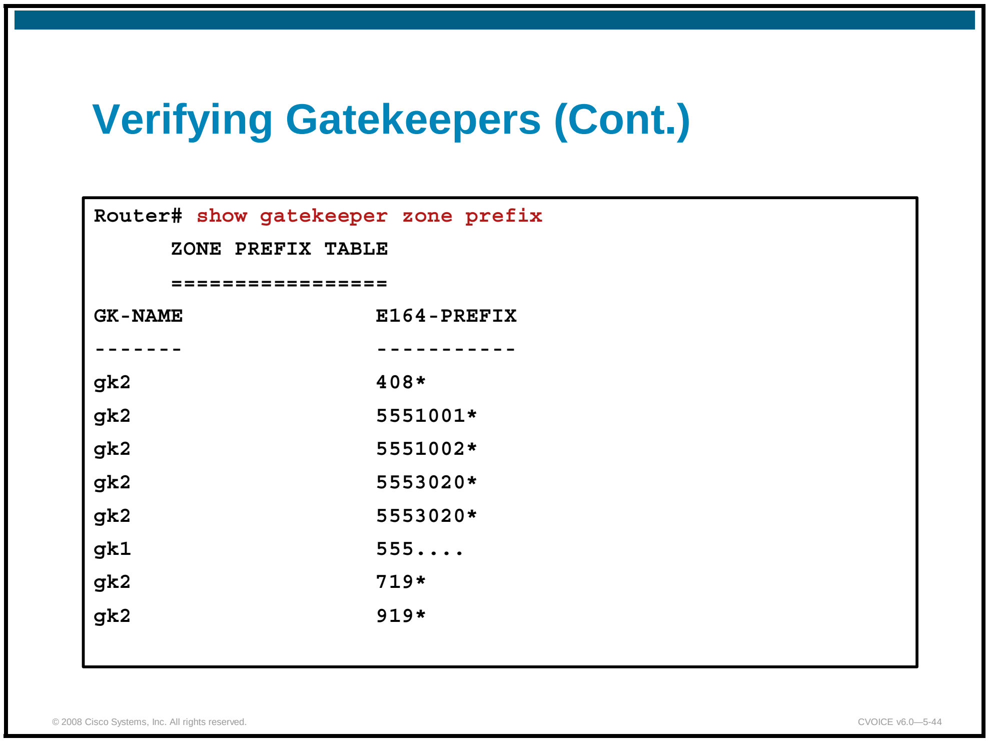
Use the **show gatekeeper status** command to display overall gatekeeper status, including authorization and authentication status and zone status.



Verifying Gatekeepers (Cont.)

```
GK# show gatekeeper endpoint
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type    Flags
--------------- ----- --------------- ----- ---------         ----    -----
10.100.100.100  1720  10.100.100.100  56937 SJ                VOIP-GW
    E164-ID: 4085551212
    H323-ID: GW-SJ
    Voice Capacity Max.=  Avail.=  Current.= 0
10.100.100.101  1720  10.100.100.101  49521 SJ                VOIP-GW
    E164-ID: 4085551213
    H323-ID: GW-SJ2
    Voice Capacity Max.=  Avail.=  Current.= 0
Total number of active registrations = 2
```

The **show gatekeeper endpoint** command displays the gateways that have registered to a gatekeeper.

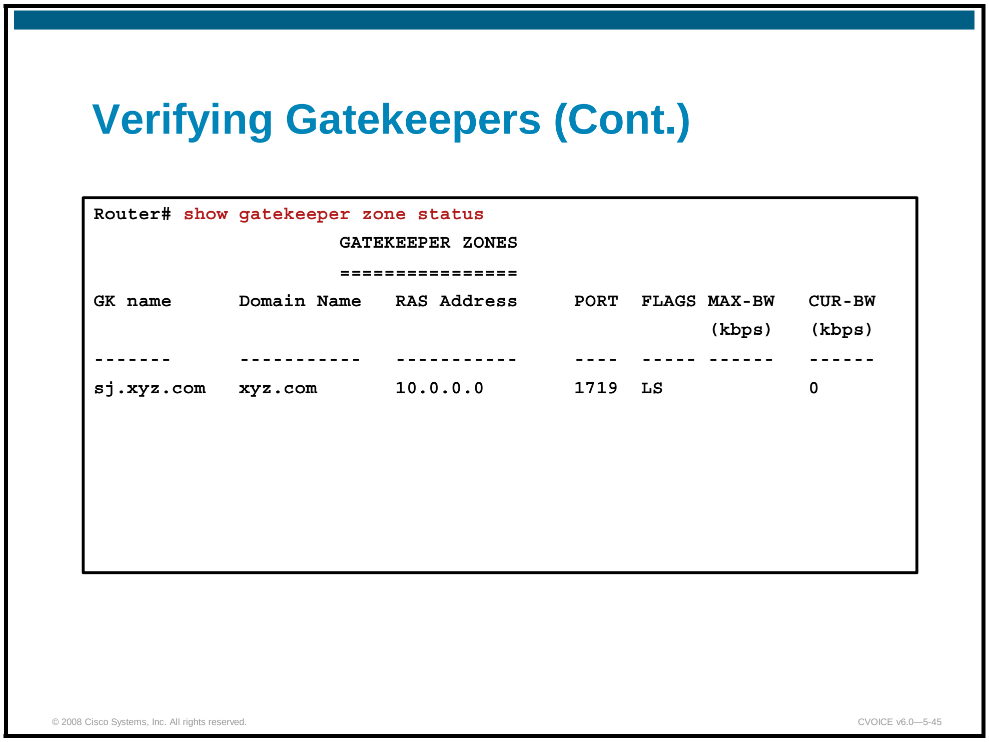


Verifying Gatekeepers (Cont.)

```
Router# show gatekeeper zone prefix
      ZONE PREFIX TABLE
      =================
GK-NAME                 E164-PREFIX
-------                 -----------
gk2                     408*
gk2                     5551001*
gk2                     5551002*
gk2                     5553020*
gk2                     5553020*
gk1                     555....
gk2                     719*
gk2                     919*
```

CVOICE v6.0—5-44

Use the **show gatekeeper zone prefix** command to display the zone prefix table for the gatekeeper.



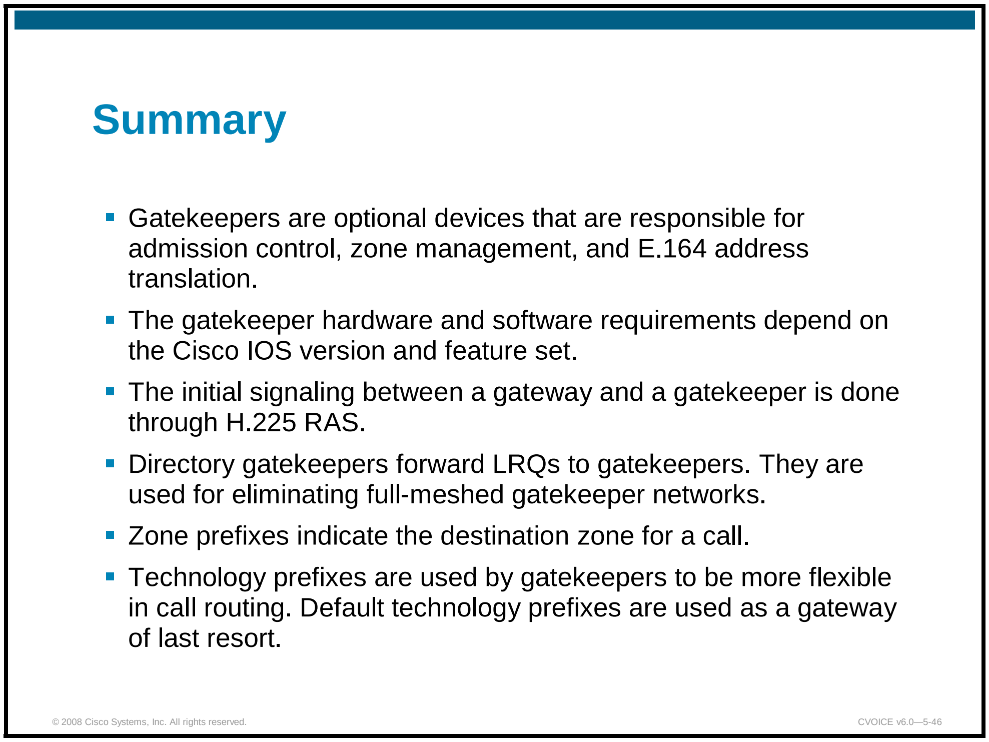
Verifying Gatekeepers (Cont.)

```
Router# show gatekeeper zone status
                      GATEKEEPER ZONES
                      ================
GK name      Domain Name    RAS Address     PORT  FLAGS MAX-BW   CUR-BW
                                                        (kbps)   (kbps)
-------      -----------    -----------     ----  ----- ------   ------
sj.xyz.com   xyz.com        10.0.0.0        1719  LS             0
```

Use the **show gatekeeper zone status** command to display the status of zones related to a gatekeeper.

Summary

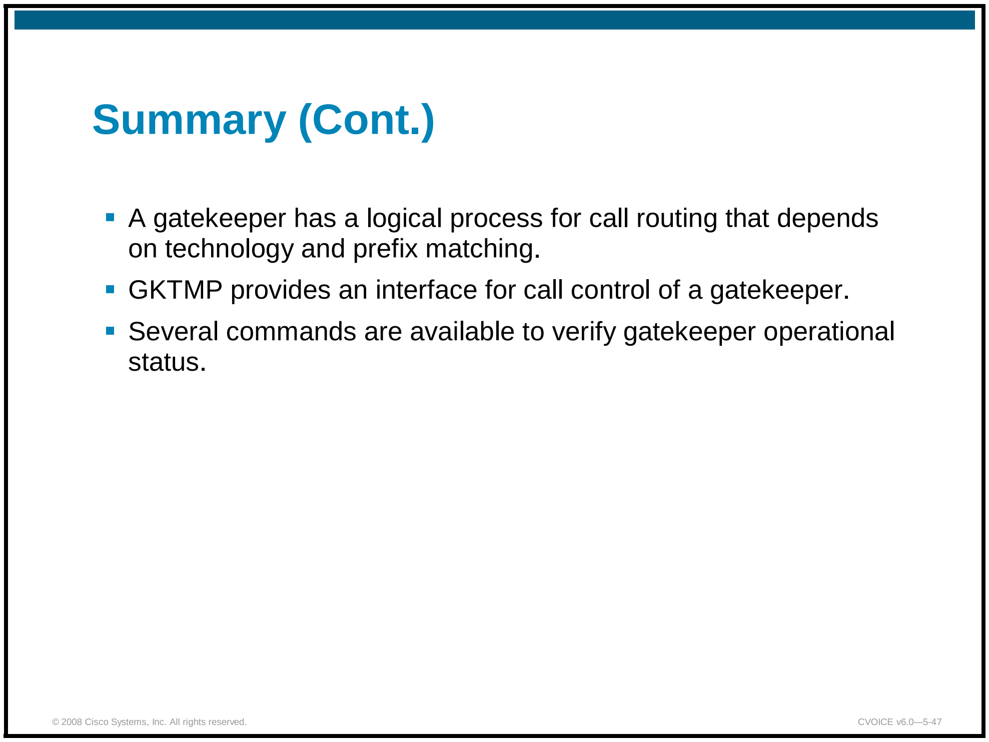
This topic summarizes the key points that were discussed in this lesson.



Summary

- Gatekeepers are optional devices that are responsible for admission control, zone management, and E.164 address translation.
- The gatekeeper hardware and software requirements depend on the Cisco IOS version and feature set.
- The initial signaling between a gateway and a gatekeeper is done through H.225 RAS.
- Directory gatekeepers forward LRQs to gatekeepers. They are used for eliminating full-meshed gatekeeper networks.
- Zone prefixes indicate the destination zone for a call.
- Technology prefixes are used by gatekeepers to be more flexible in call routing. Default technology prefixes are used as a gateway of last resort.

CVOICE v6.0—5-46



Summary (Cont.)

- A gatekeeper has a logical process for call routing that depends on technology and prefix matching.
- GKTMP provides an interface for call control of a gatekeeper.
- Several commands are available to verify gatekeeper operational status.

CVOICE v6.0—5-47

Lesson Self-Check

Use the questions here to review what you learned in this lesson. The correct answers and solutions are found in the Lesson Self-Check Answer Key.

Q1) Two primary functions of a gatekeeper are ____________________ and ___________________. (Select two.)

Relates to: Gatekeeper Overview

Q2) Gatekeeper hardware and software requirements depend on the Cisco ____________ version and feature set.

Relates to: Gatekeeper Hardware and Software Requirements

A) router
B) switch
C) IOS
D) gateway

Q3) RAS is a subset of ________ signaling protocol.

Relates to: Gatekeeper Signaling

Q4) Zone prefixes are usually used to associate a(n) _______________ to a configured zone.

Relates to: Zone Prefixes

A) IP address
B) gatekeeper
C) area code
D) endpoint

Q5) Gatekeepers use tech-prefixes to route calls when there is no ____________________ registered (by a gateway) that matches the called number.

Relates to: Technology Prefixes

Q6) A gatekeeper has a logical process for call routing that depends on technology and _________ prefix matching.

Relates to: Gatekeeper Call Routing

Q7) Directory gatekeepers forward _______ to gatekeepers.

Relates to: Directory Gatekeepers

Q8) GKTMP converts incoming RAS messages to _______ messages and sends them to an off-board server.

Relates to: Gatekeeper Transactional Message Protocol

Lesson Self-Check Answer Key

Q1)	zone management, admission control
Q2)	C
Q3)	H.225
Q4)	C
Q5)	E.164 address
Q6)	zone
Q7)	LRQs
Q8)	text

Lesson 2

Configuring Basic Gatekeeper Functionality

Overview

In this lesson, you will learn how to configure basic gatekeeper functionality. You will learn how to configure gatekeepers and Cisco Unified Communications Manager to operate together. You will also learn how to configure gateways to register with a gatekeeper.

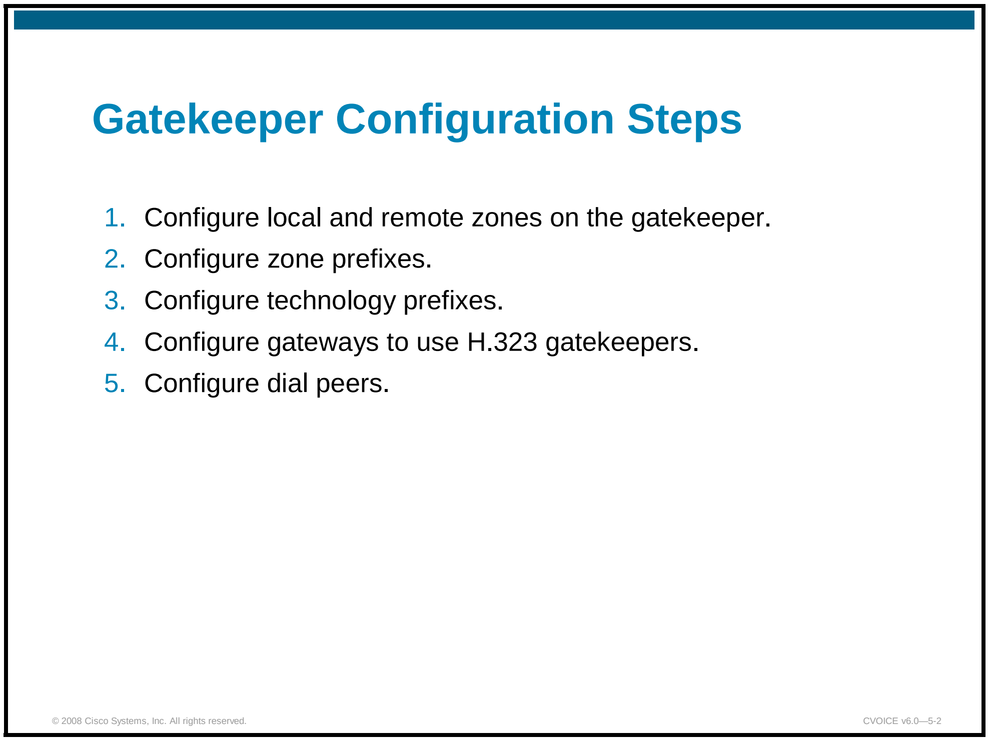
Objectives

Upon completing this lesson, you will be able to configure gatekeepers for device registration, address resolution, and call routing. This ability includes being able to meet these objectives:

- List the steps necessary to configure a multizone gatekeeper for local and remote zone call routing
- Configure local and remote zones on a gatekeeper
- Configure zone prefixes on a gatekeeper
- Configure technology prefixes
- Configure gateways to register with a gatekeeper
- Configure dial peers for gatekeepers
- Verify that H.323 endpoints are registered properly and calls are correctly routed across a single gatekeeper

Gatekeeper Configuration Steps

This topic lists the steps necessary to configure a gatekeeper for local and remote zone call routing.



Gatekeeper Configuration Steps

1. Configure local and remote zones on the gatekeeper.
2. Configure zone prefixes.
3. Configure technology prefixes.
4. Configure gateways to use H.323 gatekeepers.
5. Configure dial peers.

CVOICE v6.0—5-2

These are the basic steps necessary to configure a Cisco IOS gatekeeper and gateways:

Step 1 Configure local and remote zones on the gatekeeper.

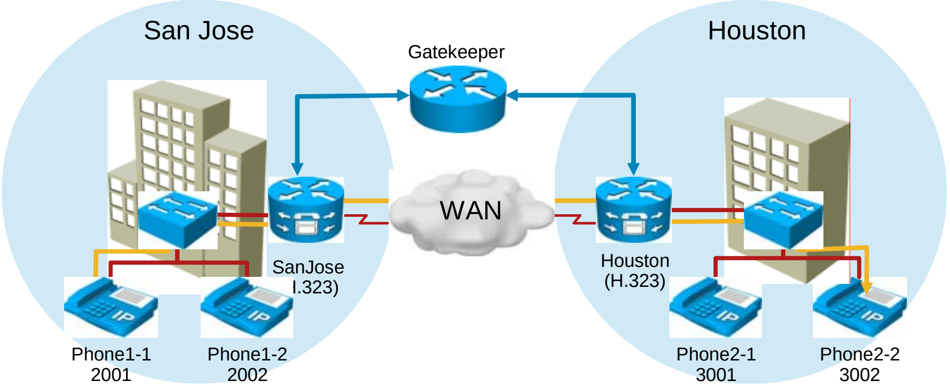
Step 2 Configure zone prefixes for all zones where calls should be routed.

Step 3 Configure technology prefixes to provide more flexibility in call routing.

Step 4 Configure gateways to use H.323 gatekeepers.

Step 5 Configure dial peers.

Single Gatekeeper—Multizone Configuration Scenario



CVOICE v6.0—5-3

This figure shows a common topology where a single device (which in this scenario is the gatekeeper) manages multiple zones. There can be only one gatekeeper controlling a zone at any time. The San Jose gateway is registered with the gatekeeper in the San Jose zone and the Houston gateway is registered in the Houston zone with the gatekeeper. The gatekeeper is responsible for call resolution, Call Admission Control (CAC), and so on. After the call setup, the IP phones (which in this case are Phone 1-1 and Phone 2-2) are directly connected.

Gateway Selection Process

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 prohibit 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.

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 to use to complete a call.

Configuration Considerations

When configuring a gatekeeper, keep these things in mind:

- Multiple local zones can be defined. The gatekeeper manages all configured local zones. Intrazone behavior is between the gatekeeper and the endpoints and gateways within a specific zone. A gatekeeper can support more than one zone. Even though there is a single gatekeeper per local zone, the communication between zones is interzone. So, the same gatekeeper can support both intrazone and interzone communications.
- Only one **ras-***IP-address* argument can be defined for all local zones. You cannot configure each zone to use a different Registration, Admission, and Status (RAS) IP address. If you define this argument in the first zone, you can omit it for all subsequent zones, because they will automatically pick up this address. If you set it in a subsequent **zone local** command, it also changes the RAS address of all previously configured local zones. After the argument is defined, you can change it by reissuing any **zone local** command with a different **ras-***IP-address* argument.
- You cannot remove a local zone if there are endpoints or gateways registered in it. To remove the local zone, shut down the gatekeeper first; this forces the endpoints, gateways, and local zone to unregister.
- Multiple logical gatekeepers control the multiple zones on the same Cisco IOS platform.
- The maximum number of local zones defined in a gatekeeper should not exceed 100.

Basic Gatekeeper Configuration Commands

The following is a table of some basic gatekeeper configuration commands.

Basic Gatekeeper Configuration Commands

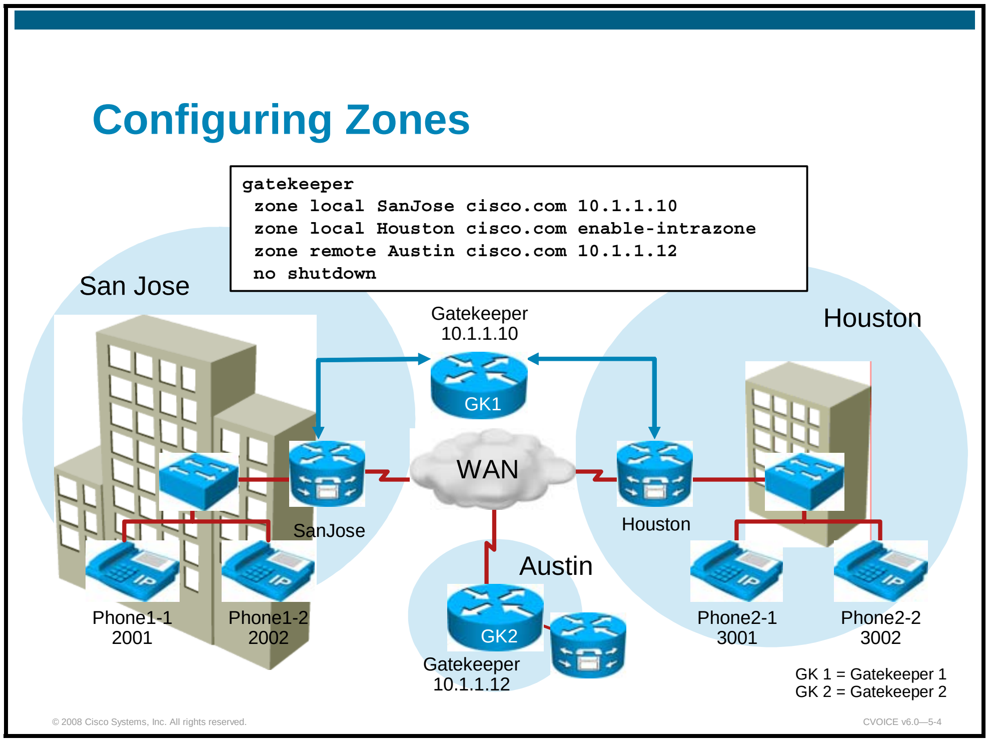
Command	Purpose
gatekeeper	Enters gatekeeper configuration mode.
zone local *gatekeeper-name domain-name* [*ras-IP-address*] [**invia** *inbound gatekeeper* | **outvia** *outbound gatekeeper* [**enable-intrazone**]]	Specifies a zone controlled by a gatekeeper. *gatekeeper-name*: Specifies the zone name. This is usually the fully domain-qualified host name of the gatekeeper. *domain-name*: Specifies the domain name served by this gatekeeper. *ras-IP-address*: (Optional) Specifies the IP address of one of the interfaces on the gatekeeper. When the gatekeeper responds to gatekeeper discovery messages, it signals the endpoint or gateway to use this address in future communications. **invia** *inbound gatekeeper:* Specifies the gatekeeper for calls entering this zone. **outvia** *outbound gatekeeper:* Specifies the gatekeeper for calls leaving this zone. **enable-intrazone**: Forces all intrazone calls to use the via-zone gatekeeper.
zone remote *other-gatekeeper-name other-domain-name other-gatekeeper-ip-address* [*port-number*] [**cost** *cost-value*	Statically specifies a remote zone if the Domain Name System (DNS) is unavailable or undesirable. *other-gatekeeper-name:* Name of the remote gatekeeper.

[**priority** *priority-value*]] [**foreign-domain**] [**invia** *inbound gatekeeper*] | [**outvia** *outbound gatekeeper*]	*other-domain-name*: Domain name of the remote gatekeeper. *other-gatekeeper-ip-address:* IP address of the remote gatekeeper. *port-number:* (Optional) RAS signaling port number for the remote zone. Range is from 1 to 65535. If the value is not set, the default is the well-known RAS port number 1719. **cost** *cost-value:* (Optional) Cost of the zone. Range is from 1 to 100. The default is 50. **priority** *priority-value:* (Optional) Priority of the zone. Range is from 1 to 100. The default is 50. **foreign-domain**: (Optional) Cluster is in a different administrative domain. **invia** *inbound gatekeeper:* Specifies the gatekeeper for calls entering this zone. **outvia** *outbound gatekeeper:* Specifies the gatekeeper for calls leaving this zone.
zone prefix *gatekeeper-name e164-prefix* **[blast | seq] [gw-priority** *priority gw-alias [gw-alias, ...]***]**	Adds a prefix to the gatekeeper zone list. The optional **blast** and **seq** parameters are for fault-tolerant gatekeeper networks. *gatekeeper-name e164-prefix:* Name of a local or remote gatekeeper, which must have been defined by using the **zone local** or **zone remote** command. *e164-prefix:* E.164 prefix in standard form followed by dots (.). Each dot represents a number in the E.164 address. **blast**: (Optional) If you list multiple hopoffs, this indicates that the Location Requests (LRQs) should be sent simultaneously to the gatekeepers based on the order in which they were listed. The default is **seq**. **seq**: (Optional) If you list multiple hopoffs, this indicates that the LRQs should be sent sequentially to the gatekeepers based on the order in which they were listed. **gw-priority** *priority gw-alias:* (Optional) Defines how the gatekeeper selects gateways in its local zone for calls to numbers beginning with prefix e164-prefix. Range is from 0 to 10, where 0 prevents the gatekeeper from using the gateway gw-alias for that prefix and 10 places the highest priority on the gateway gw-alias. The default is 5.
gw-type-prefix *type-prefix* [[**hopoff** *gkid1*] [**hopoff** *gkid2*] [**hopoff** *gkidn*] [**seq** | **blast**]] [**default-technology**] [[**gw ipaddr** *ipaddr* [*port*]]]	Configures a technology prefix (tech-prefix) in the gatekeeper. Tech-prefixes can be configured either on the gatekeeper or directly on the gateway. When using special flags (hopoff or default-technology), configure the prefix on the gatekeeper and on the gateway. *type-prefix:* A tech-prefix is recognized and is stripped before checking for the zone prefix. **hopoff** *gkid:* (Optional) Use this option to specify the gatekeeper where the call is to hop off, regardless of the zone prefix in the destination address. The gkid argument refers to a gatekeeper previously configured using the zone local or zone remote comment. **seq | blast**: Optional) If you list multiple hopoffs, this indicates that the LRQs should be sent sequentially or simultaneously (blast) to the gatekeepers according to the order in which they were listed.

	default-technology: (Optional) Gateways registering with this prefix option are used as the default for routing any addresses that are otherwise unresolved. **gw ipaddr** *ipaddr* [*port*]: (Optional) Use this option to indicate that the gateway is incapable of registering tech-prefixes. When it registers, it adds the gateway to the group for this type of prefix, just as if it had sent the tech-prefix in its registration.
`no shutdown`	Brings the gatekeeper online.

Configuring Gatekeeper Zones

This topic describes how to configure local and remote zones on a gatekeeper.



Configuring Zones

```
gatekeeper
 zone local SanJose cisco.com 10.1.1.10
 zone local Houston cisco.com enable-intrazone
 zone remote Austin cisco.com 10.1.1.12
 no shutdown
```

GK 1 = Gatekeeper 1
GK 2 = Gatekeeper 2

CVOICE v6.0—5-4

The figure shows the basic steps in configuring gatekeepers managing two local zones. The gatekeeper is configured for the two zones: San Jose and Houston.

Follow this procedure to configure zones on a gatekeeper:

Step 1 Enter gatekeeper configuration mode.

```
Router(config)# gatekeeper
```

Step 2 Specify a local zone to be controlled by the gatekeeper.

```
Router(config-gk)# zone local SanJose cisco.com 10.1.1.10
Router(config-gk)# zone local Houston cisco.com enable-intrazone
```

Note Setting this address for one local zone makes it the address used for all local zones.

Step 3 Specify a remote gatekeeper to which the local gatekeeper can send LRQs.

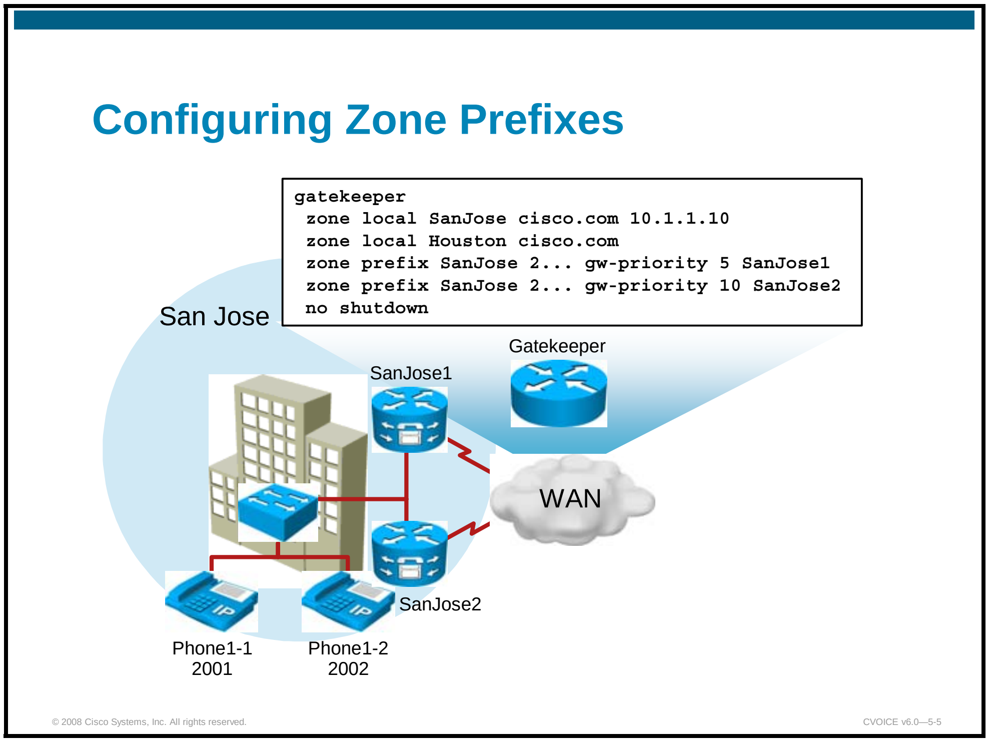
```
Router(config-gk)# zone remote Austin cisco.com 10.1.1.12
```

Step 4 Activate the gatekeeper.

```
Router(config-gk)# no shutdown
```

Configuring Zone Prefixes

This topic describes how to configure zone prefixes on a gatekeeper.



Configuring Zone Prefixes

```
gatekeeper
 zone local SanJose cisco.com 10.1.1.10
 zone local Houston cisco.com
 zone prefix SanJose 2... gw-priority 5 SanJose1
 zone prefix SanJose 2... gw-priority 10 SanJose2
 no shutdown
```

CVOICE v6.0—5-5

A zone prefix is a string of numbers that is used to associate a gateway to a dialed number in a zone. In this figure, the gatekeeper supports the 2… and 3… zone prefixes. The four digits are used by the gatekeeper for resolving the addresses. The San Jose and Houston sites will use these digits for dialing between the sites. The gateways in each zone register with either a 2 or 3 at the gatekeeper. This allows the gatekeeper to route the calls for a specific number range to the correct zone and gateway. Instead of using 2… and 3… for the zone prefix configuration, you could use 2* and 3* for the prefixes. The * symbol defines an endless number of digits. For example, a call to 24, 22224444, 2123, or 299999999999 would be routed to the designated gateway.

The figure above shows the gatekeeper configuration with 2… and 3… being used as the prefixes for each site respectively.

Complete these steps to configure zone prefixes on a gatekeeper:

Step 1 Enter gatekeeper configuration mode.

```
router(config)# gatekeeper
```

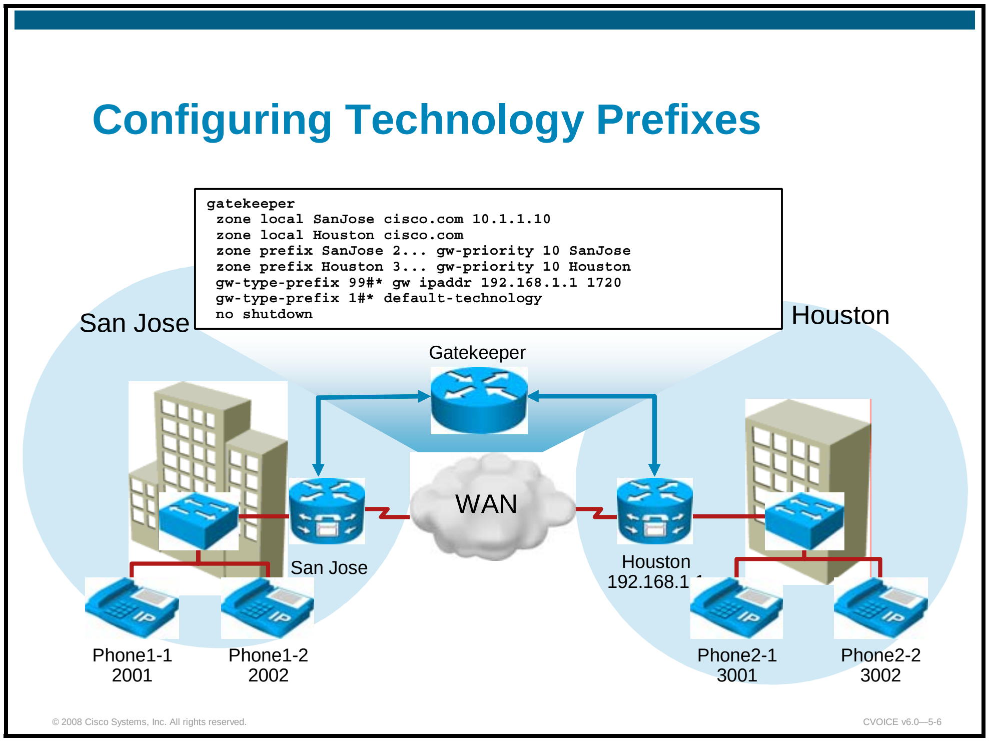
Step 2 Add a prefix to the gatekeeper zone list.

```
router(config-gk)# zone prefix SanJose 2... gw-priority 5
SanJose1
```

```
router(config-gk)# zone prefix SanJose 2... gw-priority 10
SanJose2
```

Configuring Technology Prefixes

This topic describes how to configure technology prefixes (tech-prefixes) on a gatekeeper.



Configuring Technology Prefixes

```
gatekeeper
 zone local SanJose cisco.com 10.1.1.10
 zone local Houston cisco.com
 zone prefix SanJose 2... gw-priority 10 SanJose
 zone prefix Houston 3... gw-priority 10 Houston
 gw-type-prefix 99#* gw ipaddr 192.168.1.1 1720
 gw-type-prefix 1#* default-technology
 no shutdown
```

© 2008 Cisco Systems, Inc. All rights reserved.

CVOICE v6.0—5-6

To enable the gatekeeper to select the appropriate hopoff gateway, use the **gw-type-prefix** command to configure technology- or gateway-type prefixes. Select tech-prefixes to denote different types or classes of gateways. The gateways are then configured to register with their gatekeepers using these tech-prefixes.

For example, voice gateways might register with tech-prefix 1#, and H.320 gateways might register with tech-prefix 2#. If there are several gateways of the same type, configure them to register with the same prefix type. By having several gateways register with the same prefix type, the gatekeeper treats the gateways as a pool out of which a random selection is made whenever a call for that prefix type arrives.

Callers will need to know the tech-prefixes that are defined and the type of device they are trying to reach. This enables them to prepend the appropriate tech-prefix to the destination address for the type of gateway needed to reach the destination.

Here is an example of how this command is used:

```
Router(config)# gw-type-prefix 1#* default-technology gw
ipaddr 172.16.1.1 1720
```

A tech-prefix is an optional H.323 standards-based feature that is supported by Cisco gateways and gatekeepers to enable more flexibility in call routing within an H.323 VoIP network. The network administrator selects tech-prefixes to denote different types or classes of gateways. The gateways are then configured to register with their gatekeepers with these prefixes. For example, voice gateways can register with tech-prefix 99#, H.320 gateways with technology prefix 2#, and voice-mail gateways with tech-prefix 3#. More than one gateway can register with the same type prefix. When this happens, the gatekeeper makes a random selection among gateways of the same type (if no zone prefixes are configured with **gw-priority**).

If callers know the type of device that they are trying to reach, they can include the tech-prefix in the destination address to indicate the type of gateway to use to get to the destination. For example, if a caller knows that address 2125551111 belongs to a regular telephone, the destination address of 99#2125551111 can be used, with 99# indicating that the address should be resolved by a voice gateway. When the voice gateway receives the call for 99#2125551111, it strips off the tech-prefix and bridges the next leg of the call to the telephone at 2125551111. The figure shows a configuration for a tech-prefix 99# and for a default tech-prefix 1#.

Additionally, when you use the **gw-type-prefix** command, you can define a specific gateway-type prefix as the default gateway type to be used for addresses that cannot be resolved. This also forces a technology prefix to always hop off in a particular zone.

If the majority of calls hop off on a particular type of gateway, you can configure the gatekeeper to use that type of gateway as the default type so that callers no longer have to prepend a tech-prefix on the address. For example, if voice gateways are mostly used in a network, and all voice gateways have been configured to register with technology prefix 1#, the gatekeeper can be configured to use 1# gateways as the default technology if this command is entered:

```
gatekeeper(config-gk)# gw-type-prefix 1# default-technology
```

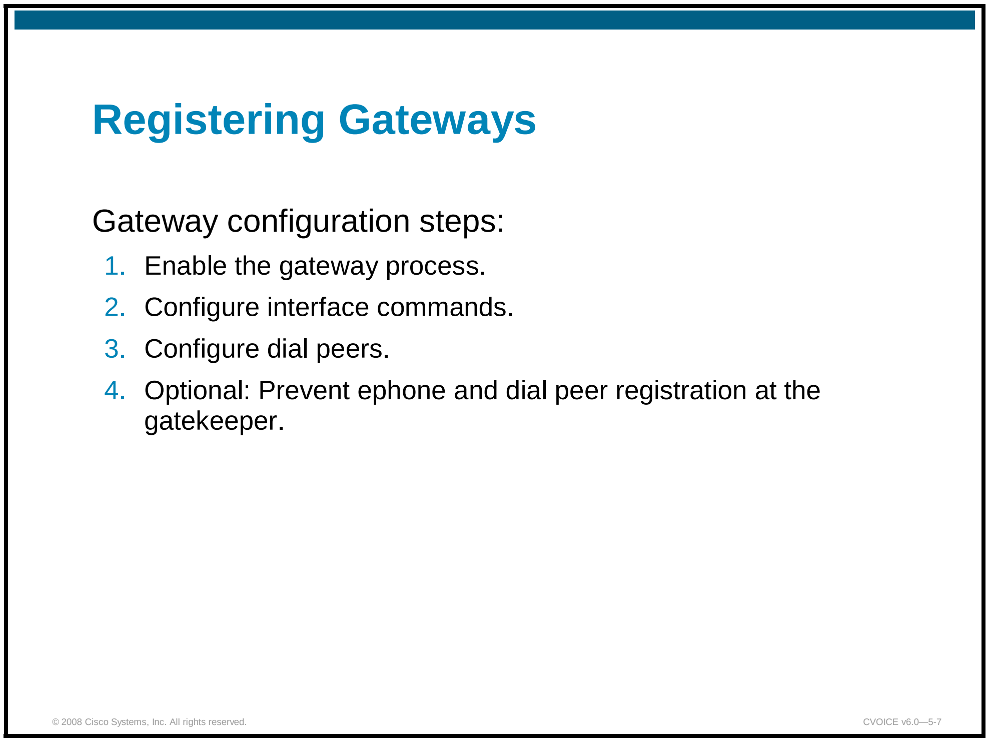
Now a caller no longer needs to prepend 1# to use a voice gateway. Any address that does not contain an explicit tech-prefix will be routed to one of the voice gateways that registered with 1#.

With this default tech-definition, a caller could ask the gatekeeper for admission to 2125551111. If the local gatekeeper does not recognize the zone prefix as belonging to any remote zone, it will route the call to one of its local (1#) voice gateways so that the call hops off locally. However, if it knows that the San Jose gatekeeper handles the 212 area code, it can send a location request for 2125551111 to that gatekeeper. This requires that the San Jose gatekeeper also be configured with some default gateway-type prefix and that its voice gateways be registered with that prefix type.

Note You must use consistent tech-prefixes throughout a gatekeeper deployment and have a consistent dial plan mapped out prior to implementation.

Configuring Gateways to Use H.323 Gatekeepers

This topic describes how to configure gateways to register with a gatekeeper.



Registering Gateways

Gateway configuration steps:

1. Enable the gateway process.
2. Configure interface commands.
3. Configure dial peers.
4. Optional: Prevent ephone and dial peer registration at the gatekeeper.

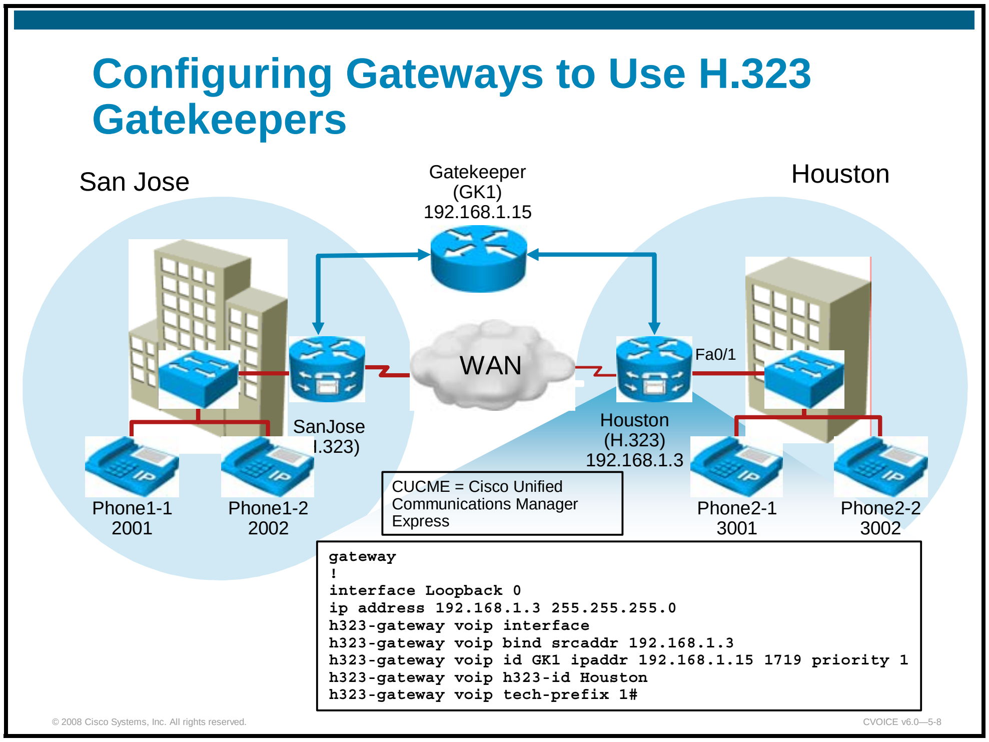
The figure shows the configuration steps for registering a gateway at a gatekeeper:

Step 1 Enable the gateway process on the router.

Step 2 Configure interface commands for H.323 registration at the gatekeeper.

Step 3 Configure the dial peers that are pointing to the gatekeeper.

Step 4 If necessary, prevent Ethernet phone (ephone) and dial-peer registration at the gatekeeper.



Configuring Gateways to Use H.323 Gatekeepers

```
gateway
!
interface Loopback 0
ip address 192.168.1.3 255.255.255.0
h323-gateway voip interface
h323-gateway voip bind srcaddr 192.168.1.3
h323-gateway voip id GK1 ipaddr 192.168.1.15 1719 priority 1
h323-gateway voip h323-id Houston
h323-gateway voip tech-prefix 1#
```

CVOICE v6.0—5-8

This figure shows how to register a gateway with a gatekeeper.

Follow these steps to configure gateways to use H.323 gatekeepers.

Step 1 Enable the H.323 VoIP gateway to register with the gatekeeper.

```
router(config)# gateway
```

Sometimes it is helpful to enable the gateway process at the end of your gateway configuration in order to avoid automatic gateway registration at the gatekeeper. For example, this is useful if you have multiple gatekeepers and want to make sure you are unicasting to a specific gatekeeper or using a specific H.323 ID. This allows all interface commands to be entered before the gateway attempts to register with the gatekeeper.

Step 2 Enter interface configuration mode for the interface you intend to use for use with the H.323 gatekeeper.

```
router(config)# interface Loopback 0
```

Step 3 Give the interface an IP address.

```
router(config-if)# ip-address 192.168.1.3 255.255.255.0
```

Step 4 Configure the interface as an H.323 gateway interface.

```
router(config-if)# h323-gateway voip interface
```

To configure an H.323 gateway interface, use the **h323-gateway voip interface** command in interface configuration mode.

Step 5 Bind the interface

```
router(config-if)# h323-gateway voip bind srcaddr 192.168.1.3
```

Step 6 Define the name and location of the gatekeeper.

```
router(config-if)# h323-gateway voip id Houston ipaddr
192.168.1.15 1719 priority 1
```

This command is used to specify the IP address of the gatekeeper and the zone the gateway should register with--in this case, **Houston**. Without the **voip id** command, the gateway will use multicast for gatekeeper discovery. When using multicast, the gateway will register with the first available zone on the gatekeeper. Use either the IP address of the gatekeeper or use multicast for discovery. The gatekeeper ID is the zone the gateway should register with.

Step 7 Specify the H.323 gateway name to identify it to its associated gatekeeper.

```
router(config-if)# h323-gateway voip h323-id Houston
```

This is an optional command used to configure the H.323 gateway and identify it to its associated gatekeeper. In this case, the gateway will register with the name **Houston** at the gatekeeper.

Step 8 Specify the tech-prefix that the gateway registers with the gatekeeper.

```
router(config-if)# h323-gateway voip tech-prefix 1#
```

The gateway will inform the gatekeeper that it wants to register with a tech-prefix of 1#. Each tech-prefix can contain up to 11 characters. Although not strictly necessary, a pound sign (#) is frequently used as the last digit in a tech-prefix.

Following is a table of gateway interface configuration commands and their purpose.

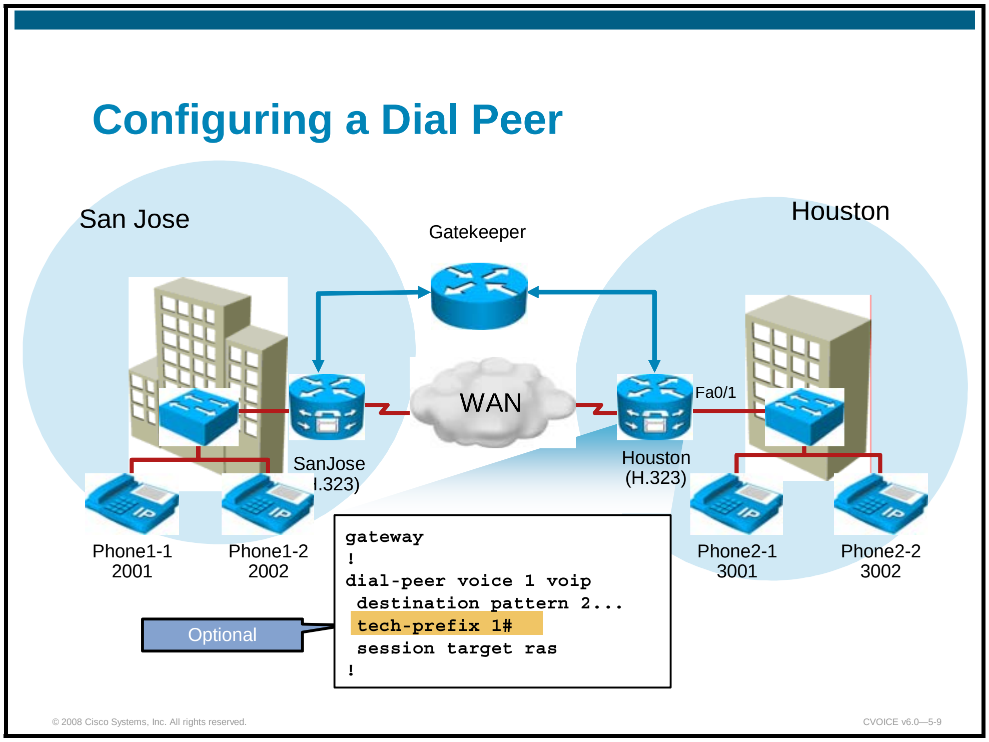
H.323 Gateway Interface Configuration Commands

Command	Purpose
h323-gateway voip interface	Identifies this as a VoIP gateway interface.
h323-gateway voip id *gatekeeper-id* {**ipaddr** *ip-address [port]*| **multicast**} [**priority** *priority*]	(Optional) Defines the name and location of the gatekeeper for this gateway. These are the keywords and arguments: ■ *gatekeeper-id*: H.323 identification of the gatekeeper, which should match a zone configured on a gatekeeper. If no match is found, the gatekeeper will register the gateway with the first configured local zone. ■ **ipaddr** *ip-address*: IP address to be used to identify the gatekeeper. ■ *port*: Port number used. ■ **multicast**: Used by the gateway to locate the gatekeeper. ■ **priority** *priority*: This is the priority of this gatekeeper. The acceptable range is 1 to 127, and the default is 127.
h323-gateway voip h323-id *interface-id*	(Optional) Defines the H.323 name of the gateway that identifies this gateway to its associated gatekeeper. Usually this ID is the name of the gateway, with the gatekeeper domain name appended to the end: name@domainname.
h323-gateway voip tech-prefix *prefix*	(Optional) Defines the numbers used as the tech- prefix that the gateway registers with the gatekeeper.

	This command can contain up to 11 characters. Although it is not strictly necessary, a pound symbol (#) is frequently used as the last digit in a prefix. Valid characters are 0 to 9, #, and *.

Dial Peer Configuration

This topic describes how to configure dial peers for gatekeepers.



Configuring a Dial Peer

```
gateway
!
dial-peer voice 1 voip
 destination pattern 2...
 tech-prefix 1#
 session target ras
!
```

CVOICE v6.0—5-9

The VoIP dial peer determines how to direct calls that originate from a local voice port into the VoIP cloud to the RAS session target. The session target indicates the address of the remote gateway where the call is terminated. In the example above, all calls designated for 2… will be routed from Houston to the gatekeeper.

Follow these steps to create a dial peer to be used with a gatekeeper:

Step 1 Enter dial-peer configuration mode.

```
Router(config)# dial-peer voice 1 voip
```

Step 2 Specify the E.164 address associated with this dial peer.

```
Router(config-dial-peer)# destination pattern 2...
```

Step 3 (Optional) Define the numbers used as the technology prefix that the gateway registers with the gatekeeper.

```
Router(config-dial-peer)# tech-prefix 1#
```

Note In this example, no prepending of a technology prefix is necessary due to the default technology configuration on the gatekeeper.

Step 4 Specify that the RAS protocol is being used to determine the IP address of the session target (meaning that a gatekeeper translates the E.164 address to an IP address).

```
Router(config-dial-peer)# session target ras
```

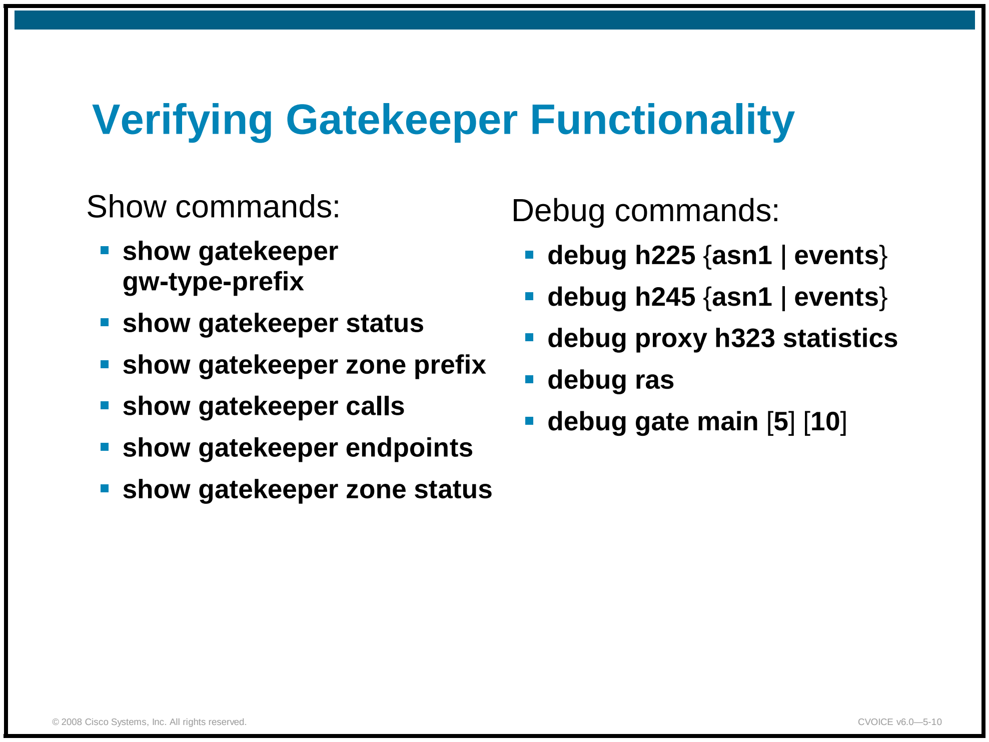
Caution When dealing with services numbers, such as 911, make sure to include the **no e.164 register** command.

The following is an example of using this command:

```
dial-peer voice 911 pots
 destination pattern 911
 prefix 911
 no e.164 register
 port 0/1/0
```

Verifying Gatekeeper Functionality

This topic describes how to verify gatekeeper functionality.



Verifying Gatekeeper Functionality

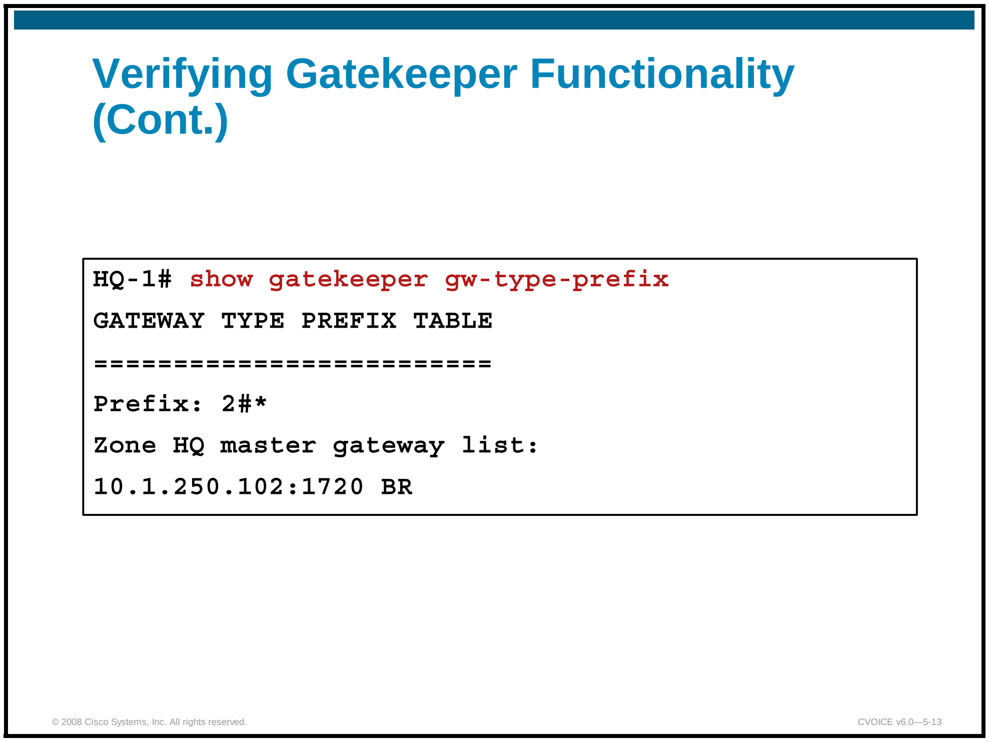
Show commands:

- **show gatekeeper gw-type-prefix**
- **show gatekeeper status**
- **show gatekeeper zone prefix**
- **show gatekeeper calls**
- **show gatekeeper endpoints**
- **show gatekeeper zone status**

Debug commands:

- **debug h225** {**asn1** | **events**}
- **debug h245** {**asn1** | **events**}
- **debug proxy h323 statistics**
- **debug ras**
- **debug gate main** [**5**] [**10**]

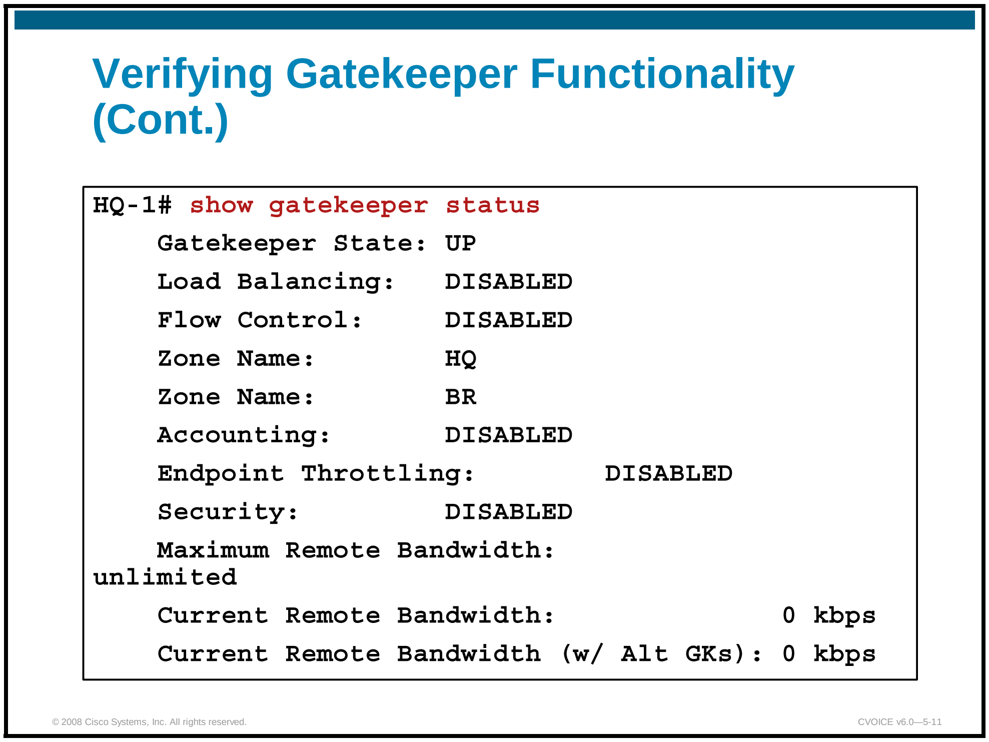
This figure lists the commands that can be used to monitor and debug gatekeeper configurations and interoperability with gateways. Following are examples of **show** commands outputs.



Verifying Gatekeeper Functionality (Cont.)

```
HQ-1# show gatekeeper gw-type-prefix
GATEWAY TYPE PREFIX TABLE
=========================
Prefix: 2#*
Zone HQ master gateway list:
10.1.250.102:1720 BR
```

Use the **show gatekeeper gw-type-prefix** command to display configured prefixes.

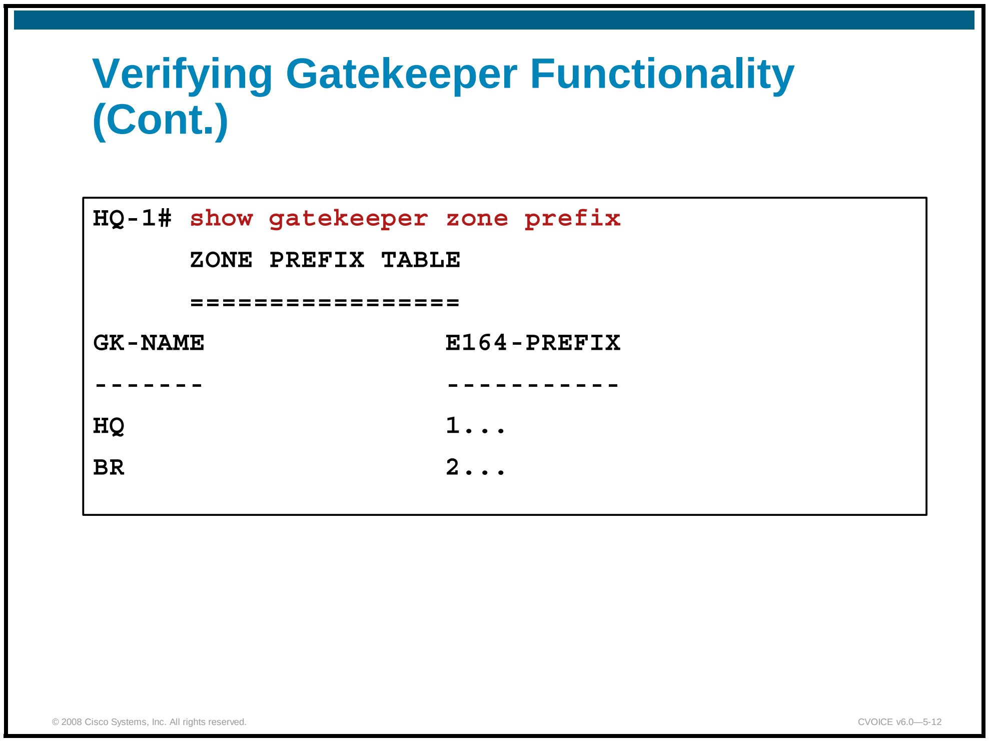


Verifying Gatekeeper Functionality (Cont.)

```
HQ-1# show gatekeeper status
    Gatekeeper State: UP
    Load Balancing:   DISABLED
    Flow Control:     DISABLED
    Zone Name:        HQ
    Zone Name:        BR
    Accounting:       DISABLED
    Endpoint Throttling:        DISABLED
    Security:         DISABLED
    Maximum Remote Bandwidth:
unlimited
    Current Remote Bandwidth:              0 kbps
    Current Remote Bandwidth (w/ Alt GKs): 0 kbps
```

CVOICE v6.0—5-11

Use the **show gatekeeper status** command to display the status of the gatekeeper.

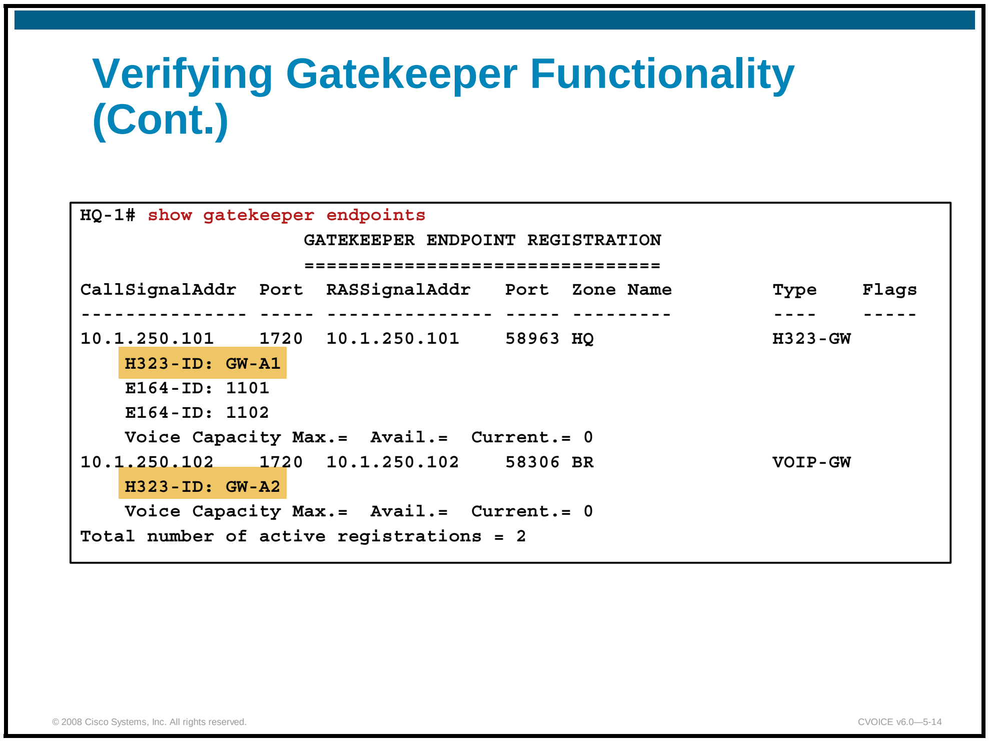


Verifying Gatekeeper Functionality (Cont.)

```
HQ-1# show gatekeeper zone prefix
      ZONE PREFIX TABLE
      =================
GK-NAME               E164-PREFIX
-------               -----------
HQ                    1...
BR                    2...
```

CVOICE v6.0—5-12

Use the **show gatekeeper zone prefix** command to display configured zone prefixes.



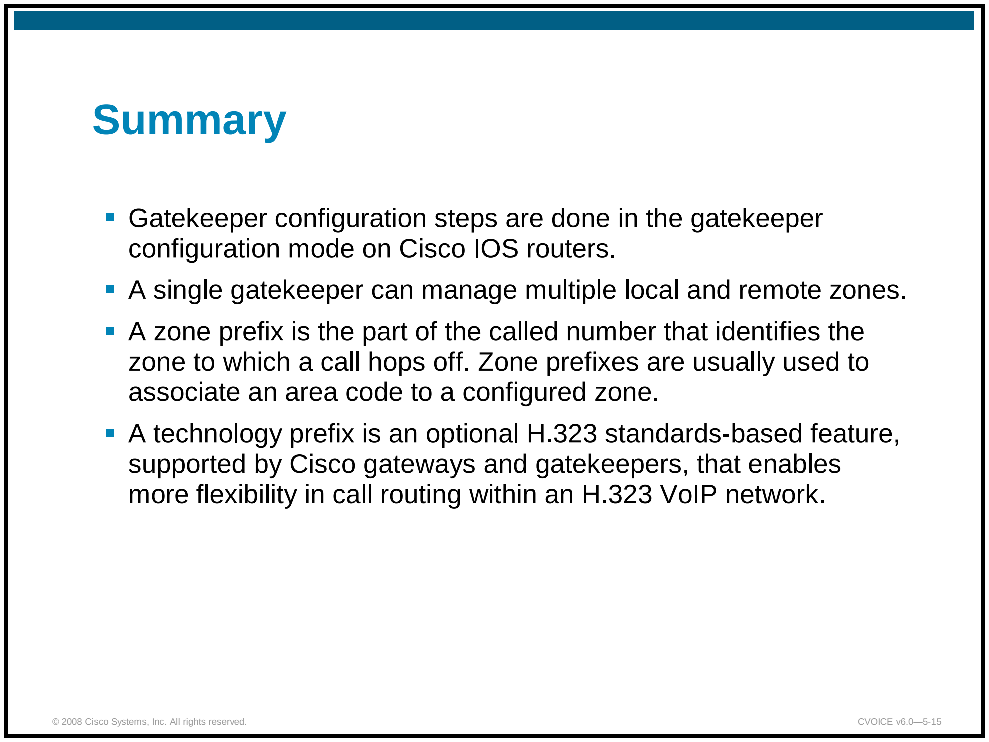
Verifying Gatekeeper Functionality (Cont.)

```
HQ-1# show gatekeeper endpoints
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type    Flags
--------------- ----- --------------- ----- ---------         ----    -----
10.1.250.101    1720  10.1.250.101    58963 HQ                H323-GW
    H323-ID: GW-A1
    E164-ID: 1101
    E164-ID: 1102
    Voice Capacity Max.=  Avail.=  Current.= 0
10.1.250.102    1720  10.1.250.102    58306 BR                VOIP-GW
    H323-ID: GW-A2
    Voice Capacity Max.=  Avail.=  Current.= 0
Total number of active registrations = 2
```

Use the **show gatekeeper endpoints** command to display registered endpoints of the gatekeeper.

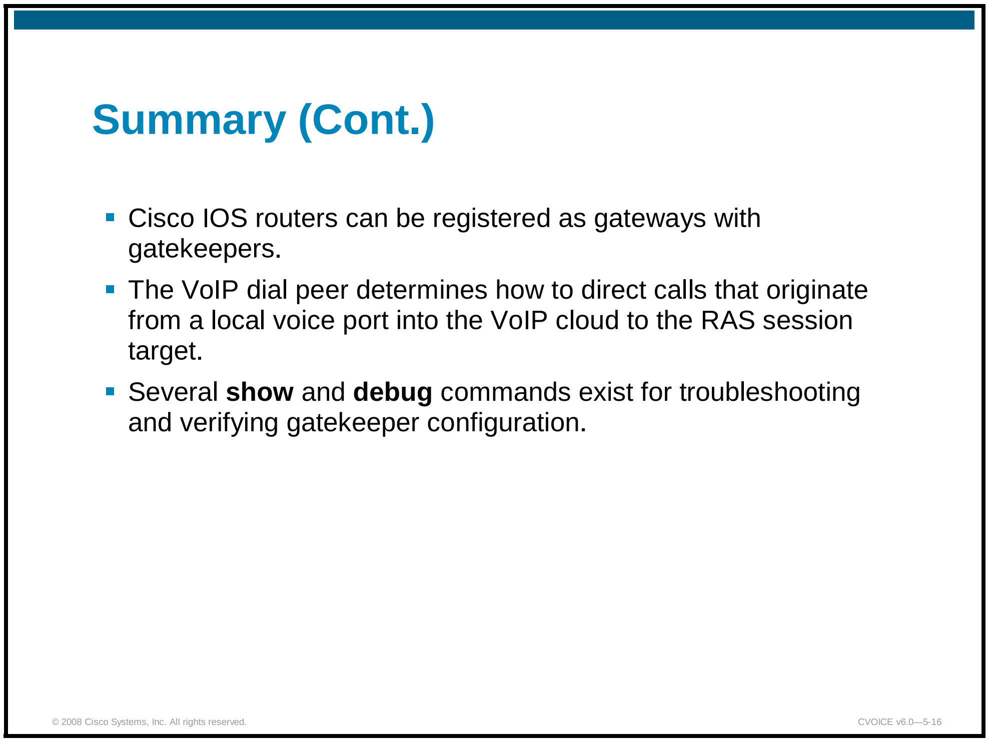
Summary

This topic summarizes the key points that were discussed in this lesson.



Summary

- Gatekeeper configuration steps are done in the gatekeeper configuration mode on Cisco IOS routers.
- A single gatekeeper can manage multiple local and remote zones.
- A zone prefix is the part of the called number that identifies the zone to which a call hops off. Zone prefixes are usually used to associate an area code to a configured zone.
- A technology prefix is an optional H.323 standards-based feature, supported by Cisco gateways and gatekeepers, that enables more flexibility in call routing within an H.323 VoIP network.



Summary (Cont.)

- Cisco IOS routers can be registered as gateways with gatekeepers.
- The VoIP dial peer determines how to direct calls that originate from a local voice port into the VoIP cloud to the RAS session target.
- Several **show** and **debug** commands exist for troubleshooting and verifying gatekeeper configuration.

Lesson Self-Check

Use the questions here to review what you learned in this lesson. The correct answers and solutions are found in the Lesson Self-Check Answer Key.

Q1) A single gatekeeper can manage multiple local and remote __________.

Relates to: Gatekeeper Configuration Steps

Q2) Gatekeeper configuration steps are done in the _____________ configuration mode on Cisco IOS routers.

Relates to: Configuring Gatekeeper Zones

Q3) Zone prefixes are usually used to associate a(n) __________ to a configured zone.

Relates to: Configuring Zone Prefixes

Q4) A ___________ prefix is an optional H.323 standards-based feature supported by Cisco gateways and gatekeepers that enables more flexibility in call routing within an H.323 VoIP network.

Relates to: Configuring Technology Prefixes

Q5) Cisco IOS routers can be registered as ____________ with gatekeepers.

Relates to: Configuring Gateways to Use H.323 Gatekeepers

Q6) The ________ dial peer determines how to direct calls that originate from a local voice port into the VoIP cloud to the RAS session target.

Relates to: Dial Peer Configuration

Q7) Use the ________________ command to display registered endpoints of the gatekeeper.

Relates to: Verifying Gatekeeper Functionality

Lesson Self-Check Answer Key

Q1) zones

Q2) gatekeeper

Q3) area code

Q4) “technology” or “tech-“

Q5) gateways

Q6) VoIP

Q7) **show gatekeeper endpoints**

Lesson 3

Implementing Gatekeeper-Based CAC

Overview

In this lesson, you will learn how to implement gatekeeper-based Call Admission Control (CAC). You will also learn how CAC is working and how it is responsible for managing admission control and bandwidth for both voice and video calls. Further, you will learn the functions of Resource Availability Indication (RAI) and how it is configured in an H.323 network.

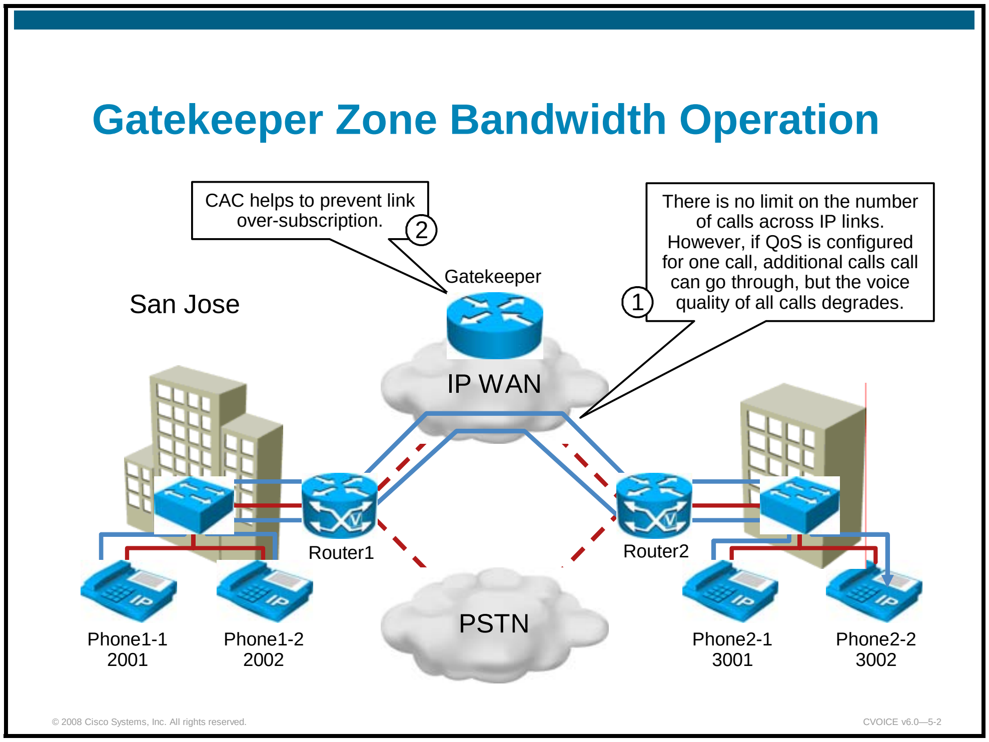
Objectives

Upon completing this lesson, you will be able to implement gatekeeper-based CAC. This ability includes being able to meet these objectives:

- Describe bandwidth operation in a gatekeeper zone
- Describe zone bandwidth calculation in a gatekeeper network
- Configure zone bandwidth on a gatekeeper
- Verify zone bandwidth operation on gatekeepers
- Describe how RAI performs resource-availability in gatekeeper networks
- Configure RAI in a gatekeeper network
- Verify RAI operation in gatekeeper networks

Gatekeeper Zone Bandwidth Operation

This topic describes bandwidth operation in a gatekeeper zone.



Gatekeeper Zone Bandwidth Operation

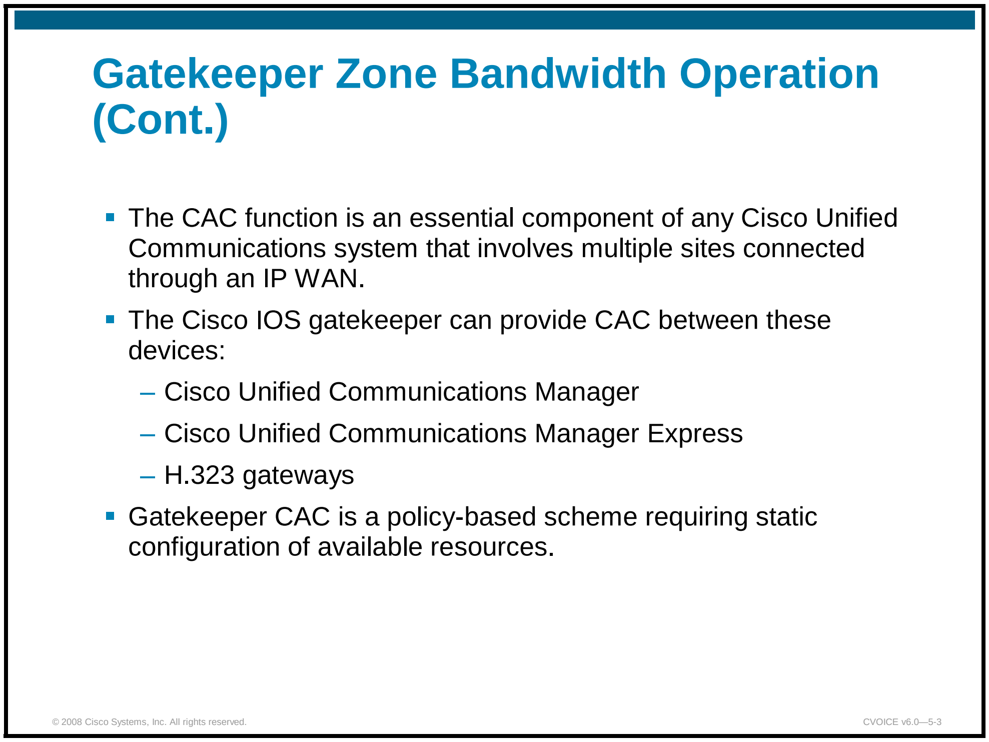
2 CAC helps to prevent link over-subscription.

1 There is no limit on the number of calls across IP links. However, if QoS is configured for one call, additional calls call can go through, but the voice quality of all calls degrades.

CVOICE v6.0—5-2

Consider the Cisco Unified Communications system shown in the figure. Because the IP network is based on a packet-switched network (PSN), no dedicated circuits are established to set up an IP communications call. Instead, the IP packets containing the voice samples are simply routed across the IP network together with other types of data packets. Quality of Service (QoS) is used to differentiate the voice packets from the data packets, but bandwidth resources, especially on IP WAN links, are not infinite. Therefore, network administrators dedicate a certain amount of "priority" bandwidth to voice traffic on each IP WAN link.

However, once the provisioned bandwidth has been fully utilized, the Cisco Unified IP Communications system must reject subsequent calls to avoid oversubscription of the priority queue on the IP WAN link, which would cause quality degradation for all voice calls. This function, known as CAC, is essential to guarantee good voice quality in a multisite deployment. The gatekeeper maintains a record of all active calls so that it can manage bandwidth in a zone.



Gatekeeper Zone Bandwidth Operation (Cont.)

- The CAC function is an essential component of any Cisco Unified Communications system that involves multiple sites connected through an IP WAN.
- The Cisco IOS gatekeeper can provide CAC between these devices:
  - Cisco Unified Communications Manager
  - Cisco Unified Communications Manager Express
  - H.323 gateways
- Gatekeeper CAC is a policy-based scheme requiring static configuration of available resources.

Use CAC to maintain a desired level of voice quality over a WAN link. For example, you can use CAC to regulate the voice quality on a T1 line that connects your main campus and a remote site.

CAC regulates voice quality by limiting the number of calls that can be active on a particular link at the same time. CAC does not guarantee a particular level of audio quality on the link, but it does allow you to regulate the amount of bandwidth consumed by active calls on the link.

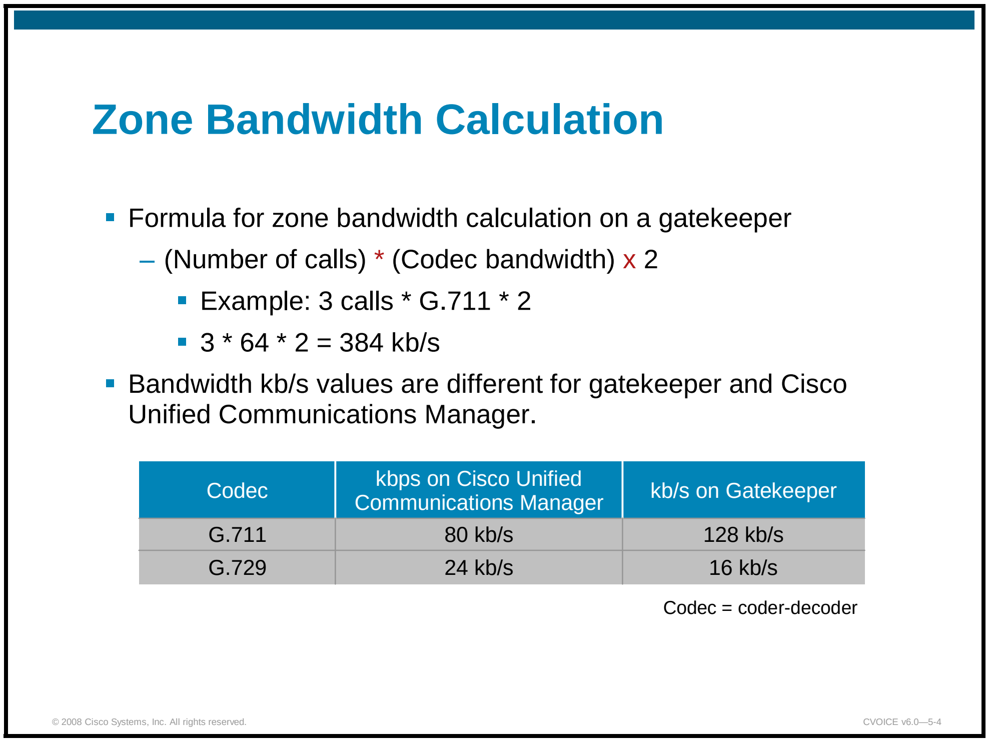
The Cisco IOS gatekeeper is the device in the IP communications network that is responsible for CAC between these devices:

- Cisco Unified Communications Manager
- Cisco Unified Communications Manager Express
- H.323 gateways

The gatekeeper requires a static policy-based configuration of the available resources. The gatekeeper cannot assign variable resources like the Resource Reservation Protocol (RSVP) is able to do.

Zone Bandwidth Calculation

This topic describes zone bandwidth calculation in a gatekeeper network.



Zone Bandwidth Calculation

- Formula for zone bandwidth calculation on a gatekeeper
  - (Number of calls) * (Codec bandwidth) x 2
    - Example: 3 calls * G.711 * 2
    - 3 * 64 * 2 = 384 kb/s
- Bandwidth kb/s values are different for gatekeeper and Cisco Unified Communications Manager.

Codec	kbps on Cisco Unified Communications Manager	kb/s on Gatekeeper
G.711	80 kb/s	128 kb/s
G.729	24 kb/s	16 kb/s

Codec = coder-decoder

Zone bandwidth in a gatekeeper network can be calculated with this simple formula:

Bandwidth = (Number of calls) * (Codec Bandwidth) * 2

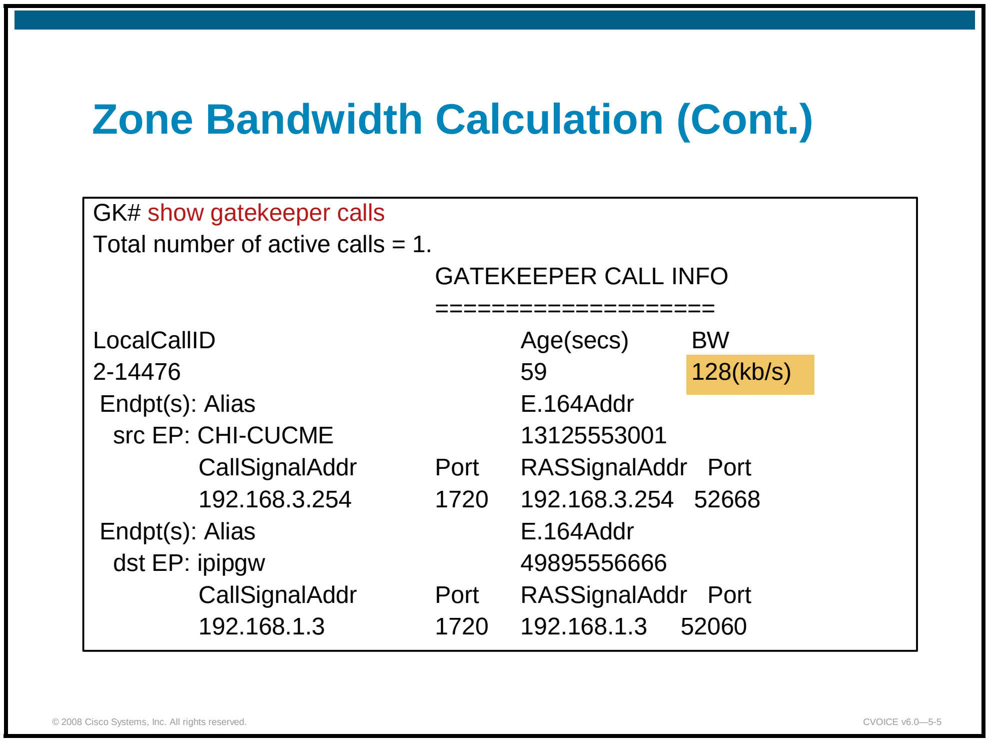
With this formula, the needed bandwidth in a gatekeeper network can be easily defined.

Note The numbers listed here are only raw numbers. For detailed numbers, a network survey is necessary:

For example, here is a calculation for three simultaneous G.711 calls in a gatekeeper network:

3 * 64kbs * 2 = 384 kb/s

An important point for every bandwidth calculation is the number of devices, for which you want to calculate the bandwidth. Gatekeepers and Cisco Unified Communications Managers have different bandwidth values for the same coder-decoders (codecs). In a Cisco Unified Communications Manager environment, a G.711 call consumes 80 kb/s and a G.729 call consumes 24 kb/s. In a gatekeeper environment, a G.711 call consumes 128 kb/s and a G.729 call consumes 16 kb/s. If a call is signaled from a Cisco Unified Communications Manager to a gatekeeper, the Cisco Unified Communications Manager will use internal 80 kb/s for a G.711 call and will signal Admission Request (ARQ) message a G.711 call with 128 kb/s to the gatekeeper. When using G.729, Cisco Unified Communications Manager will use 24 kb/s for internal CAC calculations, but request 16 kb/s from a gatekeeper.



Zone Bandwidth Calculation (Cont.)

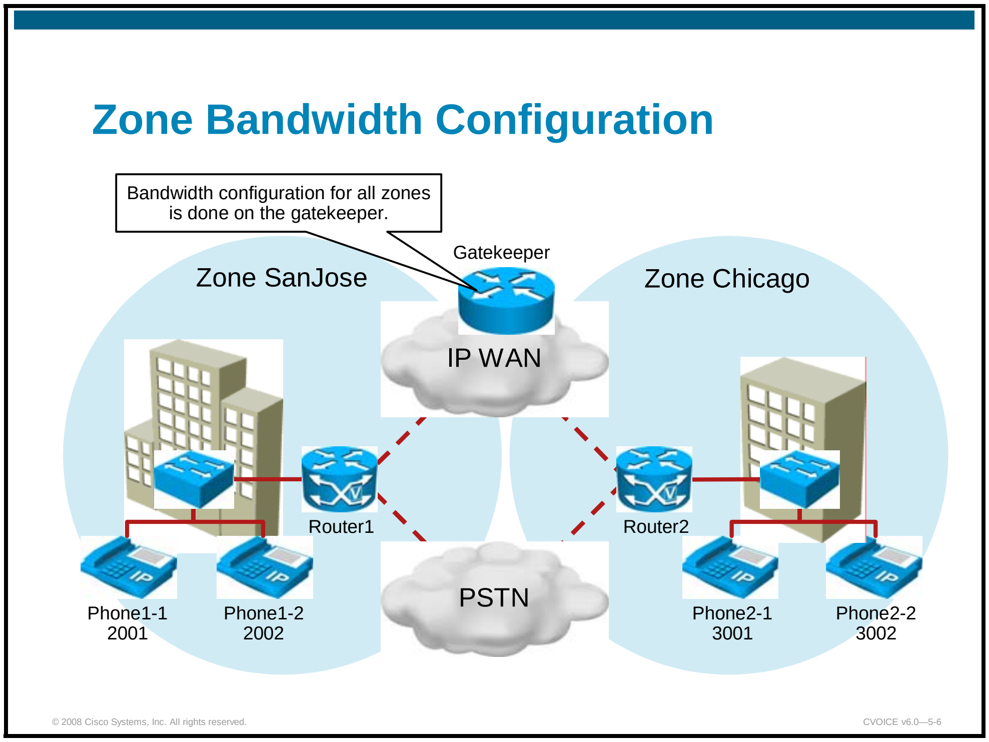
```
GK# show gatekeeper calls
Total number of active calls = 1.
                          GATEKEEPER CALL INFO
                          ====================
LocalCallID                     Age(secs)    BW
2-14476                         59           128(kb/s)
 Endpt(s): Alias                E.164Addr
  src EP: CHI-CUCME             13125553001
        CallSignalAddr    Port  RASSignalAddr  Port
        192.168.3.254     1720  192.168.3.254  52668
 Endpt(s): Alias                E.164Addr
  dst EP: ipipgw                49895556666
        CallSignalAddr    Port  RASSignalAddr  Port
        192.168.1.3       1720  192.168.1.3    52060
```

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—5-5

The example above shows a gatekeeper with an active call requested by Cisco Unified Communications Manager. Note the 128 kb/s in the BW column.

Zone Bandwidth Configuration

This topic describes how to configure zone bandwidth on a gatekeeper.

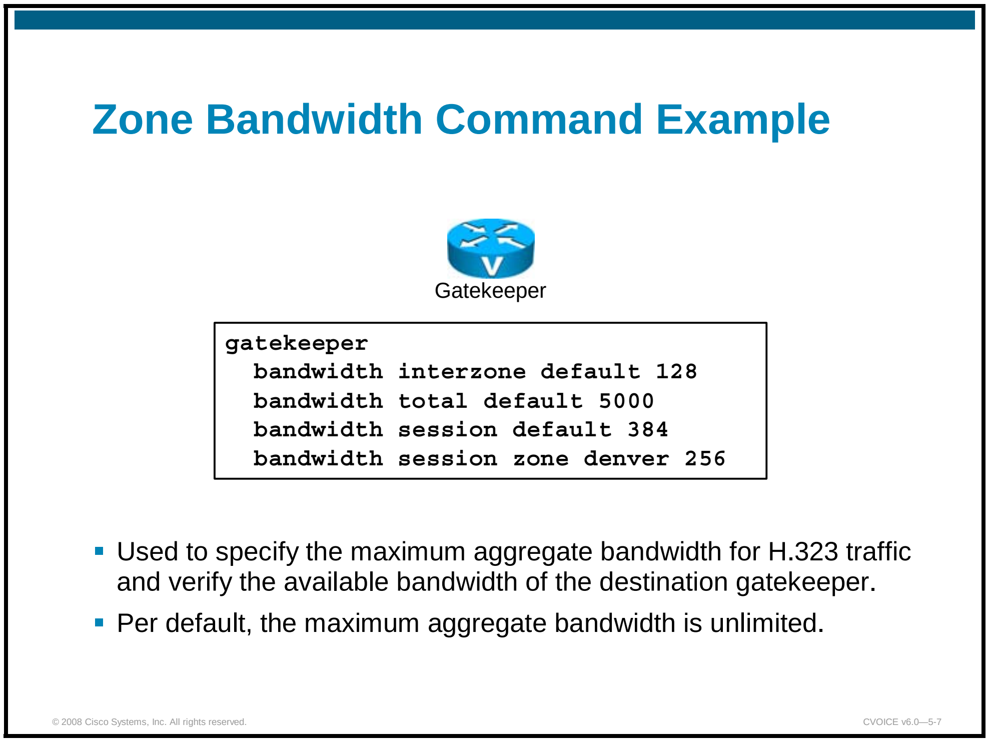


Zone Bandwidth Configuration

Bandwidth configuration for all zones is done on the gatekeeper.

CVOICE v6.0—5-6

The gatekeeper is the central device in the network. The bandwidth is configured for the network on the gatekeeper. The bandwidth will be checked for every call, which is signaled over the gatekeeper.



Zone Bandwidth Command Example

Gatekeeper

```
gatekeeper
  bandwidth interzone default 128
  bandwidth total default 5000
  bandwidth session default 384
  bandwidth session zone denver 256
```

- Used to specify the maximum aggregate bandwidth for H.323 traffic and verify the available bandwidth of the destination gatekeeper.
- Per default, the maximum aggregate bandwidth is unlimited.

CVOICE v6.0—5-7

The **bandwidth** command allows the gatekeeper to manage the bandwidth limitations within a zone, across zones, and at a per-session level. By default, the maximum aggregate bandwidth is unlimited.

The example above configures the default maximum bandwidth for traffic between one zone and another zone to 128 kb/s, the default maximum bandwidth for all zones to 5 Mb/s, the default maximum bandwidth for a single session within any zone up to 384 kb/s, the default maximum bandwidth for a single session with zone “Denver” up to 256 kb/s

Command Syntax

```
bandwidth {interzone | total | session | remote | check-
destination} {default | zone zone-name} bandwidth-size
```

Bandwidth Commands

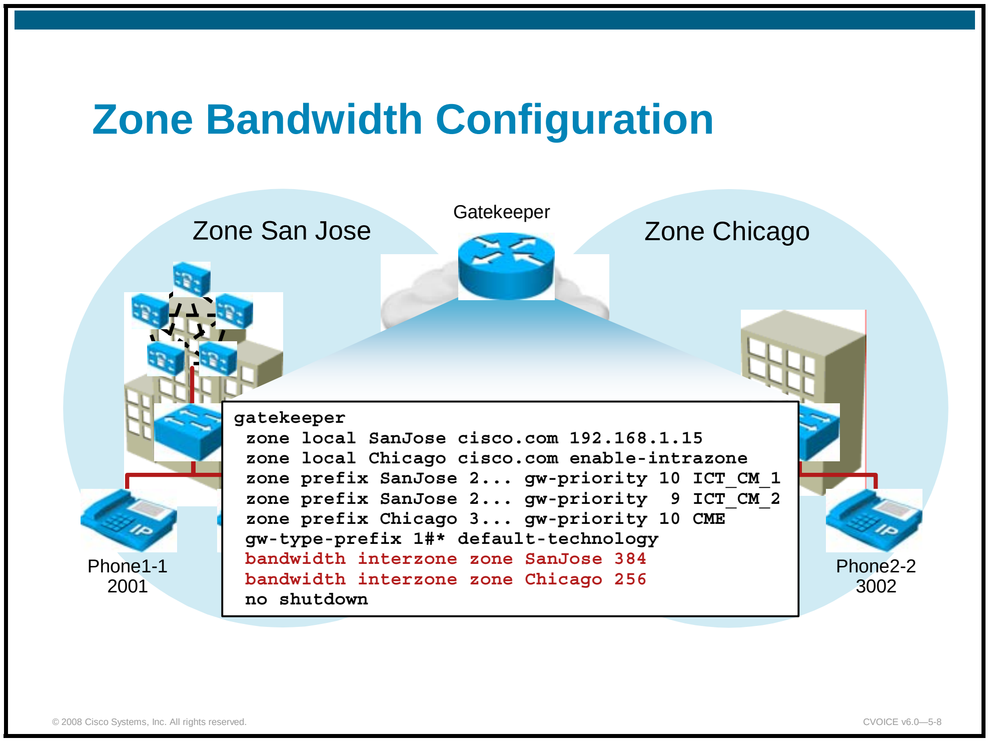
Parameter	Description
interzone	Total amount of bandwidth for H.323 traffic from the zone to any other zone.
total	Total amount of bandwidth for H.323 traffic allowed in the zone.
session	Maximum bandwidth allowed for a session in the zone.
remote	Total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper.
check-destination	Enables the gatekeeper to verify available bandwidth resources at the destination endpoint.
default	Default value for all zones.
zone *zone-name*	A particular zone.
bandwidth-size	Maximum bandwidth, in kb/s.

	For **interzone**, **remote** and **total**, the range is from 1 to 10,000,000. For **session**, the range is from 1 to 5000.

Usage Guidelines

Following are some usage guidelines:

- To specify maximum bandwidth for traffic between one zone and any other zone, use the **default** keyword with the **interzone** keyword.
- To specify maximum bandwidth for traffic within one zone or for traffic between that zone and another zone (interzone or intrazone), use the **default** keyword with the **total** keyword.
- To specify maximum bandwidth for a single session within a specific zone, use the **zone** keyword with the **session** keyword.
- To specify maximum bandwidth for a single session within any zone, use the **default** keyword with the **session** keyword.



Zone Bandwidth Configuration

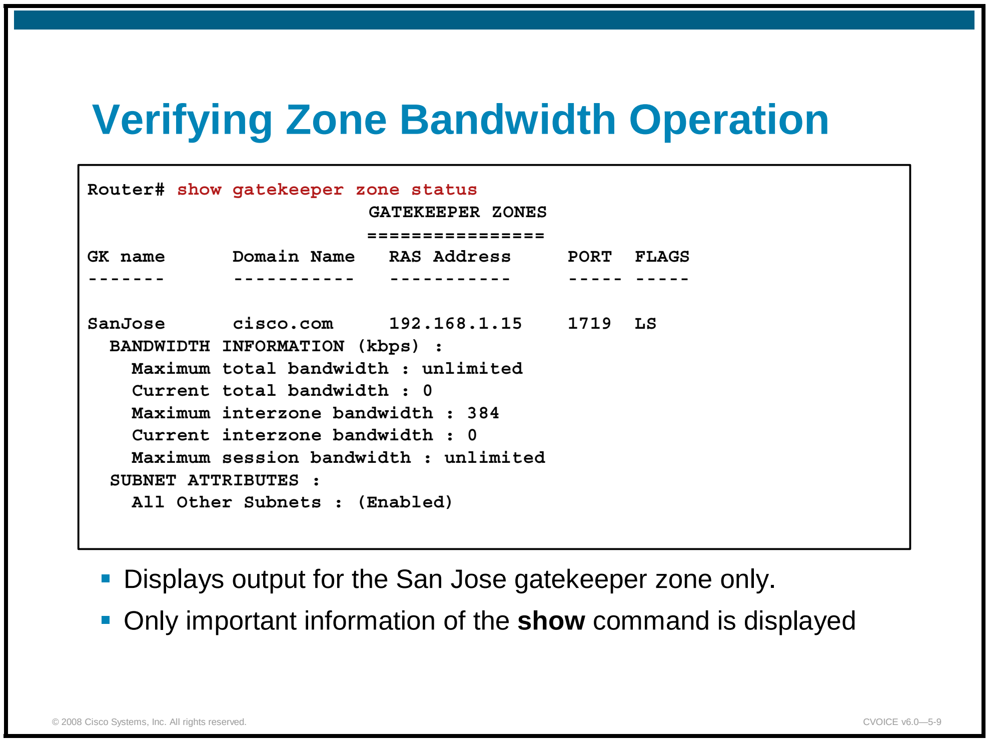
```
gatekeeper
 zone local SanJose cisco.com 192.168.1.15
 zone local Chicago cisco.com enable-intrazone
 zone prefix SanJose 2... gw-priority 10 ICT_CM_1
 zone prefix SanJose 2... gw-priority  9 ICT_CM_2
 zone prefix Chicago 3... gw-priority 10 CME
 gw-type-prefix 1#* default-technology
 bandwidth interzone zone SanJose 384
 bandwidth interzone zone Chicago 256
 no shutdown
```

The figure shows a sample of the configuration for the gatekeeper. There are two local zones: San Jose and Chicago. Notice that the **bandwidth interzone** commands are highlighted. In the **bandwidth** command, the **interzone** option specifies the bandwidth from one zone to another zone. The first **bandwidth** command allocates 384 kb/s of bandwidth for H.323 traffic between the San Jose zone and any other zone. The second **bandwidth** command allocates 256 kb/s of bandwidth for H.323 traffic between the Chicago zone and any other zone.

A Cisco Unified Communications Manager will always signal the bandwidth configuration in the region to the gatekeeper, which is configured on the Cisco Unified Communications Manager. For a G.711 call, the Cisco Unified Communications Manager will signal 128 kb/s to the gatekeeper, and for a G.729 call, the Cisco Unified Communications Manager will signal 16 kb/s to the gatekeeper. A gateway (such as a Cisco Unified Communications Manager Express) will signal the bandwidth corresponding to the codec configured on the dial peer, which is pointing to the Registration, Admission, and Status **(**RAS) destination.

Verifying Zone Bandwidth Operation

This topic describes how to verify zone bandwidth operation.



Verifying Zone Bandwidth Operation

```
Router# show gatekeeper zone status
                         GATEKEEPER ZONES
                         ================
GK name      Domain Name   RAS Address     PORT  FLAGS
-------      -----------   -----------     ----- -----

SanJose      cisco.com     192.168.1.15    1719  LS
  BANDWIDTH INFORMATION (kbps) :
    Maximum total bandwidth : unlimited
    Current total bandwidth : 0
    Maximum interzone bandwidth : 384
    Current interzone bandwidth : 0
    Maximum session bandwidth : unlimited
  SUBNET ATTRIBUTES :
    All Other Subnets : (Enabled)
```

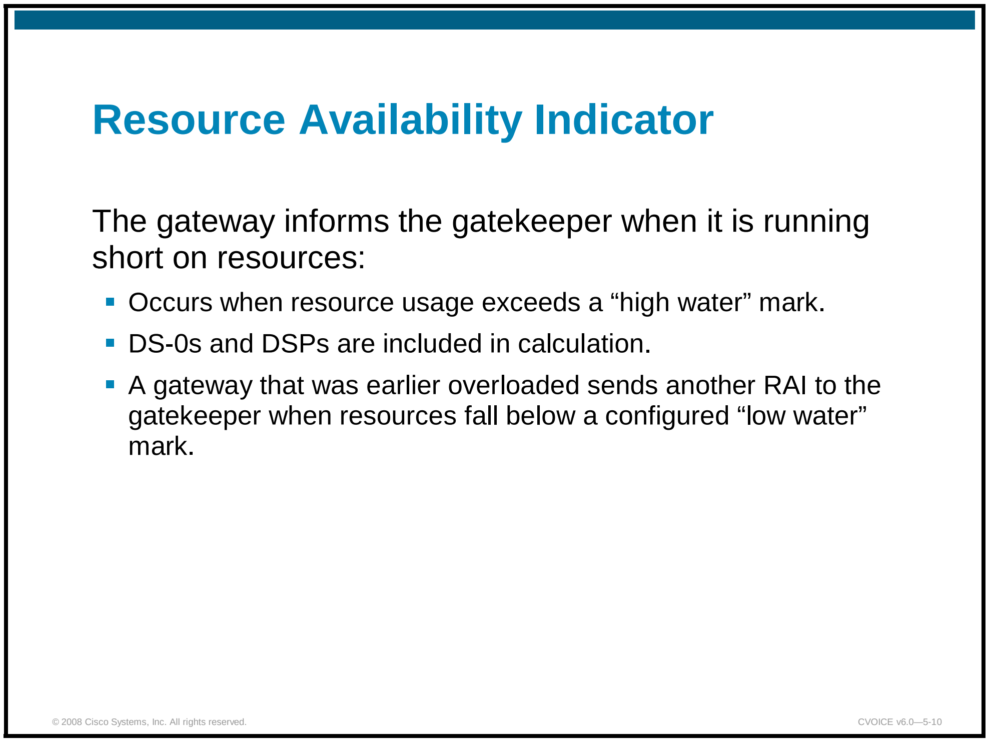
- Displays output for the San Jose gatekeeper zone only.
- Only important information of the **show** command is displayed

CVOICE v6.0—5-9

This figure shows the output of the **show gatekeeper zone status** command. In the bandwidth information output, you can see the maximum interzone bandwidth for all calls in the SanJose zone. In this scenario, there is a bandwidth of 384 kb/s configured.

RAI in Gatekeeper Networks

This topic describes how the RAI performs resource-availability in gatekeeper networks.



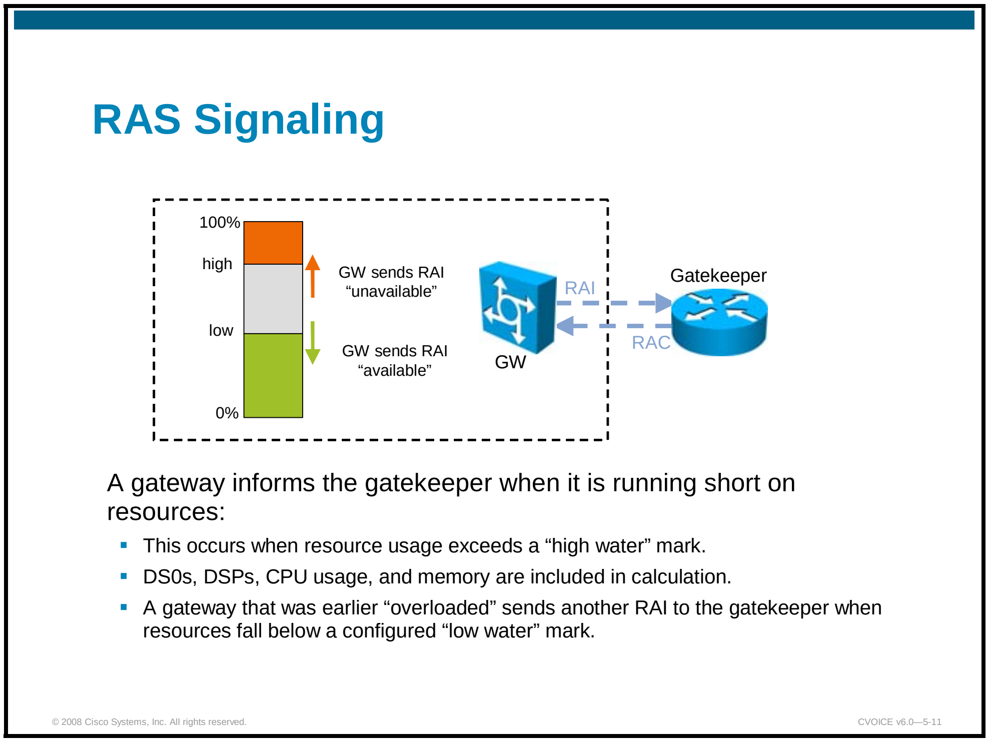
Resource Availability Indicator

The gateway informs the gatekeeper when it is running short on resources:

- Occurs when resource usage exceeds a “high water” mark.
- DS-0s and DSPs are included in calculation.
- A gateway that was earlier overloaded sends another RAI to the gatekeeper when resources fall below a configured “low water” mark.

To enable gatekeepers to make intelligent call-routing decisions, the gateway can be configured to report the status of its resource availability to its gatekeeper. Resources that are monitored are digital service level 0 (DS0) and digital signal processor (DSP) channels.

The gateway reports its resource status to the gatekeeper with the use of RAS RAI. When a monitored resource falls below a configurable threshold, the gateway sends an RAI to the gatekeeper that indicates that the gateway is almost out of resources. When the available resources then exceed another configurable threshold, the gateway sends an RAI that indicates that the resource depletion condition no longer exists.



RAS Signaling

A gateway informs the gatekeeper when it is running short on resources:

- This occurs when resource usage exceeds a “high water” mark.
- DS0s, DSPs, CPU usage, and memory are included in calculation.
- A gateway that was earlier “overloaded” sends another RAI to the gatekeeper when resources fall below a configured “low water” mark.

Resource reporting thresholds are configured by using the resource threshold command under the **gateway** command-line interface (CLI). The upper and lower thresholds are separately configurable to prevent the gateway from operating sporadically due to the availability or lack of resources.

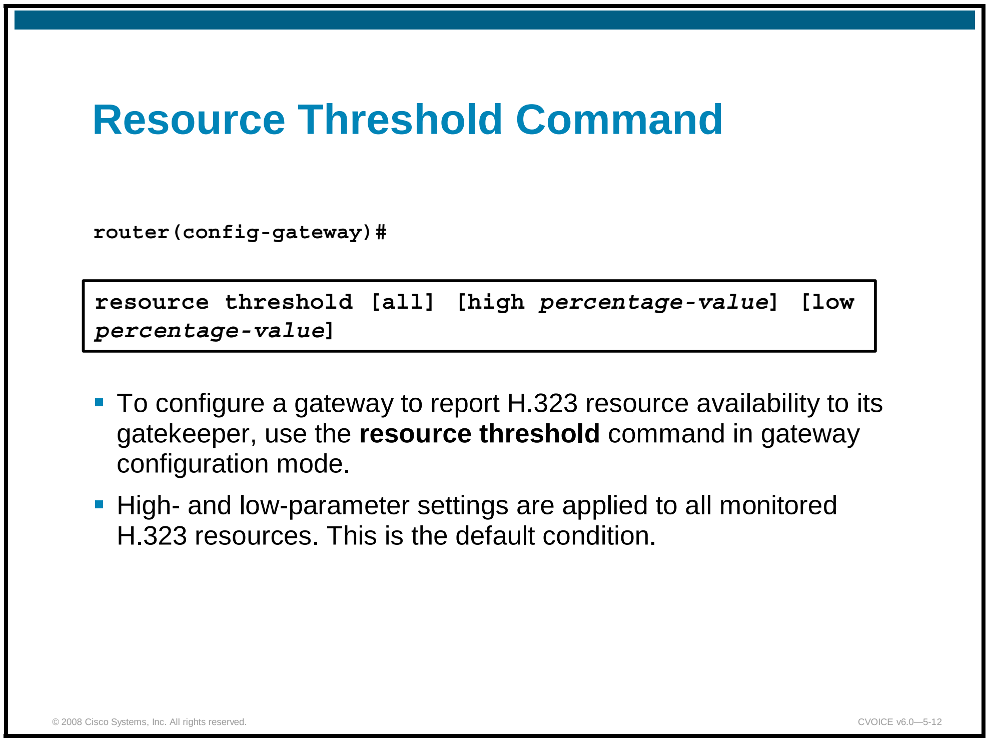
The RAI message is sent by an endpoint to indicate when it has neared resource limits or is no longer near a resource limit. The gatekeeper replies with Resource Available Confirm (RAC) message.

RAI is very useful in RAS for signalized load sharing. For example, consider a case with more than one possible gateway that can be used to reach a number. This can be a situation where a point is peering to the public switched telephone network (PSTN). A sample call flow follows:

1. A gatekeeper receives a location request (LRQ) or an ARQ. It has potential gateways to use to reach the requested E.164 number within the PSTN.
2. The gatekeeper asks the gateway cluster which gateway is under heavy load.
3. The decision of which gateway to use now comes from the same originating gatekeeper by sending an admission confirmation (ACF) or location confirmation (LCF) message back to the requester (gateway, gatekeeper, or directory gatekeeper) with the IP address of the gateway that is under low load conditions.

RAI Configuration

This topic describes the configuration of RAI in a network.



Resource Threshold Command

```
router(config-gateway)#
```

```
resource threshold [all] [high percentage-value] [low
percentage-value]
```

- To configure a gateway to report H.323 resource availability to its gatekeeper, use the **resource threshold** command in gateway configuration mode.
- High- and low-parameter settings are applied to all monitored H.323 resources. This is the default condition.

CVOICE v6.0—5-12

The figure describes the **resource threshold** command, which is available on a Cisco IOS gateway to enable RAI on endpoints.

Use the **resource threshold** command in gateway configuration mode to configure a gateway to report H.323 resource availability to its gatekeeper. You can specify **all** or specific **high** and **low** values. The default for high and low values is 90. Use the **no** form of this command to disable gateway resource-level reporting.

```
gateway1(config-gateway)# resource threshold [all] [high
percentage-value] [low percentage-value] report-policy [
addressable | idle-only]
```

Tip To be more flexible with call routing, you should always configure two different values for **high** and **low**.

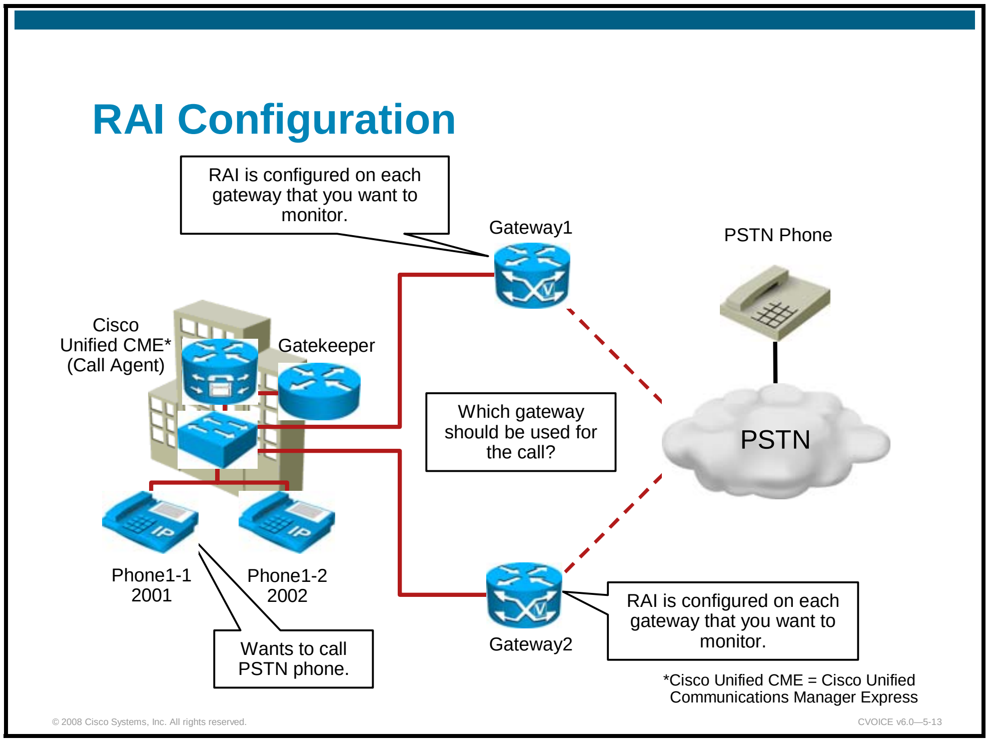
- **all:** (Optional) The default condition. High- and low-parameter settings are applied to all monitored H.323 resources.
- **high** *percentage-value***:** (Optional) Resource utilization level that triggers an RAI message indicating that H.323 resource use is high. Enter a number between 1 and 100 that represents the high-resource utilization percentage. A value of 100 specifies high-resource usage when any H.323 resource is unavailable. Default is 90 percent.
- **low** *percentage-value***:** (Optional) Resource utilization level that triggers an RAI message that indicates H.323 resource usage has dropped below the high-usage level. Enter a number between 1 and 100 that represents the acceptable resource utilization percentage.

After the gateway sends a high-utilization message, it waits to send the resource recovery message until the resource use drops below the value defined by the **low** parameter. Default is 90 percent. The following example defines the H.323 resource limits for a gateway.

```
gateway1(config-gateway)# resource threshold high 70 low 60
```

This command also includes an optional **report-policy** parameter to specify how resource utilization is calculated. Either of these available resource types may be reported:

- **Idle-only:** Only free and in-use channels are reported as available resources. This is the default calculation.
- **Addressable:** Addressable (for DS0) and total (for DSP) channels are reported as available resources.



RAI Configuration

RAI is configured on each gateway that you want to monitor.

Which gateway should be used for the call?

Wants to call PSTN phone.

RAI is configured on each gateway that you want to monitor.

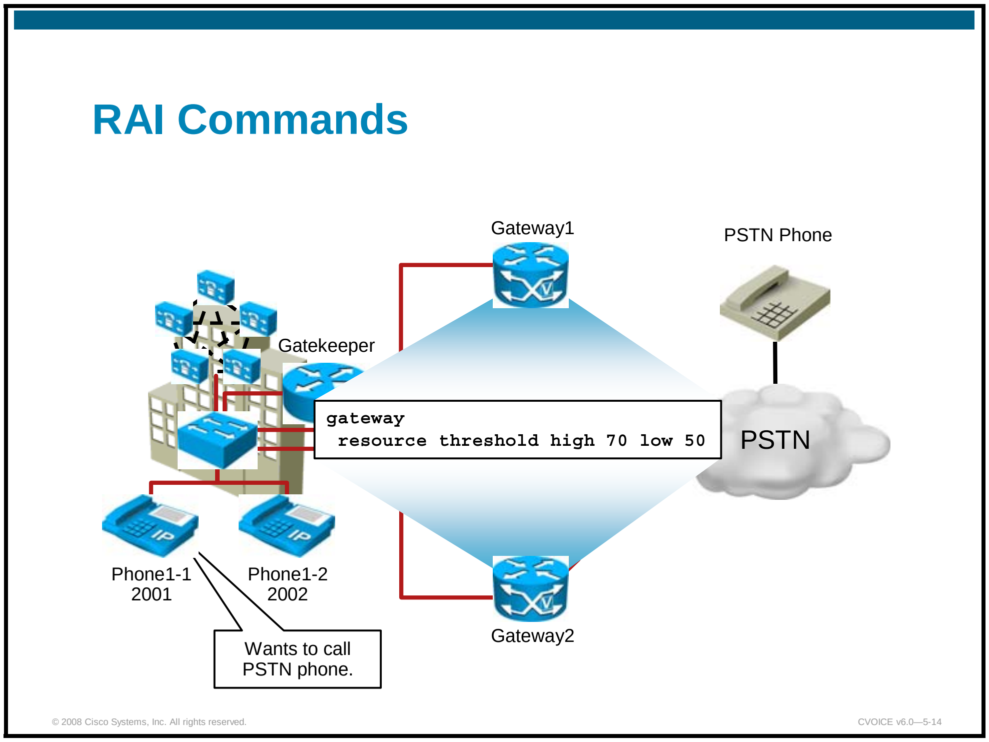
*Cisco Unified CME = Cisco Unified Communications Manager Express

CVOICE v6.0—5-13

RAI has to be configured on each endpoint that should send RAI information in your network. The figure shows two gateways that send RAI information to the gatekeeper. The gatekeeper will check the RAI information to verify the load on each gateway in order to route the call.

RAI Configuration Example

This example shows a typical RAI configuration.



RAI Commands

```
gateway
 resource threshold high 70 low 50
```

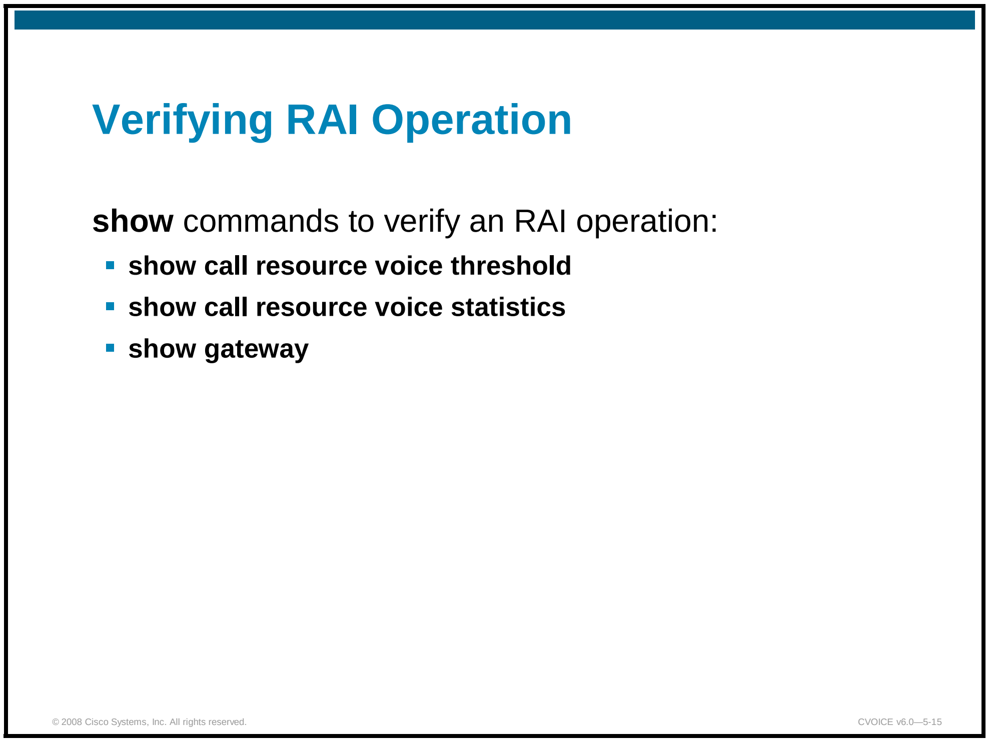
CVOICE v6.0—5-14

The figure above shows two gateways being configured for RAI operation. The upper and lower thresholds are separately configurable to prevent the gateway from operating sporadically due to the availability or lack of resources. In the figure, a **high** threshold of 70 is configured, which represents the high-resource utilization percentage. The default for the **high** threshold is 90 percent.

After the gateway sends a high-utilization message, it waits to send the resource recovery message until the resource use drops below the value defined by the **low** parameter (which in this case is 50). The default for the **low** parameter is 90 percent.

Verifying RAI Operation

This topic describes how to verify RAI operation in a gatekeeper network.



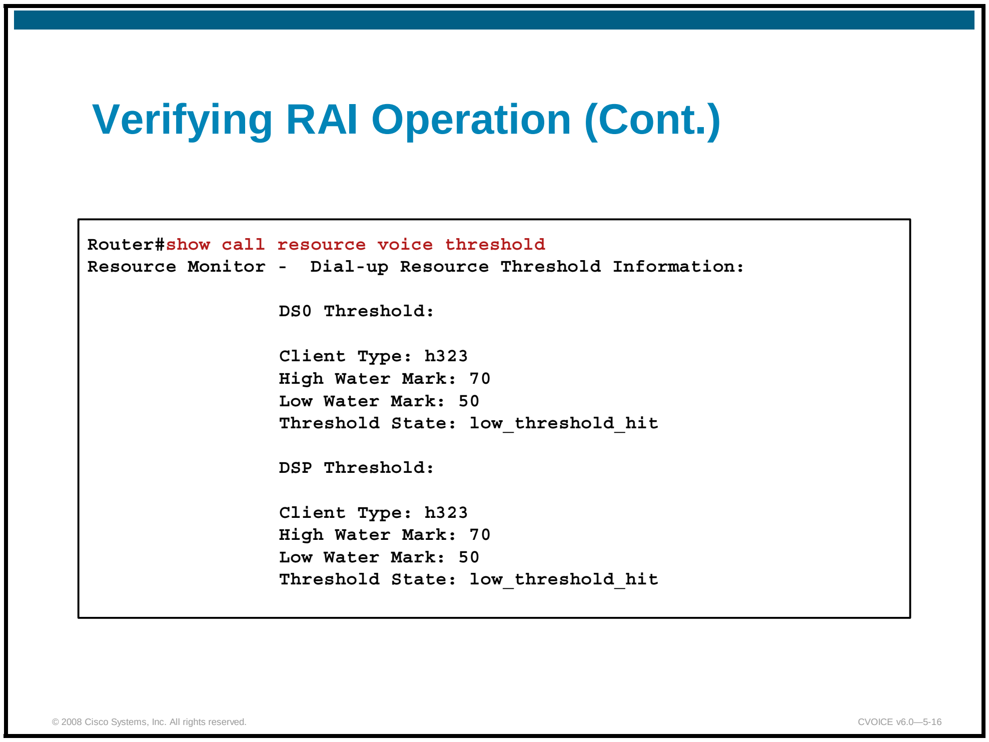
Verifying RAI Operation

show commands to verify an RAI operation:

- **show call resource voice threshold**
- **show call resource voice statistics**
- **show gateway**

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—5-15

Various **show** commands are available to verify RAI operation. Use the **show call resource voice threshold** command in privileged EXEC mode to display the threshold configuration settings and status for an H.323 gateway. The **show call resource voice stat** and **show gateway** commands are also useful to verify RAI operation.

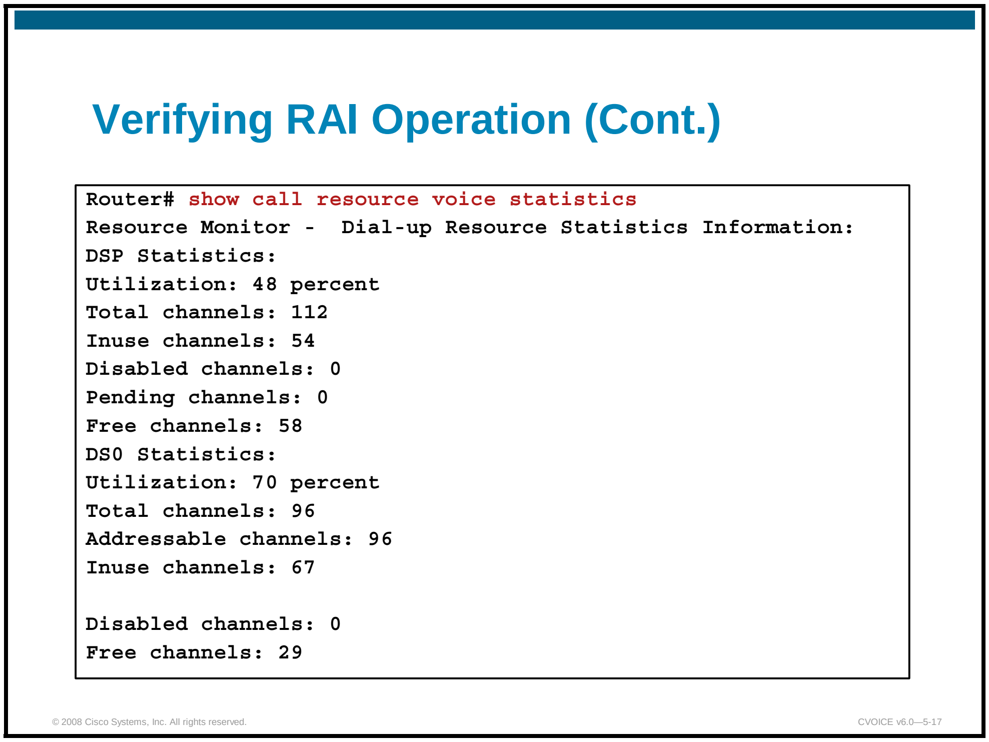


Verifying RAI Operation (Cont.)

```
Router#show call resource voice threshold
Resource Monitor -  Dial-up Resource Threshold Information:

                 DS0 Threshold:

                 Client Type: h323
                 High Water Mark: 70
                 Low Water Mark: 50
                 Threshold State: low_threshold_hit

                 DSP Threshold:

                 Client Type: h323
                 High Water Mark: 70
                 Low Water Mark: 50
                 Threshold State: low_threshold_hit
```

CVOICE v6.0—5-16

Use the **show call resource voice threshold** command from enable mode to check the threshold state on the gateway. This figure shows the output of the **show call resource voice threshold** command.



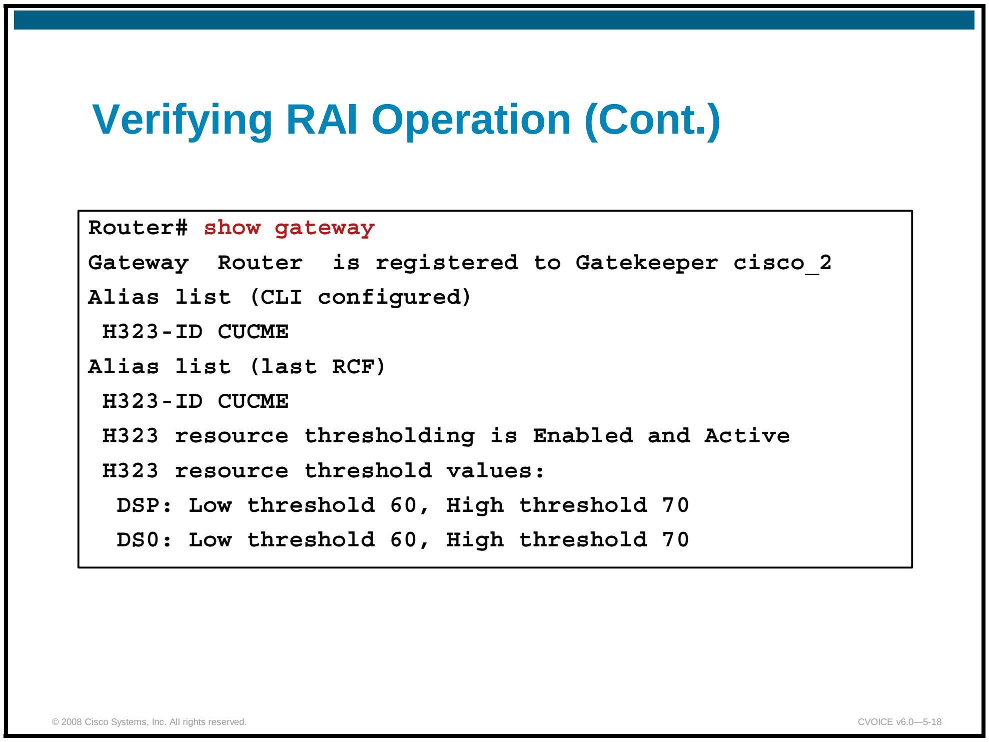
Verifying RAI Operation (Cont.)

```
Router# show call resource voice statistics
Resource Monitor -  Dial-up Resource Statistics Information:
DSP Statistics:
Utilization: 48 percent
Total channels: 112
Inuse channels: 54
Disabled channels: 0
Pending channels: 0
Free channels: 58
DS0 Statistics:
Utilization: 70 percent
Total channels: 96
Addressable channels: 96
Inuse channels: 67

Disabled channels: 0
Free channels: 29
```

CVOICE v6.0—5-17

Use the **show call resource voice statistics** command from the enable mode to show the statistics of all the resources (DSPs and DS0s).

In this output, the DSP utilization is 54/112 = 48 percent, the DS0 utilization is 67/96 = 70 percent, and the high threshold value configured in both cases (DSP and DS0 utilization) is not exceeded.

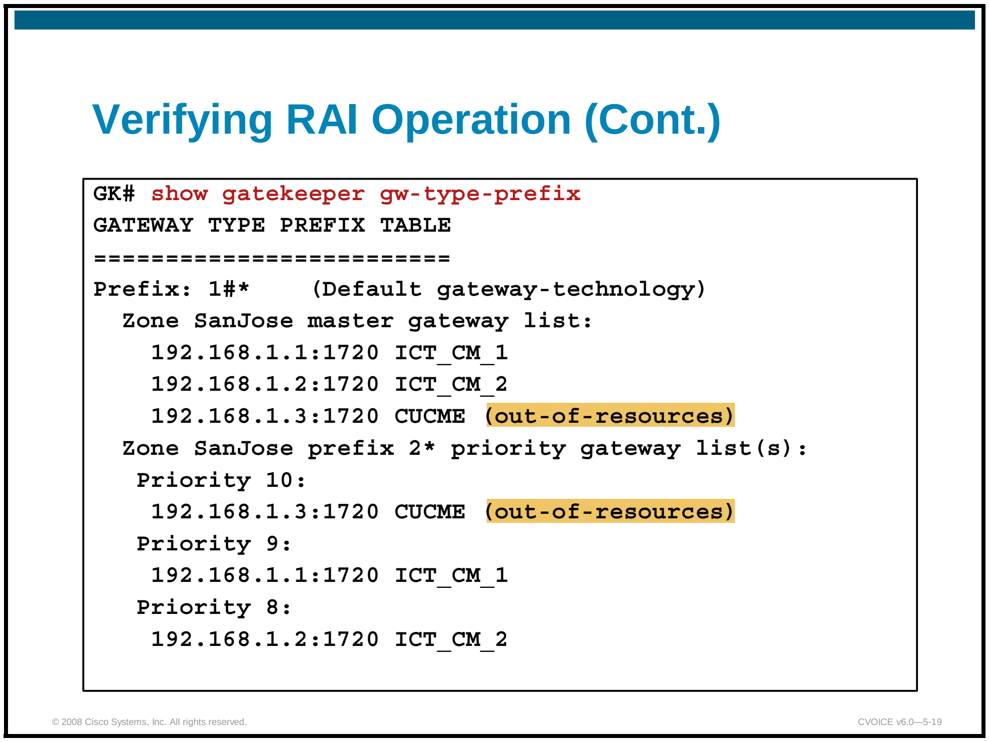


Verifying RAI Operation (Cont.)

```
Router# show gateway
Gateway  Router  is registered to Gatekeeper cisco_2
Alias list (CLI configured)
 H323-ID CUCME
Alias list (last RCF)
 H323-ID CUCME
 H323 resource thresholding is Enabled and Active
 H323 resource threshold values:
  DSP: Low threshold 60, High threshold 70
  DS0: Low threshold 60, High threshold 70
```

CVOICE v6.0—5-18

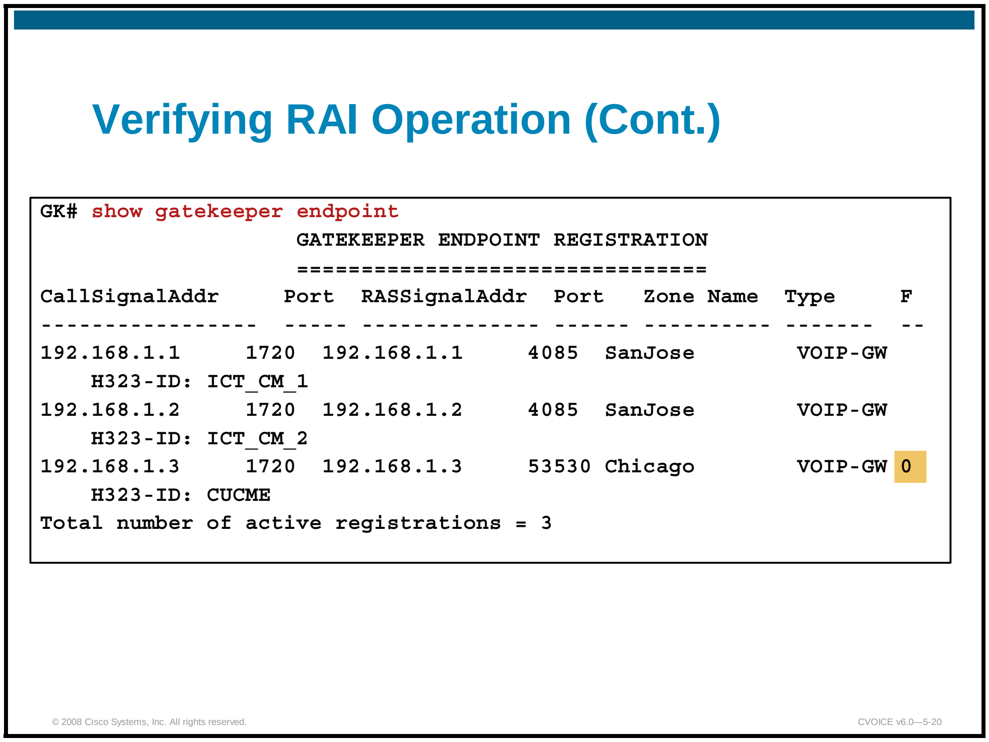
Use the **show gateway** command to check the status of the H.323 resource threshold if it is enabled and active. This also gives you the configured low and high threshold values. In this output, you can see that the "resource threshold" is enabled and active. "Enabled" means configured and "Active" means that the H.323 RAS processes in the Cisco IOS software are registered with the Resource Monitor. As an example, if the gateway is not registered with the gatekeeper, the H.323 RAS process is not initialized and the resource threshold is enabled, but not active. The figure shows the output of the **show gateway** command:



Verifying RAI Operation (Cont.)

```
GK# show gatekeeper gw-type-prefix
GATEWAY TYPE PREFIX TABLE
=========================
Prefix: 1#*    (Default gateway-technology)
  Zone SanJose master gateway list:
    192.168.1.1:1720 ICT_CM_1
    192.168.1.2:1720 ICT_CM_2
    192.168.1.3:1720 CUCME (out-of-resources)
  Zone SanJose prefix 2* priority gateway list(s):
   Priority 10:
    192.168.1.3:1720 CUCME (out-of-resources)
   Priority 9:
    192.168.1.1:1720 ICT_CM_1
   Priority 8:
    192.168.1.2:1720 ICT_CM_2
```

Use the **show gatekeeper gw-type-prefix** and **show gatekeeper endpoint** commands to check the RAI status for each gateway on the gatekeeper.



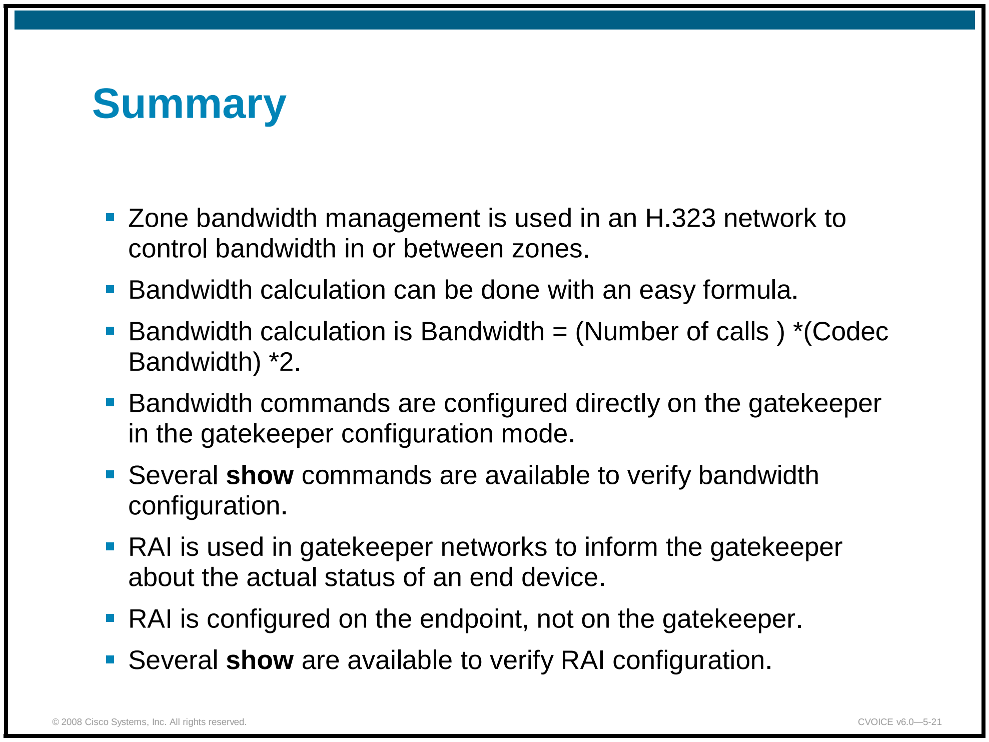
Verifying RAI Operation (Cont.)

```
GK# show gatekeeper endpoint
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr     Port  RASSignalAddr  Port   Zone Name  Type     F
-----------------  ----- -------------- ------ ---------- -------  --
192.168.1.1     1720  192.168.1.1     4085  SanJose        VOIP-GW
    H323-ID: ICT_CM_1
192.168.1.2     1720  192.168.1.2     4085  SanJose        VOIP-GW
    H323-ID: ICT_CM_2
192.168.1.3     1720  192.168.1.3     53530 Chicago        VOIP-GW 0
    H323-ID: CUCME
Total number of active registrations = 3
```

This is the output of the **show gatekeeper endpoint** command, where the **0** flag in the output indicates that the gateway is out of resources.

Summary

This topic summarizes the key points that were discussed in this lesson.



Summary

- Zone bandwidth management is used in an H.323 network to control bandwidth in or between zones.
- Bandwidth calculation can be done with an easy formula.
- Bandwidth calculation is Bandwidth = (Number of calls) *(Codec Bandwidth) *2.
- Bandwidth commands are configured directly on the gatekeeper in the gatekeeper configuration mode.
- Several **show** commands are available to verify bandwidth configuration.
- RAI is used in gatekeeper networks to inform the gatekeeper about the actual status of an end device.
- RAI is configured on the endpoint, not on the gatekeeper.
- Several **show** are available to verify RAI configuration.

Lesson Self-Check

Use the questions here to review what you learned in this lesson. The correct answers and solutions are found in the Lesson Self-Check Answer Key.

Q1) ______________________ regulates voice quality by limiting the number of calls that can be active on a particular link at the same time.

Relates to: Gatekeeper Zone Bandwidth Operation

Q2) The formula for calculating the zone bandwidth in a gatekeeper-controlled network is ______________.

Relates to: Zone Bandwidth Calculation

Q3) The ________________ command allows the gatekeeper to manage the bandwidth limitations within a zone, across zones, and at a per-session level.

Relates to: Zone Bandwidth Configuration

Q4) Use the _______________________ command to verify zone bandwidth.

Relates to: Verifying Zone Bandwidth Operation

Q5) The gateway reports its resource status to the gatekeeper with the use of the RAS _______________.

Relates to: RAI in Gatekeeper Networks

Q6) Use the _________________________ command in gateway configuration mode to configure a gateway to report H.323 resource availability to its gatekeeper.

Relates to: RAI Configuration

Q7) Use the _________________________ command to display the threshold configuration settings and status for an H.323 gateway.

Relates to: Verifying RAI Operation

Lesson Self-Check Answer Key

Q1) Call Admission Control (CAC)

Q2) Bandwidth = Number of calls * Codec Bandwidth * 2

Q3) **bandwidth**

Q4) **show gatekeeper zone status**

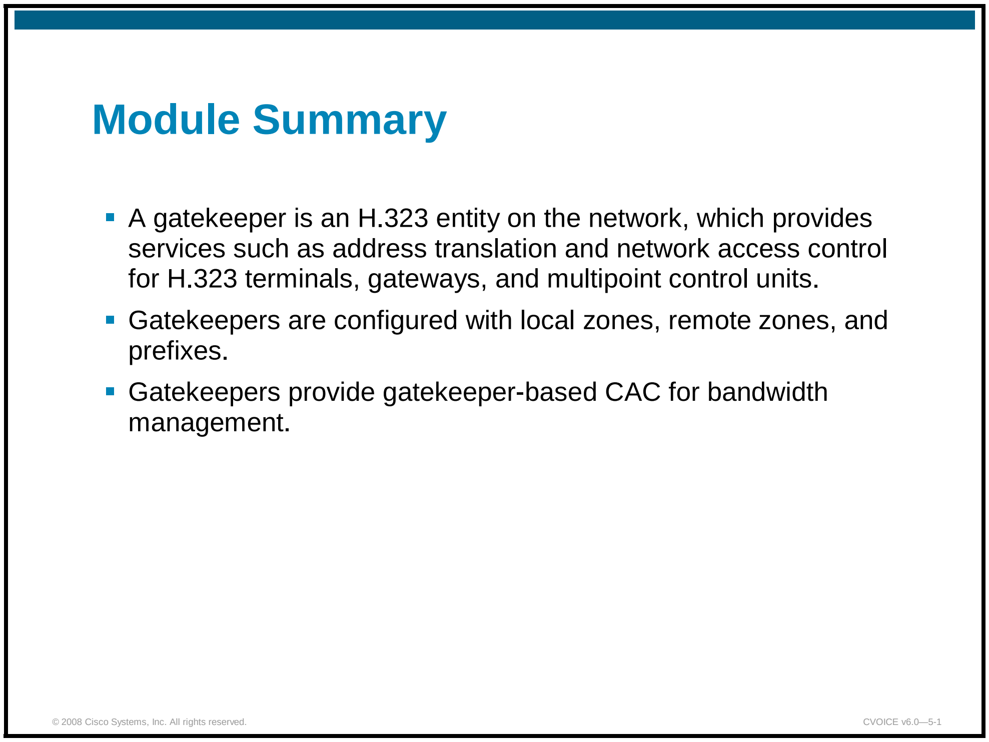
Q5) Resource Ability Indicator (RAI)

Q6) **resource threshold**

Q7) **show call resource voice threshold**

Module Summary

This topic summarizes the key points that were discussed in this module.



Module Summary

- A gatekeeper is an H.323 entity on the network, which provides services such as address translation and network access control for H.323 terminals, gateways, and multipoint control units.
- Gatekeepers are configured with local zones, remote zones, and prefixes.
- Gatekeepers provide gatekeeper-based CAC for bandwidth management.

This module discussed which functions gatekeepers provide, how these devices signal endpoints, and how gatekeepers provide a means for redundancy. The module also talked about directory gatekeepers and how gatekeeper CAC is used to manage bandwidth in H.323 VoIP networks. Knowing how to manage gatekeepers and configure these devices is very important in an H.323-converged network.

References

For additional information, refer to these resources:

- *Cisco IOS H.323 Configuration Guide:* http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_configuration_guide_chapter09186a00801fc997.html#wp1013623
- *Cisco IOS Voice Command Reference:* http://www.cisco.com/en/US/products/ps6441/products_command_reference_book09186a00804973c0.html
- *Cisco Voice Gateways and Gatekeepers, Cisco Press*

Module 6

ITSP Connectivity

Overview

A Cisco Unified Border Element (Cisco UBE) has the ability to interconnect voice and VoIP networks, offering protocol interworking, address hiding, and security services.

This module gives an overview of the Cisco UBE functionality and describes how to implement a Cisco UBE within an enterprise voice network.

Module Objectives

Upon completing this module, you will be able to describe and configure a Cisco UBE within a Cisco Unified Communications network. This ability includes being able to meet these objectives:

- Describe Cisco UBE functions and features and how a Cisco UBE is used in current enterprise environments
- Implement a Cisco UBE to provide protocol interworking

Lesson 1

Understanding Special Requirements for External VoIP Connections

Overview

The Cisco Unified Border Element (Cisco UBE) is similar to a traditional voice gateway, the main difference being the replacement of physical voice trunks with an IP connection. This lesson describes the concepts and features of a Cisco UBE in enterprise environments.

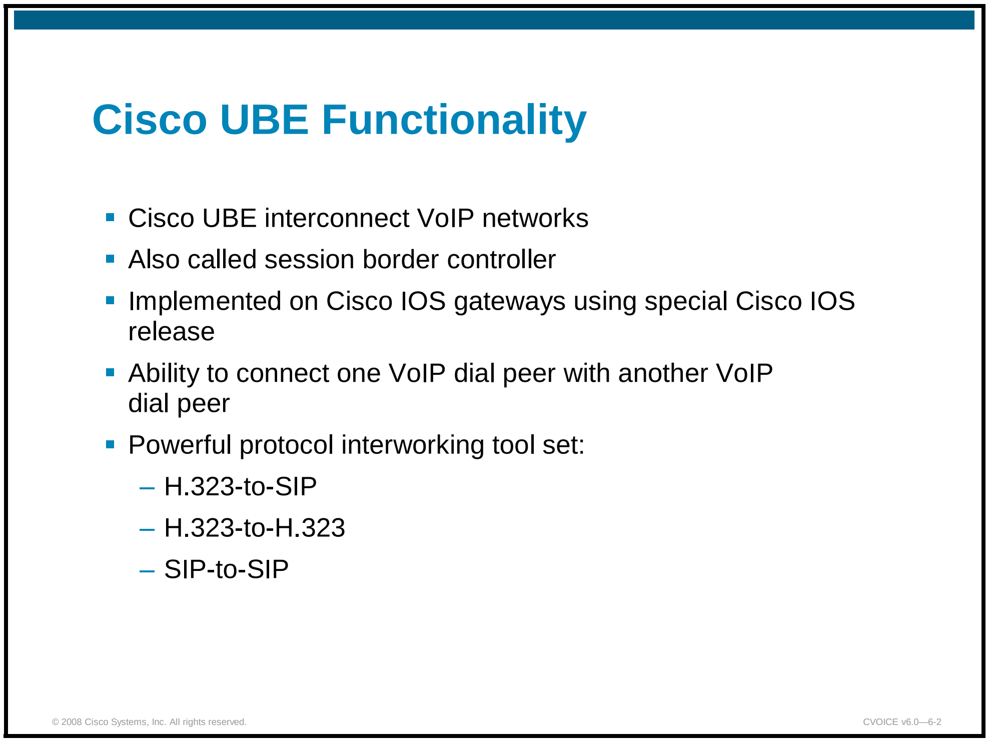
Objectives

Upon completing this lesson, you will be able to describe how Cisco UBEs are used in enterprise environments. This ability includes being able to meet these objectives:

- Describe the functionality of a Cisco UBE
- Describe how Cisco UBEs can be utilized in enterprise VoIP environments
- Describe how protocol interworking is performed on Cisco UBEs
- Describe how Cisco UBEs handle media flows
- Describe how Cisco UBEs perform codec filtering
- Describe how Cisco UBEs can be used to perform RSVP-based CAC
- Describe how a Cisco UBE can be integrated with gatekeeper networks
- Describe call flows involving Cisco UBEs

Cisco UBE Functionality

This topic describes the functionality of a Cisco UBE.



Cisco UBE Functionality

- Cisco UBE interconnect VoIP networks
- Also called session border controller
- Implemented on Cisco IOS gateways using special Cisco IOS release
- Ability to connect one VoIP dial peer with another VoIP dial peer
- Powerful protocol interworking tool set:
  - H.323-to-SIP
  - H.323-to-H.323
  - SIP-to-SIP

CVOICE v6.0—6-2

The Cisco UBE is an intelligent unified communications network border element. A Cisco UBE terminates and reoriginates both signaling (H.323 and SIP) and media streams (Real-Time Transport Protocol [RTP] and Real-Time Transport Control Protocol [RTCP]) while performing border interconnection services between IP networks. The Cisco UBE is formerly known as the Cisco Multiservice IP-to-IP Gateway. The Cisco UBE, in addition to other Cisco IOS software features, includes Session Border Controller (SBC) functions that help enable end-to-end IP-based transport of voice, video, and data between independent unified communications networks.

Originally, SBCs were used by service providers (SPs) to enable full billing capabilities within VoIP networks. But the functionality to interconnect VoIP networks is becoming more and more important for enterprise VoIP networks as well, because VoIP is becoming the new standard for any telephony solution.

Designed to meet enterprise and service-provider Session Border Controller device needs, the Cisco UBE is an integrated Cisco IOS software application that runs on various Cisco router platforms. For a list of platforms, see the following link: http://www.cisco.com/en/US/products/sw/voicesw/ps5640/products_white_paper0900aecd8067937f.shtml

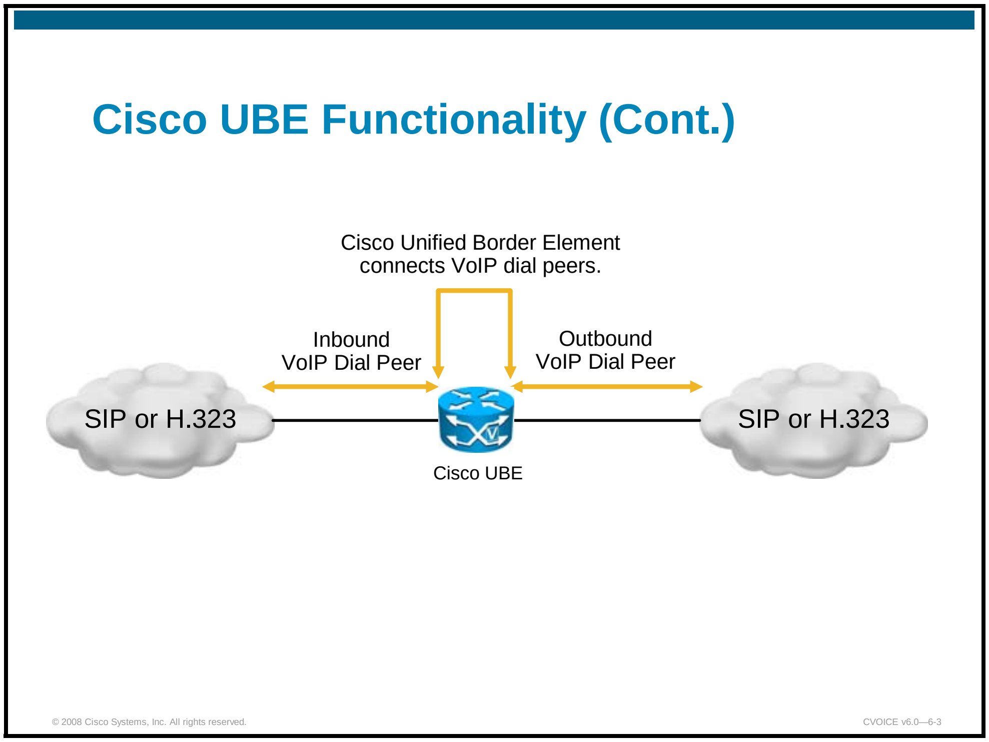
Cisco UBE functionally is implemented on Cisco IOS gateways using a special Cisco IOS feature set. Using this feature set, a Cisco UBE can route a call from one VoIP dial peer to another VoIP dial peer.

VoIP dial peers can also be handled by either the session initiation protocol (SIP) or H.323. As a result, the ability to interconnect VoIP dial peers also includes the ability to interconnect

VoIP networks using different signaling protocols, or VoIP networks using the same signaling protocols but facing interoperability issues.

Protocol interworking includes these combinations:

- H.323-to-SIP interworking
- H.323-to-H.323 interworking
- SIP-to-SIP interworking



Cisco UBE Functionality (Cont.)

Cisco Unified Border Element connects VoIP dial peers.

This figure illustrates the capability of Cisco UBE to interconnect VoIP networks, including VoIP networks that use different signaling protocols. VoIP interworking is achieved by connecting an inbound VoIP dial peer with an outbound VoIP dial peer. A standard Cisco IOS gateway without the Cisco UBE functionality will not allow VoIP-to-VoIP connections.

The Cisco UBE provides a network-to-network interface point for:

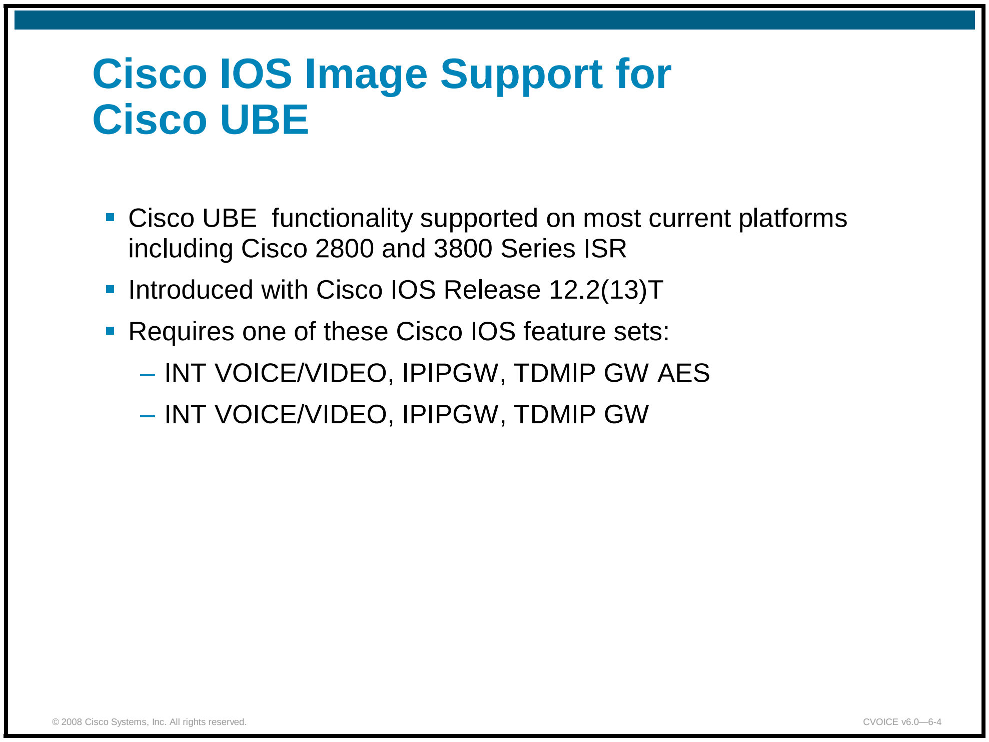
- Signaling interworking (H.323, SIP)
- Media interworking (dual-tone multifrequency [DTMF], fax, modem, and coder-decoder [codec] transcoding)
- Address and port translations (privacy and topology hiding)
- Billing and call detail record (CDR) normalization
- Quality of service (QoS) and bandwidth management (QoS marking using differentiated services code point [DSCP] or type of service [ToS], bandwidth enforcement using Resource Reservation Protocol [RSVP] and codec filtering)

A Cisco UBE interoperates with many different network elements including voice gateways, IP phones, and call-control servers in many different application environments, from advanced enterprise voice and/or video services with Cisco Unified Communications Manager or Cisco Unified Communications Manager Express, as well as simpler toll bypass and voice over IP (VoIP) transport applications.

The Cisco UBE provides organizations with all the border controller functions integrated into the network layer to interconnect unified communications voice and video enterprise-to-service-provider architectures. The Cisco UBE is used by enterprise and small and medium-sized organizations to interconnect SIP PSTN access with SIP and H.323 enterprise unified communications networks.

Cisco IOS Image Support for Cisco UBE Gateways

This subtopic describes which Cisco IOS images support the Cisco UBE functionality.



Cisco IOS Image Support for Cisco UBE

- Cisco UBE functionality supported on most current platforms including Cisco 2800 and 3800 Series ISR
- Introduced with Cisco IOS Release 12.2(13)T
- Requires one of these Cisco IOS feature sets:
  - INT VOICE/VIDEO, IPIPGW, TDMIP GW AES
  - INT VOICE/VIDEO, IPIPGW, TDMIP GW

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—6-4

The Cisco UBE functionality is supported on most current Cisco IOS routers, including the Cisco 2800 and 3800 Series Integrated Services Routers (ISRs). The first Cisco IOS release supporting the Cisco UBE functionality was Cisco IOS Release 12.2(13)T. However, many of the newer features of the Cisco UBE were introduced with Cisco IOS Release 12.4T, so you should use this more current Cisco IOS release. Visit this site for detailed information about features and version dependency:

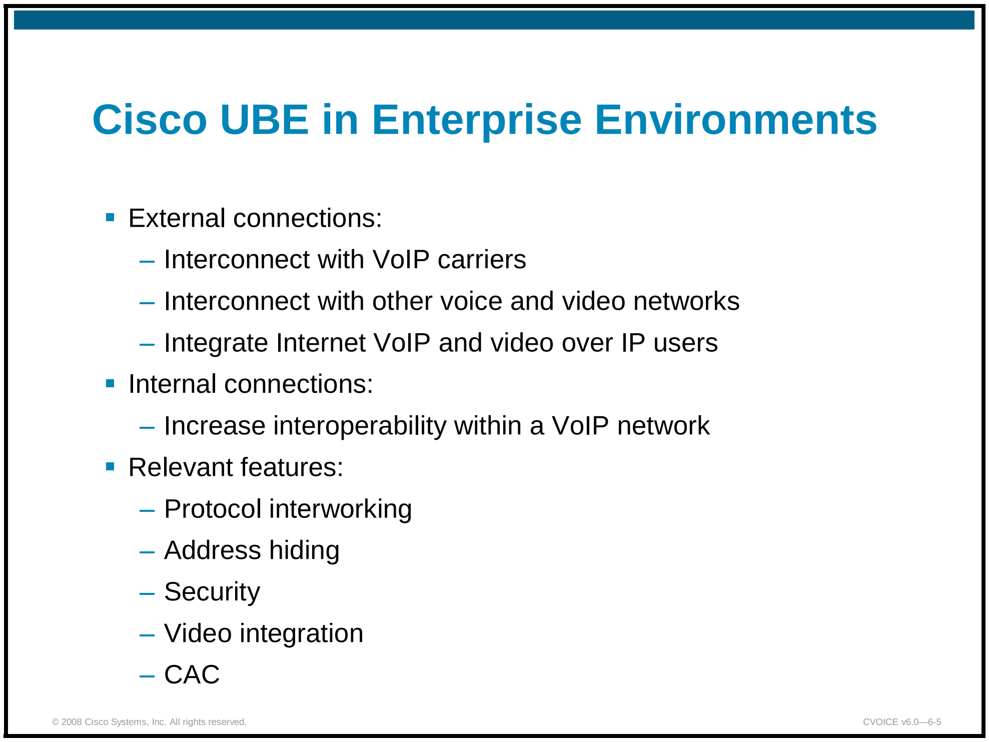
http://www.cisco.com/en/US/products/sw/voicesw/ps5640/products_configuration_guide_book09186a0080409b6d.html

The Cisco UBE is supported in the following Cisco IOS feature sets:

- Integrated Voice and Video (INT VOICE/VIDEO), Cisco Multiservice IP-to-IP gateway (IPIPGW), Time-Division Multiplexing gateway (TDMIP GW AES)
- INT VOICE/VIDEO, IPIPGW, TDMIP GW

Cisco UBE Gateways in Enterprise Environments

This topic describes how Cisco UBEs can be utilized in enterprise VoIP environments.



Cisco UBE in Enterprise Environments

- External connections:
  - Interconnect with VoIP carriers
  - Interconnect with other voice and video networks
  - Integrate Internet VoIP and video over IP users
- Internal connections:
  - Increase interoperability within a VoIP network
- Relevant features:
  - Protocol interworking
  - Address hiding
  - Security
  - Video integration
  - CAC

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—6-5

Cisco UBE in enterprise deployments serve two main purposes:

- **External connections:** A Cisco UBE can be used as a demarcation point within unified communications network and provides interconnectivity with external networks. This includes H.323 voice and video connections and SIP VoIP connections.
- **Internal connections:** When used within a VoIP network, a Cisco UBE can be used to increase the flexibility and interoperability between different devices.

These are some key features offered by Cisco UBE:

- **Protocol interworking:** The Cisco UBE supports interworking of signaling protocols, including H.323-to-H.323, H.323-to-SIP, and SIP-to-SIP.
- **Address hiding:** A Cisco UBE can hide or replace the endpoint IP addresses used for the media connection.
- **Security:** A Cisco UBE can be placed in a demilitarized zone (DMZ) and provide outside connectivity to external networks.
- **Video integration:** In addition to VoIP services, a Cisco UBE also supports H.323 video connections.
- **Call Admission Control (CAC):** A Cisco UBE can use Cisco IOS-based CAC mechanisms, including the Resource Reservation Protocol (RSVP).

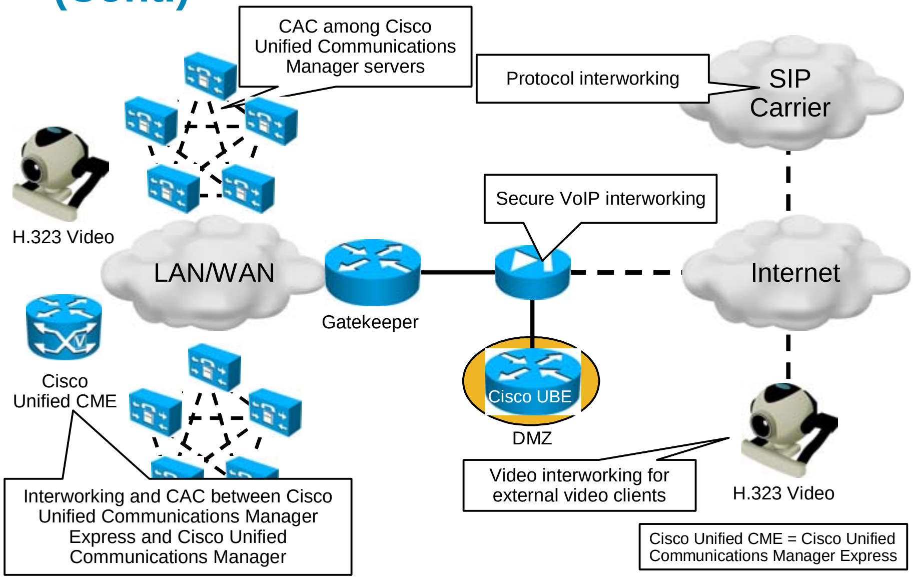
The "Key Features of the Cisco UBE Gateway" table lists key features and capabilities of the Cisco UBE. For detailed information about the Cisco UBE, visit the product page: http://www.cisco.com/en/US/products/sw/voicesw/ps5640/products_data_sheet09186a00801da698.html

Key Features of the Cisco UBE Gateway

Feature	Details
Protocols	H.323 and SIP
Network hiding	■ IP network privacy and topology hiding ■ IP network security boundary ■ Intelligent IP address translation for call media and signaling ■ Back-to-back user agent, replacing all SIP-embedded IP addressing
CAC	■ Resource Reservation Protocol (RSVP) ■ Maximum number of calls per trunk (max calls) ■ CAC based on IP circuits ■ CAC based on total calls, CPU usage, or memory usage thresholds
Protocol and signal interworking	■ H.323 to H.323 (including Cisco Unified Communications Manager) ■ H.323 to SIP (including Cisco Unified Communications Manager) ■ SIP to SIP (including Cisco Unified Communications Manager)
Media support	RTP and RTCP
Media modes	■ Media flow-through ■ Media flow-around
Video codecs	H.261, H.263, and H.264
Transport mode	■ TCP ■ User Datagram Protocol (UDP) ■ TCP-to-UDP interworking
DTMF	■ H.245 alphanumeric ■ H.245 signal ■ RFC 2833 ■ SIP Notify ■ Key Press Markup Language (KPML) Interworking capabilities: ■ H.323 to SIP ■ RFC 2833 to G.711 Inband DTMF
Fax support	■ T.38 Fax Relay ■ Fax pass-through ■ Cisco Fax Relay
Modem support	■ Modem pass-through ■ Cisco Modem Relay

Supplementary services	■ Call hold, call transfer, and call forward for H.323 networks using H.450 and transparent passing of Empty Capability Set (ECS) ■ SIP-to-SIP supplementary services (holds and transfers) support using the SIP REFER method. ■ H.323-to-SIP supplementary services for Cisco Unified Communications Manager with Media Termination Point (MTP) on the H.323 trunk
Network Address Translation (NAT) Traversal	■ NAT Traversal support for SIP phones deployed behind non-Application Line Gateway (ALG) data routers ■ Stateful NAT Traversal
QoS	IP Precedence and differentiated services code point (DSCP) marking
Voice-quality statistics	Packet loss, jitter, and round-trip time
Number translation	■ Number translation rules for VoIP numbers ■ Electronic Numbering (ENUM) support for E.164 number mapping into Domain Name System (DNS)
Codecs	■ G711 mu-law and a-law ■ G723ar53, G723ar63, G723r53, and G723r63 ■ G726r16, G726r24, and G726r32 ■ G728 ■ G729, G729A, G729B, and G729AB ■ Internet Low Bitrate Codec (iLBC)
Transcoding	Transcoding between any two different family of codecs from the following list: ■ G711 a-law and mu-law ■ G.729, G.729A, G.729B, and G.729AB ■ G.723 (5.3 and 6.3 kb/s) ■ internet Low Bit Rate Codec (iLBC)
Security	■ IP Security (IPsec) ■ Secure RTP (SRTP) ■ Transport Layer Security (TLS)
Authentication, authorization, and accounting (AAA)	AAA with Remote Authentication Dial-In User Service (RADIUS)
Voice media applications	■ Tool Command Language (TCL) scripts support for application customization ■ Voice Extensible Markup Language (VoiceXML 2.0) script support for application customization
Billing	Standard call detail records (CDRs) for accurate billing available through: ■ AAA records ■ Syslog ■ Simple Network Management Protocol (SNMP)

Cisco UBE in Enterprise Environments (Cont.)



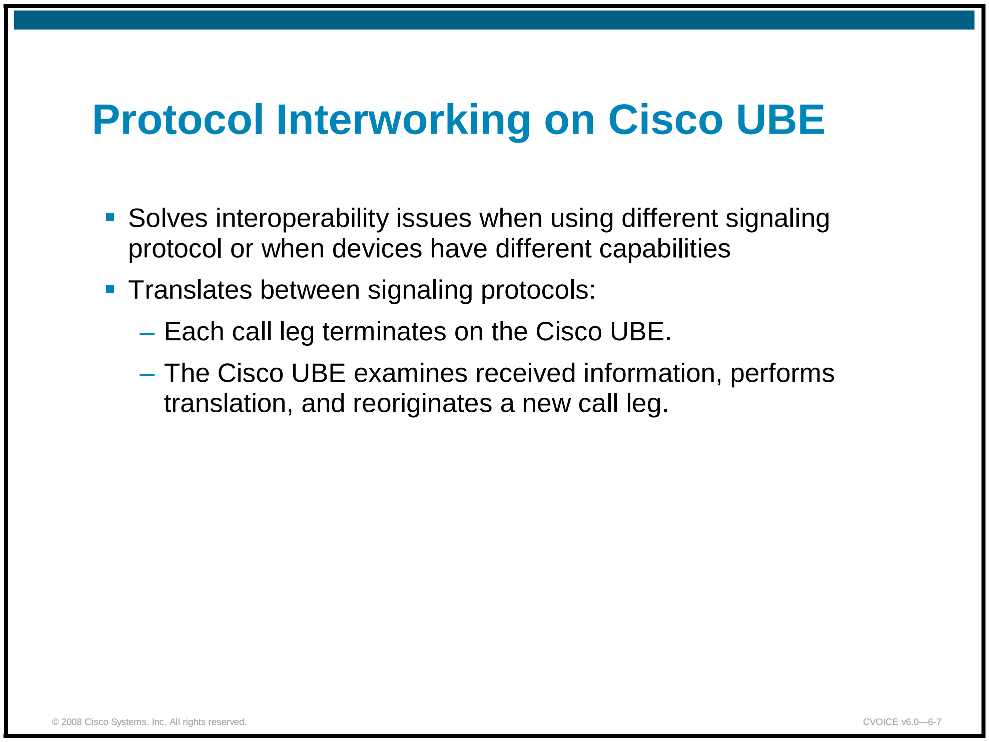
CAC among Cisco Unified Communications Manager servers
Protocol interworking
SIP Carrier
H.323 Video
Secure VoIP interworking
LAN/WAN
Gatekeeper
Internet
Cisco Unified CME
Cisco UBE
DMZ
Interworking and CAC between Cisco Unified Communications Manager Express and Cisco Unified Communications Manager
Video interworking for external video clients
H.323 Video
Cisco Unified CME = Cisco Unified Communications Manager Express

CVOICE v6.0—6-6

This figure shows the various deployment options for a Cisco UBE. Depending on the deployment scenario, multiple Cisco UBEs might be required. Whether the gateways are being deployed within a single VoIP network or used to interconnect to external VoIP networks, the same concepts apply.

Protocol Interworking on Cisco UBE Gateways

This topic describes how protocol interworking is supported on Cisco UBE.



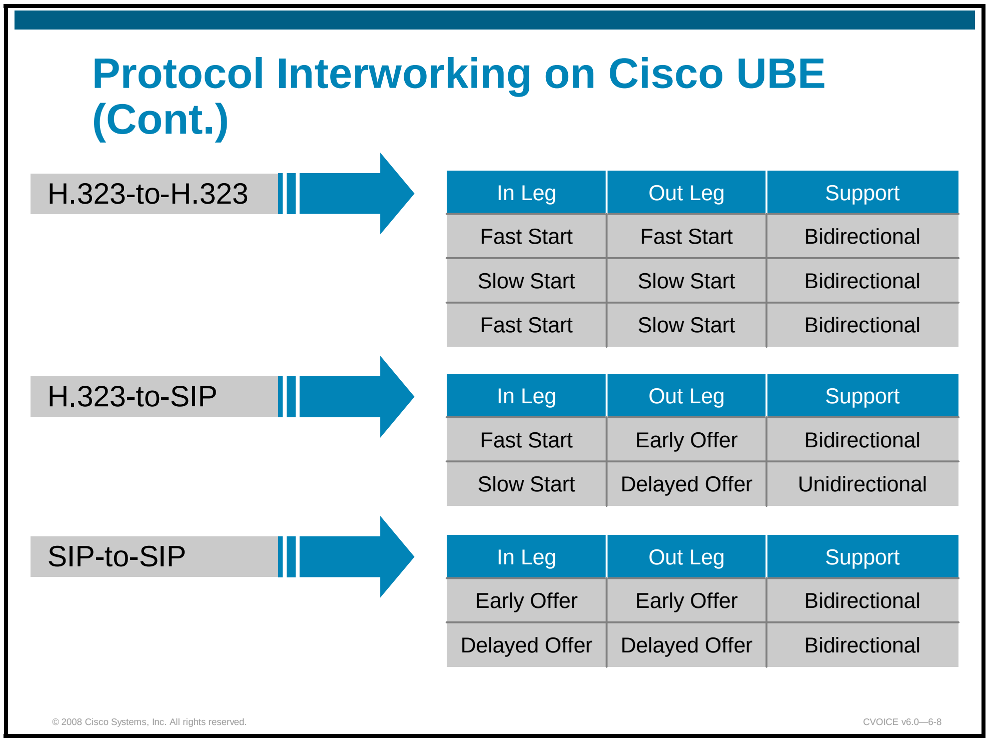
Protocol Interworking on Cisco UBE

- Solves interoperability issues when using different signaling protocol or when devices have different capabilities
- Translates between signaling protocols:
  - Each call leg terminates on the Cisco UBE.
  - The Cisco UBE examines received information, performs translation, and reoriginates a new call leg.

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—6-7

Interworking signaling protocols on Cisco UBE is similar to using a proxy. This feature can be used for two scenarios:

- **Interworking between the same signaling protocol:** A Cisco UBE that is interworking between the same signaling protocol (for example H.323-to-H.323) can be used to solve interoperability issues between two devices having different capabilities. Because the Cisco UBE builds two different call legs to each peer, it can work between those two call legs. For example, Cisco Unified Communications Manager Express uses H.450, a subset of H.323, for call transfers and call forwarding. When connected directly to a Cisco Unified Communications Manager, which does not support H.450, call forwarding and transfers might lead to hair pinned calls (calls that are sent back out of the same interface they entered) and suboptimal WAN usage. A Cisco UBE at the Cisco Unified Communications Manager site can be used to solve these issues.
- **Interworking between different signaling protocols:** A Cisco UBE can interconnect dial peers that use different signaling protocols, such as a SIP and an H.323 dial peer. This allows for greater flexibility when deploying an IP communications network.



Protocol Interworking on Cisco UBE (Cont.)

H.323-to-H.323

In Leg	Out Leg	Support
Fast Start	Fast Start	Bidirectional
Slow Start	Slow Start	Bidirectional
Fast Start	Slow Start	Bidirectional

H.323-to-SIP

In Leg	Out Leg	Support
Fast Start	Early Offer	Bidirectional
Slow Start	Delayed Offer	Unidirectional

SIP-to-SIP

In Leg	Out Leg	Support
Early Offer	Early Offer	Bidirectional
Delayed Offer	Delayed Offer	Bidirectional

CVOICE v6.0—6-8

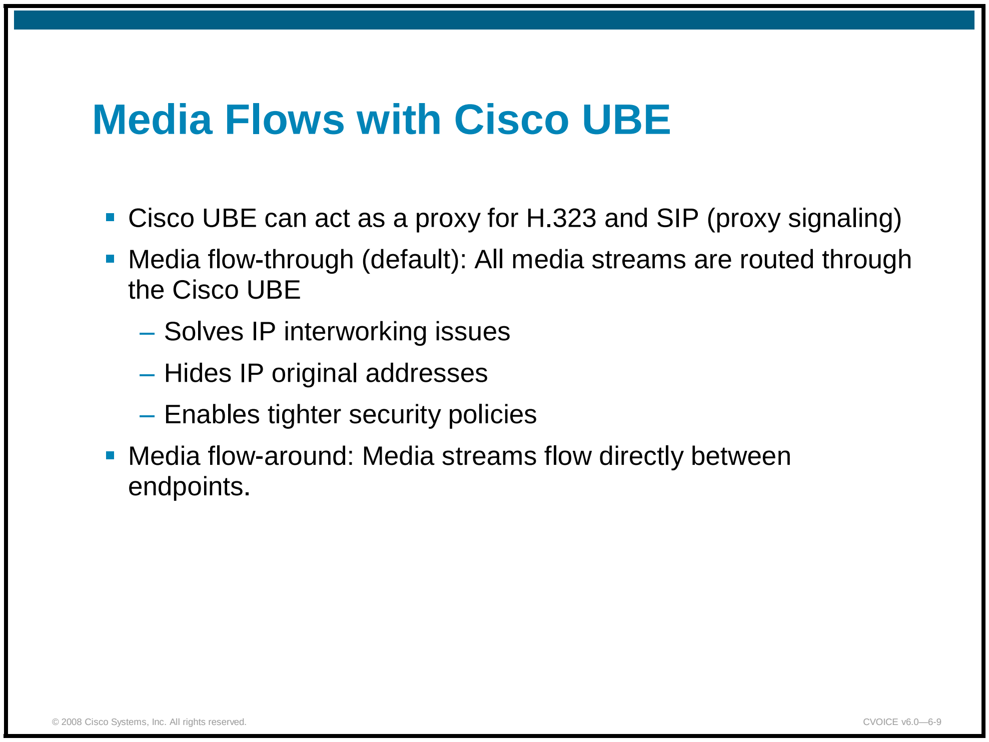
Both H.323 and SIP support two methods of call setups. H.323 uses fast start and slow start, whereas SIP uses early offer and delayed offer. Both H.323 fast start and SIP early offer are used to set up the media channel faster than during standard call setup. Problems arise when one endpoint expects an H.323 slow start or SIP delayed offer and the other endpoints uses H.323 fast start or SIP early offer.

When interworking signaling protocols, a Cisco UBE supports these combinations:

- **H.323-to-H.323:** An Cisco UBE fully supports fast start with slow start interworking in all directions.
- **H.323-to-SIP:** H.323 fast start to SIP early offer interworking is fully supported. An H.323 slow start to a SIP delayed offer is only supported for inbound H.323 to outbound SIP calls.
- **SIP-to-SIP:** Early offer and delayed offer are fully supported on a Cisco UBE in all directions.

Media Flows on Cisco UBE Gateways

This topic describes how a Cisco UBE handles media flows.



Media Flows with Cisco UBE

- Cisco UBE can act as a proxy for H.323 and SIP (proxy signaling)
- Media flow-through (default): All media streams are routed through the Cisco UBE
  - Solves IP interworking issues
  - Hides IP original addresses
  - Enables tighter security policies
- Media flow-around: Media streams flow directly between endpoints.

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—6-9

Because a Cisco UBE is a signaling proxy, it also processes all signaling messages regarding the setup of the media channels. This enables a Cisco UBE to affect the flow of media traffic. Two options exist: media flow-through and media flow-around.

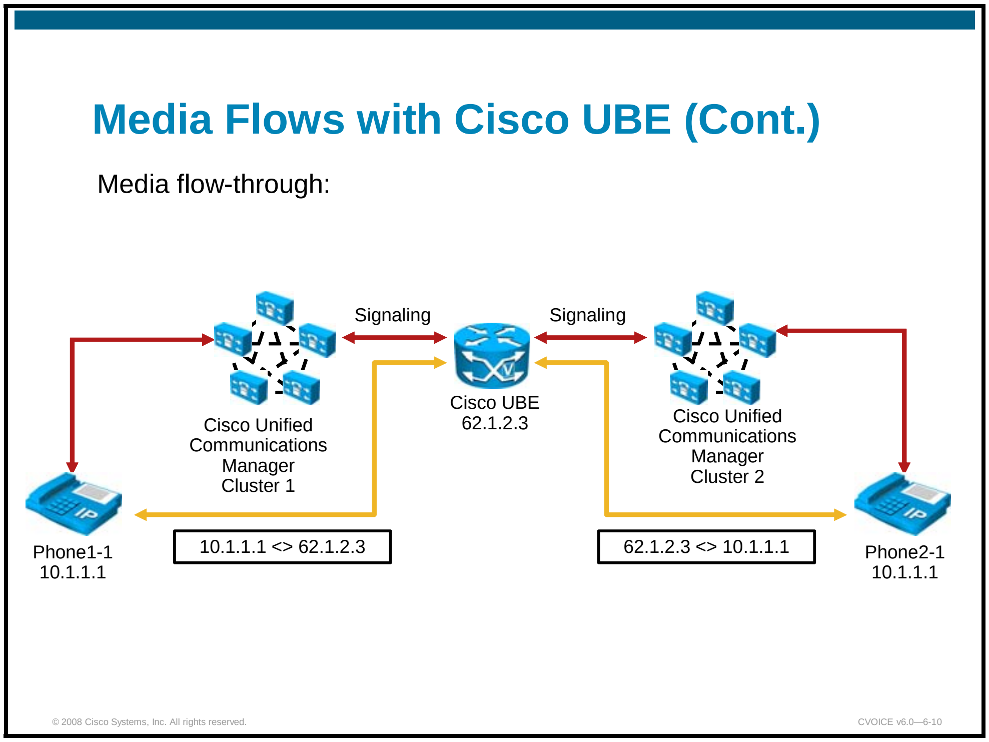
When using media flow-through, a Cisco UBE replaces the source IP address used for media connections with its own IP addresses. This operation can be utilized in different ways:

- It solves IP interworking issues, because the Cisco UBE replaces potential duplicate IP addresses with a single, easy-to-control IP address.
- It hides the original endpoint IP address from the remote endpoints.

This makes a Cisco UBE with media flow-through ideal for interworking with external VoIP networks and enforcing a tighter security policy.

When using a Cisco UBE internally, media flow-through might not be necessary or even desirable. One of the main drawbacks when using media flow-through is the higher load on a Cisco UBE router, which decreases the number of supported concurrent flows. In addition, media flow-through might result in suboptimal traffic flows, because direct endpoint-to-endpoint communications is prohibited. Thus a Cisco UBE can also be configured for media flow-around.

When using media flow-around, a Cisco UBE leaves the IP addresses used for the media connections untouched. Call signaling will still be processed by the Cisco UBE, but after the call is set up, the Cisco UBE is no longer involved with the traffic flow.



Media Flows with Cisco UBE (Cont.)

Media flow-through:

Signaling

Signaling

Cisco Unified Communications Manager Cluster 1

Cisco UBE
62.1.2.3

Cisco Unified Communications Manager Cluster 2

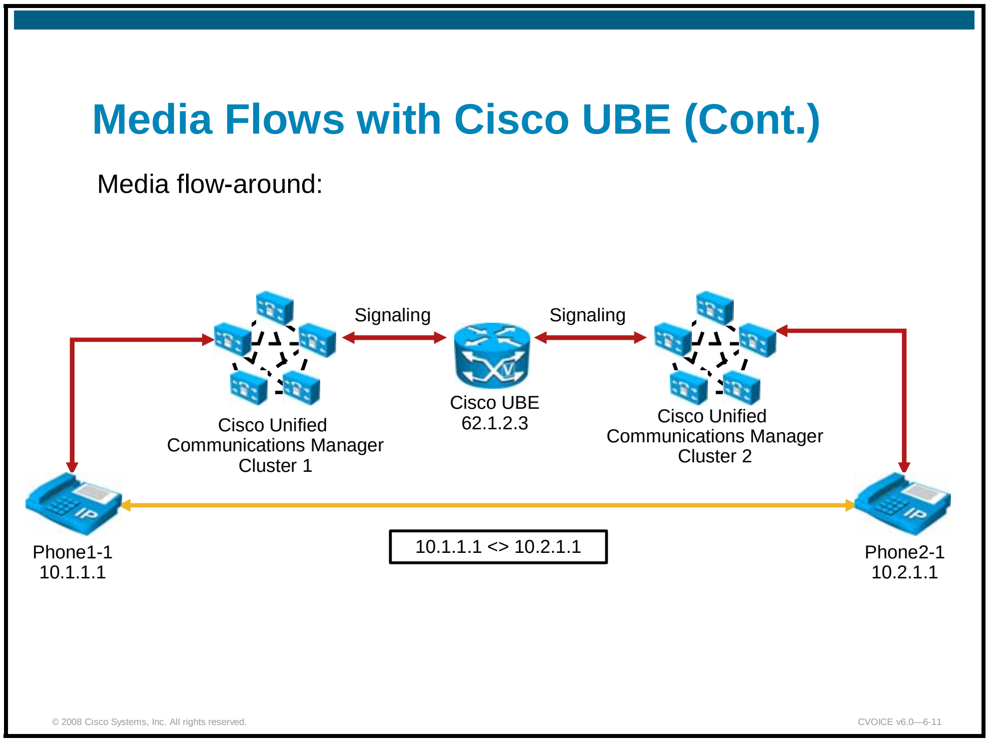
Phone1-1
10.1.1.1

10.1.1.1 <> 62.1.2.3

62.1.2.3 <> 10.1.1.1

Phone2-1
10.1.1.1

This figure shows a Cisco UBE configured for media flow-through. The signaling between the two Cisco Unified Communications Manager clusters is processed by the Cisco UBE, and the source IP addresses of the endpoints are replaced by the Cisco UBE IP address. Both endpoints have the same IP address, but because the Cisco UBE is involved, no interworking issues arise.



Media Flows with Cisco UBE (Cont.)

Media flow-around:

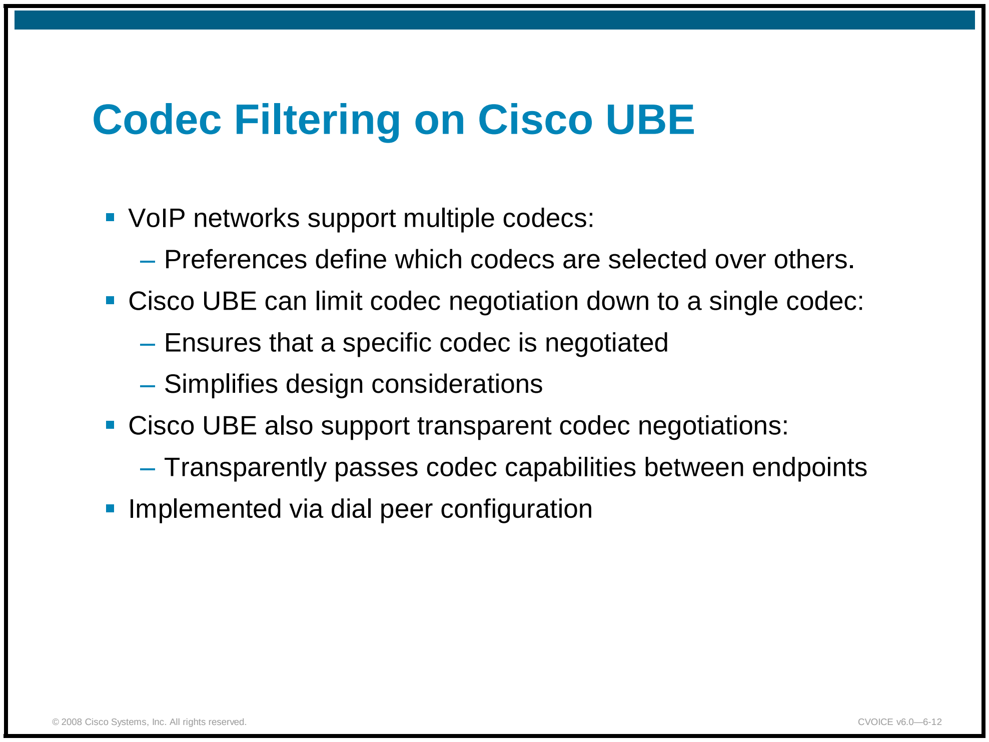
CVOICE v6.0—6-11

This figure shows a Cisco UBE configured for media flow-around. No duplicate IP address ranges exist, and IP address hiding is not required, so media flow-through is not required. The Cisco UBE still processes all signaling traffic, but the endpoints have direct media channels.

You would use media flow-around when you are not concerned with hiding your network addresses.

Codec Filtering on Cisco UBE Gateways

This topic describes how codec filtering is performed by a Cisco UBE.



Codec Filtering on Cisco UBE

- VoIP networks support multiple codecs:
  - Preferences define which codecs are selected over others.
- Cisco UBE can limit codec negotiation down to a single codec:
  - Ensures that a specific codec is negotiated
  - Simplifies design considerations
- Cisco UBE also support transparent codec negotiations:
  - Transparently passes codec capabilities between endpoints
- Implemented via dial peer configuration

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—6-12

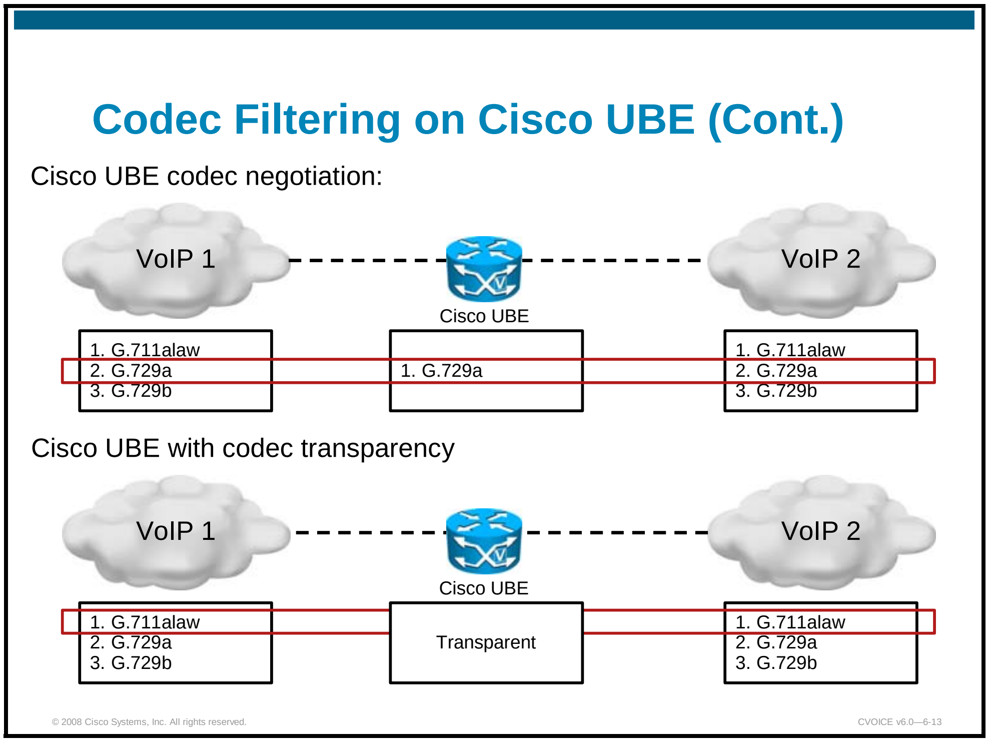
VoIP networks usually support a large variety of codecs, and mechanisms exist to perform codec negotiations between devices. Regardless of which mechanisms are used, preferences determine which codecs will be selected over others.

Because a Cisco UBE is essentially a Cisco IOS gateway with the ability to interconnect VoIP dial peers, the same codec selections mechanisms are available as on any other Cisco IOS gateway. A dial peer can be configured to allow a specific codec or to use a codec voice class to specify multiple codecs with a preference order. This enables a Cisco UBE to perform codec filtering, because a dial peer will only set up a call leg if the desired codec criteria are satisfied. This adds to the Cisco UBE role of a demarcation point within a VoIP network.

If codec filtering is not required, a Cisco UBE also supports transparent codec negotiations. This enables negotiations between endpoints with the Cisco UBE simply by leaving the codec information untouched.

Whether performing codec filtering or operating in transparent mode, a Cisco UBE is required to support the codec used between endpoints. These codecs are supported:

- **Audio codecs:** G.711u, G.711a, G.723, G.726, G.729r8, G.728, and Adaptive Multirate Narrow Band (AMR-NB)
- **Video codecs (H.323 only):** H.261, H.263, and H.264



Codec Filtering on Cisco UBE (Cont.)

Cisco UBE codec negotiation:

VoIP 1

1. G.711alaw
2. G.729a
3. G.729b

Cisco UBE

1. G.729a

VoIP 2

1. G.711alaw
2. G.729a
3. G.729b

Cisco UBE with codec transparency

VoIP 1

1. G.711alaw
2. G.729a
3. G.729b

Cisco UBE

Transparent

VoIP 2

1. G.711alaw
2. G.729a
3. G.729b

CVOICE v6.0—6-13

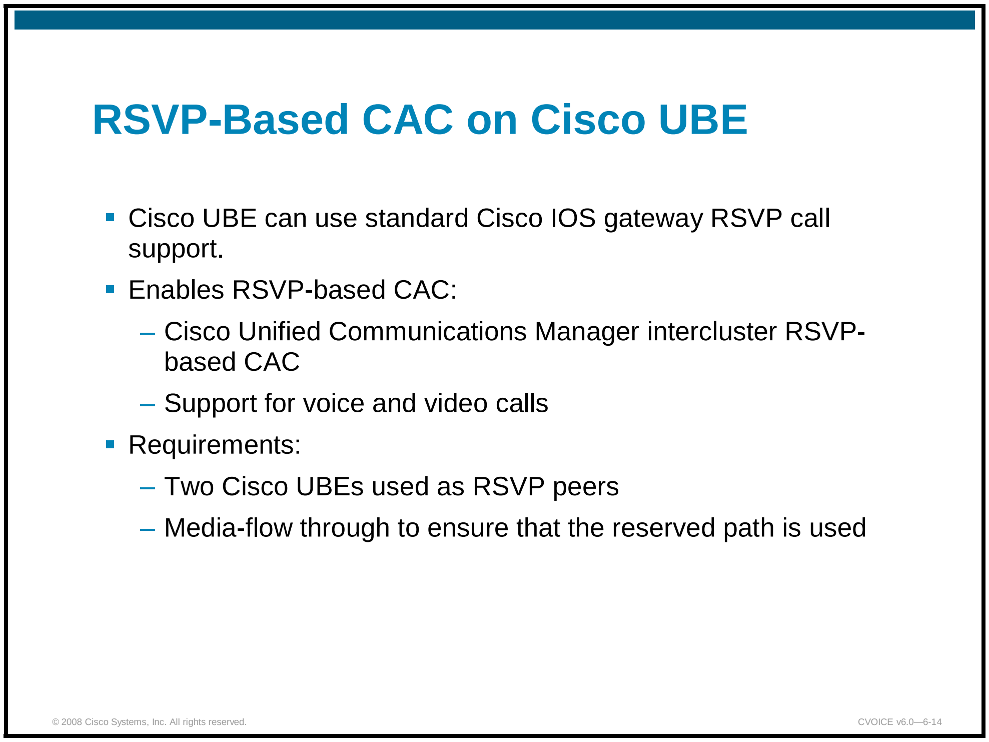
This figure shows how codec negotiation is performed on a Cisco UBE. Two VoIP clouds need to be interconnected. In this scenario, both VoIP 1 and VoIP 2 networks have G.711alaw as the preferred codec.

In the first example, the Cisco UBE is configured to use the G.729a codec. This can be done by simply using the appropriate **codec** command on both VoIP dial peers. When a call is set up, the Cisco UBE will only accept G.729a calls, thus influencing the codec negotiation.

In the second example, the Cisco UBE is configured for a transparent codec and will leave the codec information contained within the call signaling untouched. Because both VoIP 1 and VoIP 2 have G.711alaw as their first choice, the resulting call will be a G.711alaw call.

RSVP-Based CAC on Cisco UBE Gateways

This topic describes how Cisco UBE can be used to perform RSVP-based CAC.

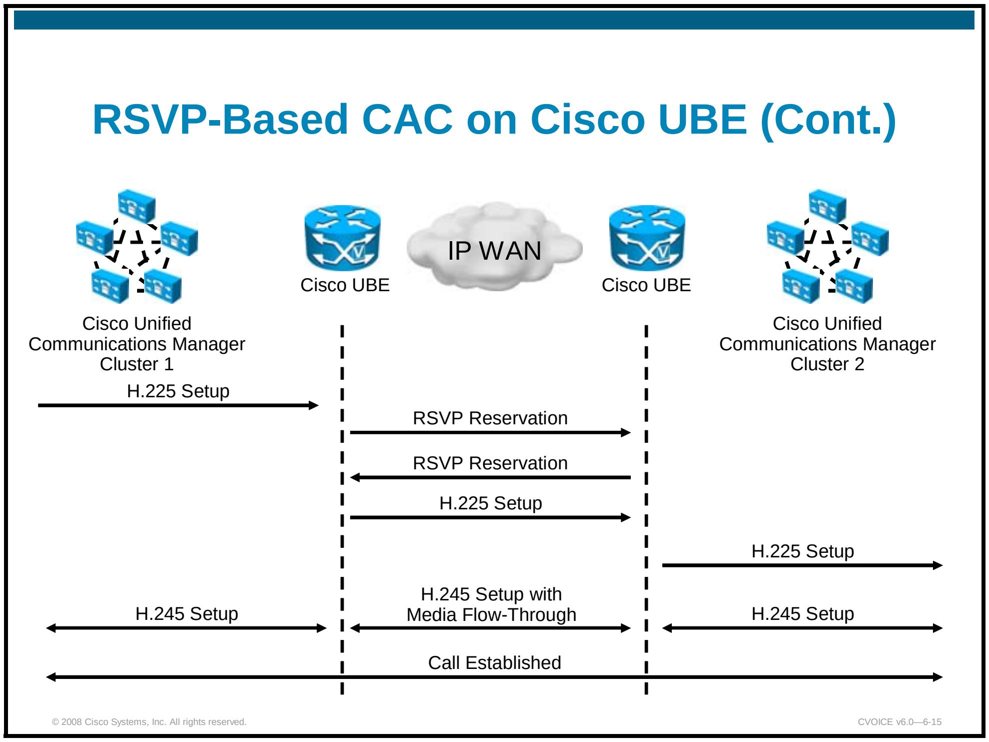


RSVP-Based CAC on Cisco UBE

- Cisco UBE can use standard Cisco IOS gateway RSVP call support.
- Enables RSVP-based CAC:
  - Cisco Unified Communications Manager intercluster RSVP-based CAC
  - Support for voice and video calls
- Requirements:
  - Two Cisco UBEs used as RSVP peers
  - Media-flow through to ensure that the reserved path is used

Because the Cisco UBE is a Cisco IOS gateway, it also supports RSVP-based CAC. Two Cisco Unified Communications Manager clusters can interconnect using Cisco UBE, thus enabling intercluster RSVP-based CAC. RSVP supports both voice and video calls.

RSVP requires at least two RSVP peers, so two Cisco UBE Gateways are required to enable RSVP-based CAC. When deploying Cisco UBE and RSVP-based CAC, ensure that the flows that should utilize RSVP are configured for media flow-through. Media flow-around is not supported together with RSVP-based CAC.



RSVP-Based CAC on Cisco UBE (Cont.)

Cisco UBE
IP WAN
Cisco UBE
Cisco Unified Communications Manager Cluster 1
Cisco Unified Communications Manager Cluster 2
H.225 Setup
RSVP Reservation
RSVP Reservation
H.225 Setup
H.225 Setup
H.245 Setup
H.245 Setup with Media Flow-Through
H.245 Setup
Call Established

CVOICE v6.0—6-15

This figure shows an example call setup combined with RSVP-based CAC. Here is the call flow:

Step 1 The Cisco Unified Communications Manager cluster 1 sends an H.225 setup to the Cisco UBE.

Step 2 The Cisco UBE processes the call setup information and associates an outbound VoIP dial peer requiring an RSVP reservation. The Cisco UBE sends out an RSVP request to the remote Cisco UBE.

Step 3 The remote Cisco UBE acknowledges the reservation and initiates the reservation for the return path, which is acknowledged by the local Cisco UBE.

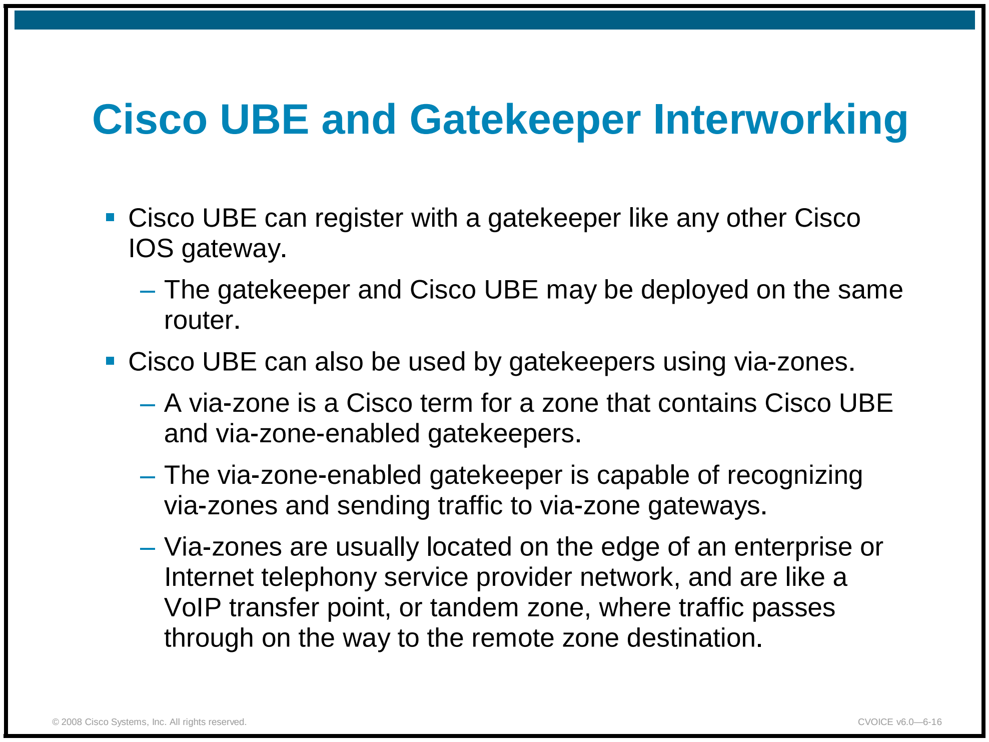
Step 4 The H.225 setup message is routed to the remote Cisco UBE, which then routes the call to the outbound VoIP dial peer pointing to Cisco Unified Communications Manager cluster 2.

Step 5 H.245 negotiation occurs with media flow-through enabled.

Step 6 The call is established.

Cisco UBE Gateways and Gatekeeper Interworking

This topic describes how a Cisco UBE can be integrated with gatekeeper networks.



Cisco UBE and Gatekeeper Interworking

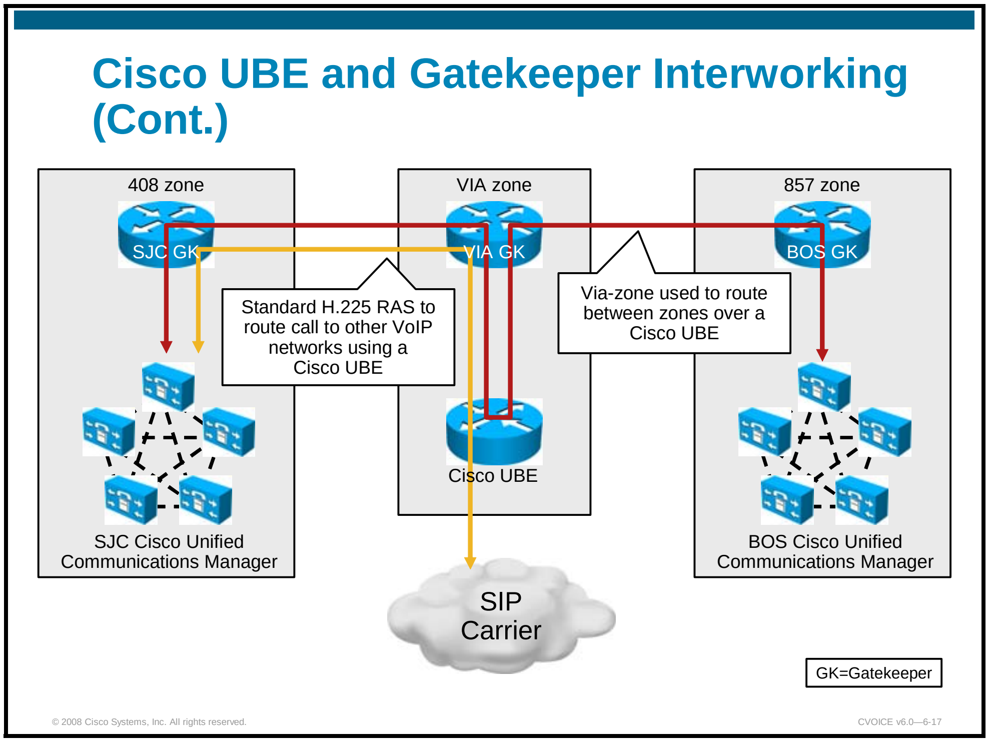
- Cisco UBE can register with a gatekeeper like any other Cisco IOS gateway.
  - The gatekeeper and Cisco UBE may be deployed on the same router.
- Cisco UBE can also be used by gatekeepers using via-zones.
  - A via-zone is a Cisco term for a zone that contains Cisco UBE and via-zone-enabled gatekeepers.
  - The via-zone-enabled gatekeeper is capable of recognizing via-zones and sending traffic to via-zone gateways.
  - Via-zones are usually located on the edge of an enterprise or Internet telephony service provider network, and are like a VoIP transfer point, or tandem zone, where traffic passes through on the way to the remote zone destination.

CVOICE v6.0—6-16

When you are interworking with gatekeepers, the Cisco UBE can be used in two ways. First, it can register with the gatekeeper, similar to a standard Cisco IOS gateway.

Note	Cisco UBE and a gatekeeper can be deployed on the same router, as long as CPU and memory requirements are met.

In addition, a gatekeeper can use a registered Cisco UBE with via-zones. This means that when routing a call between two zones, a gatekeeper can be configured to route the call via a zone containing Cisco UBE. This enables interzone networking using central Cisco UBE without the need to deploy a Cisco UBE at every site or redesigning an already-deployed H.323 network.



Cisco UBE and Gatekeeper Interworking (Cont.)

408 zone
SJC GK
SJC Cisco Unified Communications Manager
VIA zone
VIA GK
Cisco UBE
857 zone
BOS GK
BOS Cisco Unified Communications Manager
SIP Carrier

Standard H.225 RAS to route call to other VoIP networks using a Cisco UBE

Via-zone used to route between zones over a Cisco UBE

GK=Gatekeeper

CVOICE v6.0—6-17

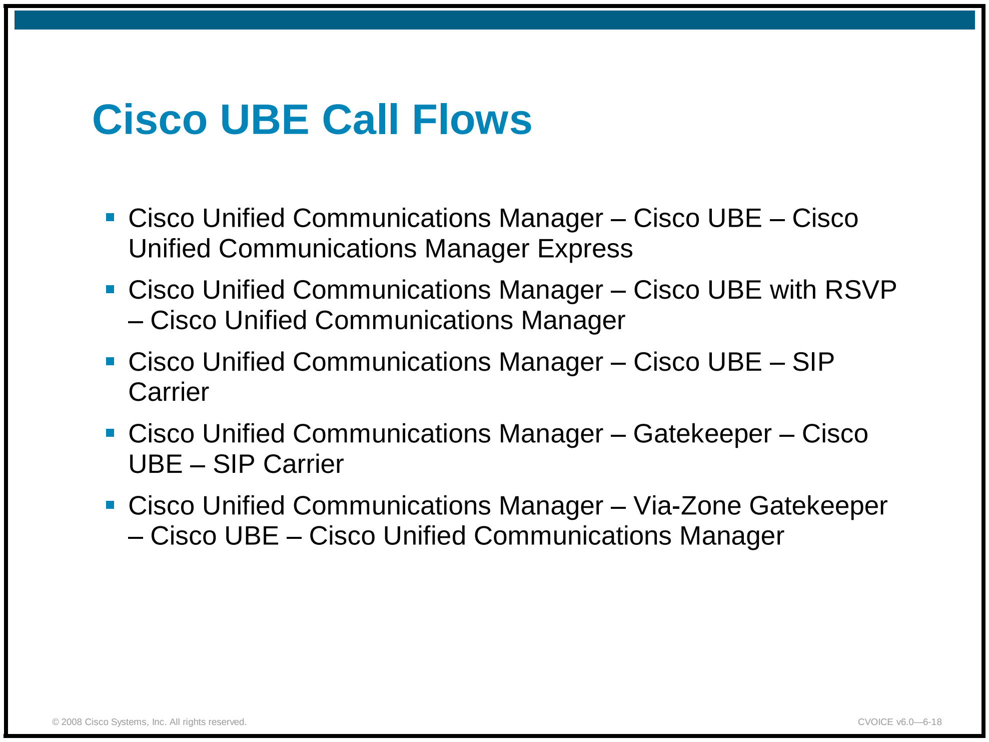
This figure shows how a Cisco UBE is integrated with gatekeeper deployments. The San Jose Campus (SJC) gatekeeper can route calls to the Boston (BOS) gatekeeper or route calls to a SIP carrier through a Cisco UBE.

Use via-zones when routing calls between zones that require Cisco UBE functionality. Existing gatekeeper deployments can easily be modified to include Cisco UBE using this concept.

Note When a Cisco UBE is used as an outbound voice gateway, the same concepts that apply when using traditional voice gateways with gatekeepers apply to Cisco UBE deployments.

Cisco UBE Gateway Call Flows

This topic describes call flows involving Cisco UBE.



Cisco UBE Call Flows

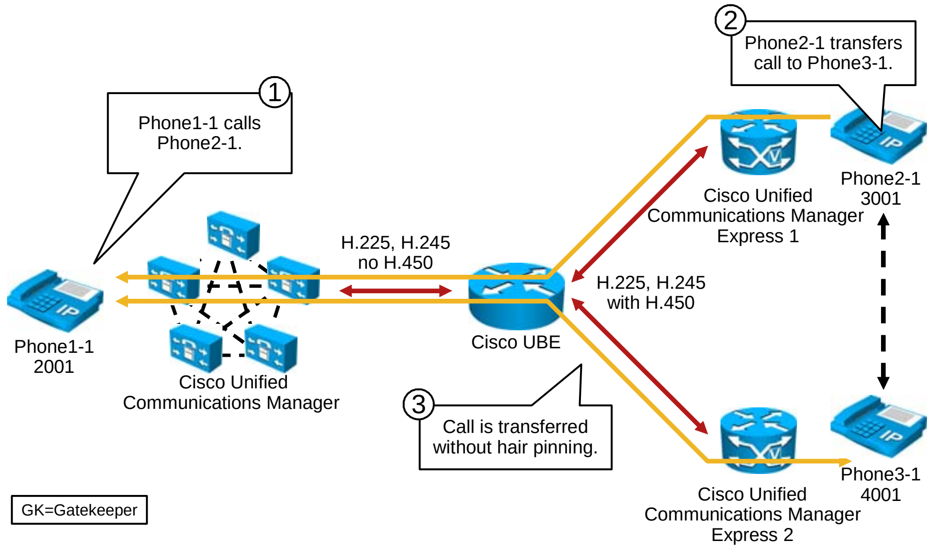
- Cisco Unified Communications Manager – Cisco UBE – Cisco Unified Communications Manager Express
- Cisco Unified Communications Manager – Cisco UBE with RSVP – Cisco Unified Communications Manager
- Cisco Unified Communications Manager – Cisco UBE – SIP Carrier
- Cisco Unified Communications Manager – Gatekeeper – Cisco UBE – SIP Carrier
- Cisco Unified Communications Manager – Via-Zone Gatekeeper – Cisco UBE – Cisco Unified Communications Manager

Cisco UBE call flow depends on the network topology and features implemented. The call flows that are listed in this figure will be used to illustrate the concepts about Cisco UBE that have been discussed thus far.

These scenarios will be used:

- Cisco Unified Communications Manager – Cisco UBE – Cisco Unified Communications Manager Express
- Cisco Unified Communications Manager – Cisco UBE with RSVP – Cisco Unified Communications Manager
- Cisco Unified Communications Manager – Cisco UBE – SIP carrier
- Cisco Unified Communications Manager – gatekeeper – Cisco UBE – SIP carrier
- Cisco Unified Communications Manager – via-zone gatekeeper – Cisco UBE – Cisco Unified Communications Manager

Cisco UBE Call Flows: Cisco Unified Communications Manager to Cisco Unified Communications Manager Express



1 Phone1-1 calls Phone2-1.

2 Phone2-1 transfers call to Phone3-1.

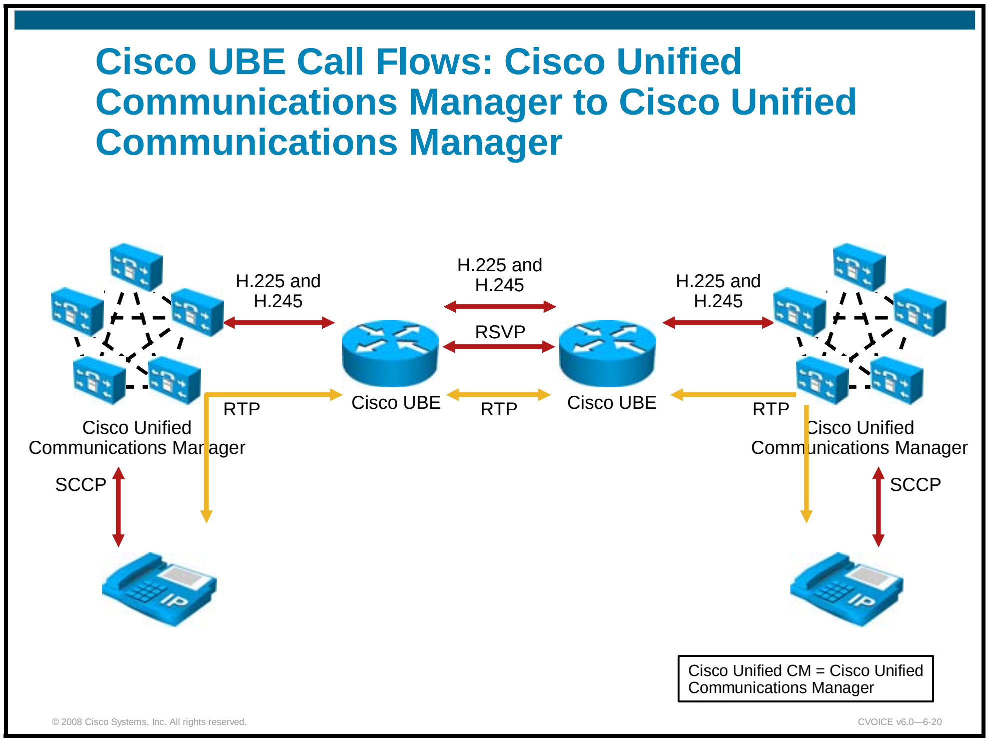
3 Call is transferred without hair pinning.

CVOICE v6.0—6-19

This figure shows a call flow between a Cisco Unified Communications Manager and a Cisco Unified Communications Manager Express using a Cisco UBE.

Cisco Unified Communications Manager Express uses H.450 for optimized call transfers and call forwards without requiring hairpinning. Because Cisco Unified Communications Manager does not support H.450, a transfer involving H.323 VoIP connections might lead to suboptimal traffic flows.

A Cisco UBE can be used to solve H.450 Cisco Unified Communications Manager and Cisco Unified Communications Manager Express interoperability issues. In this example, a call between Phone 1-1 and Phone 2-1 is transferred to Phone 3-1. Because the Cisco UBE supports H.450, the resulting traffic flow will be directly between the Cisco UBE and Cisco Unified Call Manager 2. Without a Cisco UBE, the call transfer would be done using hairpinning on Cisco Unified Call Manager 1.

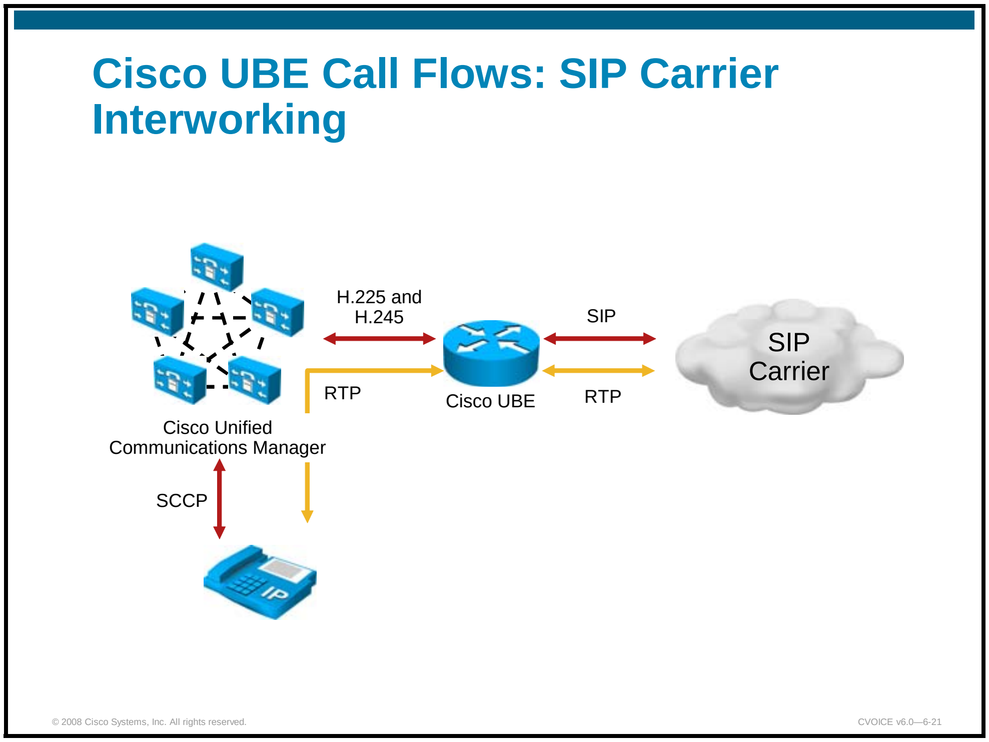


Cisco UBE Call Flows: Cisco Unified Communications Manager to Cisco Unified Communications Manager

Cisco Unified CM = Cisco Unified Communications Manager

RSVP-based intercluster CAC can be implemented using Cisco UBE. The figure shows two Cisco Unified Communications Manager clusters interconnected by two Cisco UBEs. Each Cisco Unified Communications Manager cluster has an H.323 call leg to the local Cisco UBE. The two Cisco UBEs perform RSVP-based CAC, and because RSVP-based CAC requires media flow-through, a call between the two clusters will flow through the two Cisco UBEs.

Note that phones still use Skinny Client Control Protocol (SCCP) for signaling towards Cisco Unified Communications Manager.

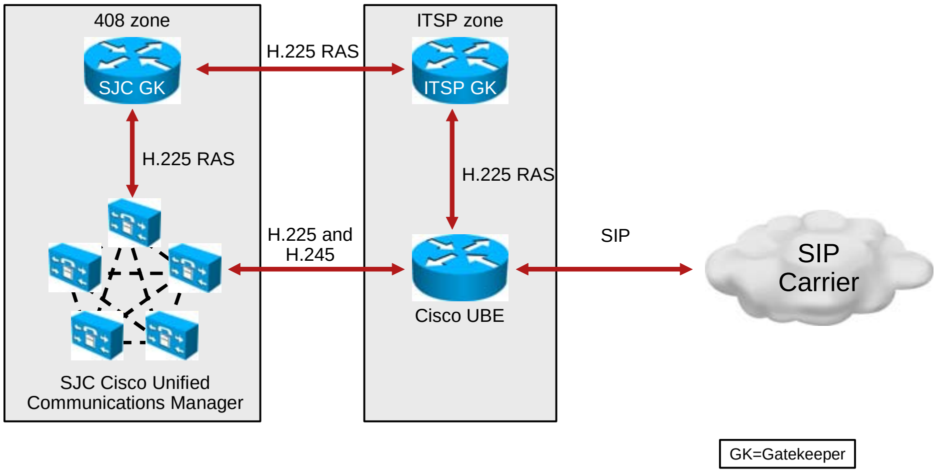


Cisco UBE Call Flows: SIP Carrier Interworking

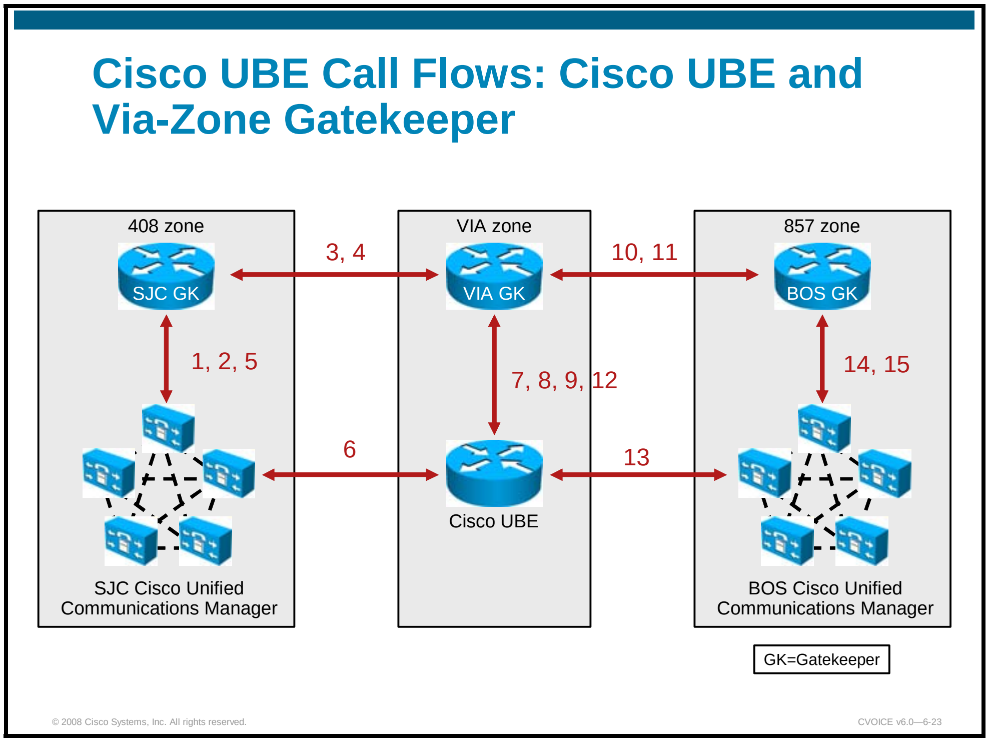
CVOICE v6.0—6-21

The figure shows a simple Cisco UBE deployment where the Cisco UBE is used to translate the H.323 call leg with the Cisco Unified Communications Manager Cluster to a SIP call leg point to a SIP carrier. Because this is a connection to an external VoIP network, media flow-through is required to hide internal IP addresses and overcome IP interworking issues, such as duplicate private IP addresses.

Cisco UBE Call Flows: Gatekeeper and SIP Carrier Interworking



This figure shows an H.323 gatekeeper deployment that includes a Cisco UBE integrated with a gatekeeper and a SIP carrier. Calls from the Cisco Unified Communications Manager cluster are routed via H.225 RAS from the San Jose gatekeeper to the Internet Telephony Service Provider (ITSP) gatekeeper, which then routes the call to the Cisco UBE. The Cisco UBE then performs standard protocol interworking, allowing connections from the Cisco Unified Communications Manager H.323 network to the SIP carrier network.



Cisco UBE Call Flows: Cisco UBE and Via-Zone Gatekeeper

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—6-23

This figure shows the concept of via-zone enabled gatekeepers using a Cisco UBE.

Three gatekeepers are deployed:

- **San Jose gatekeeper:** This gatekeeper has a single zone called 408.
- **Boston gatekeeper:** This gatekeeper has a single zone called 857.
- **Via-zone gatekeeper:** This gatekeeper has a single zone called VIA.

The San Jose Cisco Unified Communications Manager is registered at the San Jose gatekeeper, the Boston Cisco Unified Communications Manager is registered at the Boston gatekeeper, and the Cisco UBE is registered at the via-zone gatekeeper.

The San Jose gatekeeper will route all calls made to the remote 857 zone to the via-zone gatekeeper, and the Boston gatekeeper will route all calls made to the remote 408 zone to the via-zone gatekeeper.

The via-zone gatekeepers will route the calls to the remote 408 and 857 zones, but not directly to the gatekeepers in San Jose and Boston. Instead, the routing will be done using the local VIA zone.

These steps describe an example call flow from the San Jose Cisco Unified Communications Manager cluster in zone 408 on the San Jose gatekeeper to the Boston Cisco Unified Communications Manager cluster located in zone 857 on the Boston gatekeeper:

Step 1 A call is placed from the San Jose Cisco Unified Communications Manager to someone in area code 857.

Step 2 The San Jose Cisco Unified Communications Manager sends an Admission Request (ARQ) to the San Jose gatekeeper.

Step 3 The San Jose gatekeeper resolves the 857 prefix that belongs to the via-zone gatekeeper and sends a Location Request (LRQ).

Step 4 The VIA gatekeeper receives an LRQ for 857 and resolves the 857 prefix to the Cisco UBE. The VIA gatekeeper sends a Location Confirmation (LCF) to the San Jose gatekeeper.

Step 5 The San Jose gatekeeper returns an Admission Confirmation (ACF) that specifies the Cisco UBE to the San Jose Cisco Unified Communications Manager.

Step 6 The San Jose Cisco Unified Communications Manager sends a SETUP message to the Cisco UBE for the 857 number.

Step 7 The Cisco UBE sends an ARQ to the VIA gatekeeper with the **answerCall=true** parameter set to admit the incoming call.

Step 8 The VIA gatekeeper responds with an ACF to admit the call. From the perspective of the VIA gatekeeper, the first call leg is established.

Step 9 The Cisco UBEG gateway has a dial peer that specifies that RAS messages should be sent to the VIA gatekeeper for all prefixes. The Cisco UBE initiates the process of resending the call by sending the ARQ message with **answerCall=false** to the VIA gatekeeper for 857.

Step 10 The VIA gatekeeper knows that prefix 857 belongs to the Boston gatekeeper, and because the source zone is the via-zone, the VIA gatekeeper sends an LRQ to the Boston gatekeeper.

Step 11 The Boston gatekeeper sees prefix 857 as a local zone and sends an LCF pointing to the Boston Cisco Unified Communications Manager.

Step 12 The VIA gatekeeper returns an ACF to the Cisco UBE that specifies the Boston Cisco Unified Communications Manager.

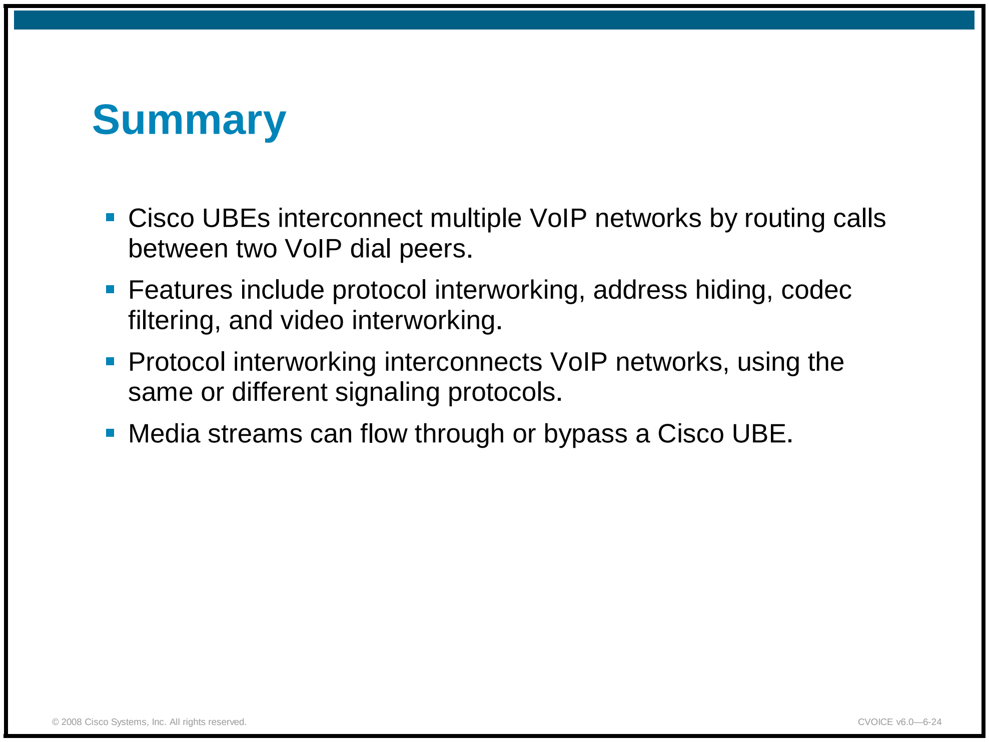
Step 13 The Cisco UBE sends a SETUP message to the Boston Cisco Unified Communications Manager for the 857 call.

Step 14 The Boston Cisco Unified Communications Manager sends an ARQ to the Boston gatekeeper to request admission for the call.

Step 15 The Boston gatekeeper sends an ACF with the **answerCall=true** parameter.

Summary

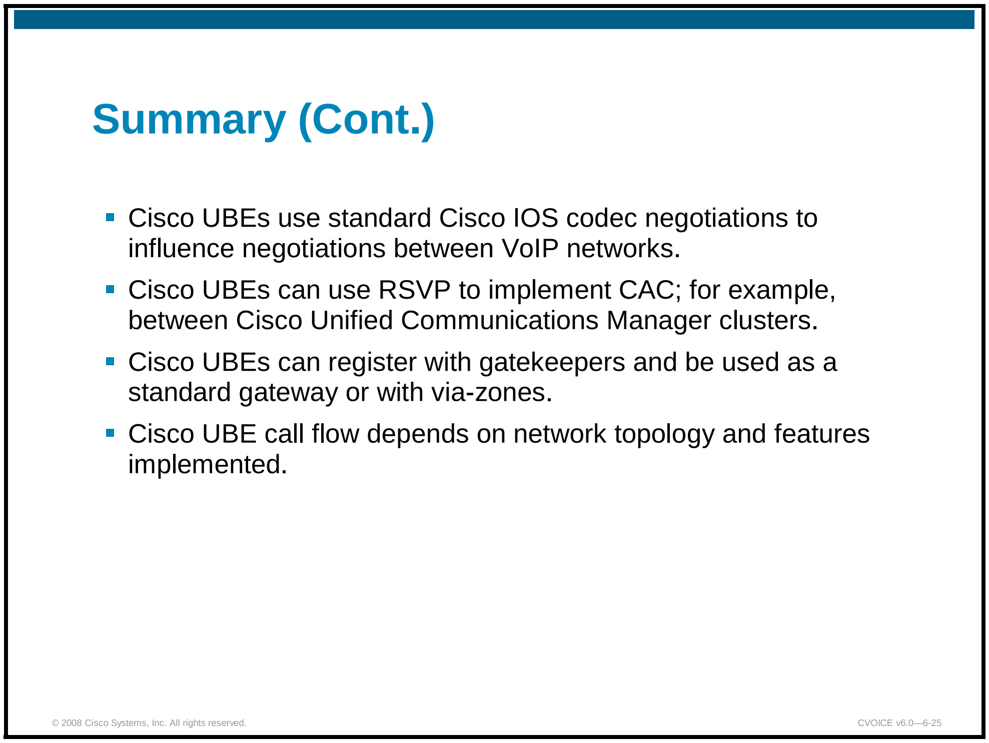
This topic summarizes the key points that were discussed in this lesson.



Summary

- Cisco UBEs interconnect multiple VoIP networks by routing calls between two VoIP dial peers.
- Features include protocol interworking, address hiding, codec filtering, and video interworking.
- Protocol interworking interconnects VoIP networks, using the same or different signaling protocols.
- Media streams can flow through or bypass a Cisco UBE.

CVOICE v6.0—6-24



Summary (Cont.)

- Cisco UBEs use standard Cisco IOS codec negotiations to influence negotiations between VoIP networks.
- Cisco UBEs can use RSVP to implement CAC; for example, between Cisco Unified Communications Manager clusters.
- Cisco UBEs can register with gatekeepers and be used as a standard gateway or with via-zones.
- Cisco UBE call flow depends on network topology and features implemented.

CVOICE v6.0—6-25

Lesson Self-Check

Use the questions here to review what you learned in this lesson. The correct answers and solutions are found in the Lesson Self-Check Answer Key.

Q1) Cisco UBEs interconnect multiple VoIP networks by routing calls between two ________ dial peers.

Relates to: Cisco Unified Border Element Overview

A) POTS
B) VoATM
C) VoFR
D) VoIP

Q2) Which three features of an IP-to-IP gateway would be required for a customer who wants to interconnect a Cisco Unified Communications Manager cluster with a SIP carrier?

Relates to: Cisco Unified Border Element Overview

Q3) Cisco UBE features include ___________________, _________________, codec filtering, and video interworking.

Relates to: Cisco UBE Gateways in Enterprise Environments

Q4) Protocol interworking interconnects VoIP networks, using the same or different __________ protocols.

Relates to: Protocol Interworking on Cisco UBE Gateways

A) signaling
B) compression
C) codec
D) transport

Q5) Media streams can ________________ or _____________ a Cisco UBE.

Relates to: Media Flows on Cisco UBE Gateways

A) bypass, flow-around
B) flow-through, bypass
C) flow-through, traverse
D) flow-through, flow-around

Q6) If codec filtering is not required, a Cisco UBE also supports ____________ codec negotiations.

Relates to: Codec Filtering on Cisco UBE Gateways

A) multiple
B) null
C) dynamic
D) transparent

Q7) When deploying Cisco UBE and RSVP-based CAC, ensure that the flows that should utilize RSVP are configured for media _______________.

Relates to: RSVP-Based CAC on Cisco UBE Gateways

A) flow-around
B) bypass
C) flow-through
D) pass-through

Q8) Two Cisco Unified Communications Manager clusters need to be interconnected using RSVP-based CAC. What are the requirements for this?

Relates to: RSVP-Based CAC on Cisco UBE Gateways

A) two IP-to-IP gateways, media flow-through
B) one IP-to-IP gateway, media flow-through
C) two IP-to-IP Gateways, media flow around
D) one IP-to-IP Gateway, media flow-around

Q9) Cisco UBEs can register with gatekeepers and be used as a standard gateway or with _______________.

Relates to: Cisco UBE Gateways and Gatekeeper Interworking

A) via-zones
B) remote-zones
C) local-zones
D) gatekeeper zones

Q10) When Cisco UBE is used to translate an H.323 call leg with the Cisco Unified Communications Manager cluster to a SIP call leg point to a SIP carrier, the call flow must ______________ the Cisco UBE.

Relates to: Cisco UBE Gateway Call Flows

A) bypass
B) flow around
C) stop at
D) flow through

Lesson Self-Check Answer Key

Q1)	D
Q2)	protocol interworking, media flow-through , codec filtering
Q3)	address hiding, protocol interworking
Q4)	A
Q5)	B
Q6)	D
Q7)	C
Q8)	A
Q9)	A
Q10)	D

Lesson 2

Implementing a Cisco UBE

Overview

A Cisco Unified Border Element (Cisco UBE) can be implemented in VoIP networks to enhance VoIP network interoperability. This lesson describes how to implement Cisco UBEs to support protocol interworking between H.323 and session initiation protocol (SIP) networks.

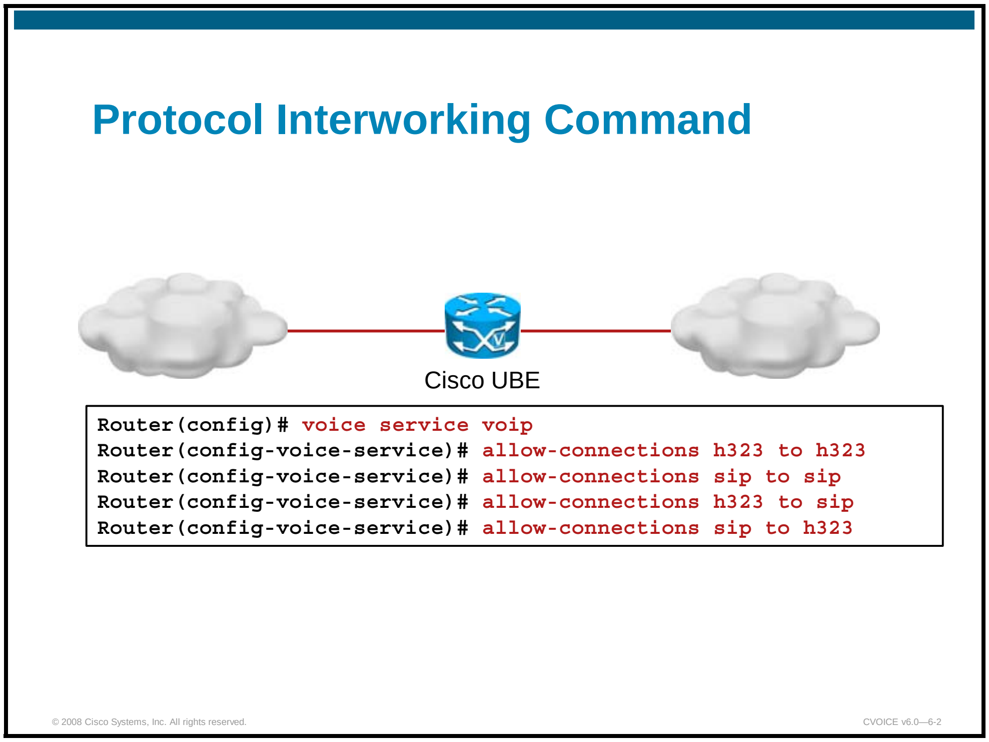
Objectives

Upon completing this lesson, you will be able to implement Cisco UBEs to provide protocol interworking. This ability includes being able to meet these objectives:

- Describe the commands that are used to configure protocol interworking
- Configure H.323-to-H.323 interworking on a Cisco UBE
- Configure H.323-to-SIP interworking on a Cisco UBE
- Describe the commands that are used to configure media flow-around, media flow-through, and transparent codec pass-through
- Configure transparent codec pass-through and media flow-around on a Cisco UBE
- Configure a Cisco UBE to register with a via-zone gatekeeper
- Verify Cisco UBE and via-zone gatekeeper operation

Protocol Interworking Command

This topic describes the command used to enable protocol interworking on a Cisco UBE.



Protocol Interworking Command

```
Router(config)# voice service voip
Router(config-voice-service)# allow-connections h323 to h323
Router(config-voice-service)# allow-connections sip to sip
Router(config-voice-service)# allow-connections h323 to sip
Router(config-voice-service)# allow-connections sip to h323
```

CVOICE v6.0—6-2

To enable protocol interworking, use the **allow-connections** *from-type* **to** *to-type* command in global voice service configuration mode. The *from-type* and *to-type* options specify the signaling protocols.

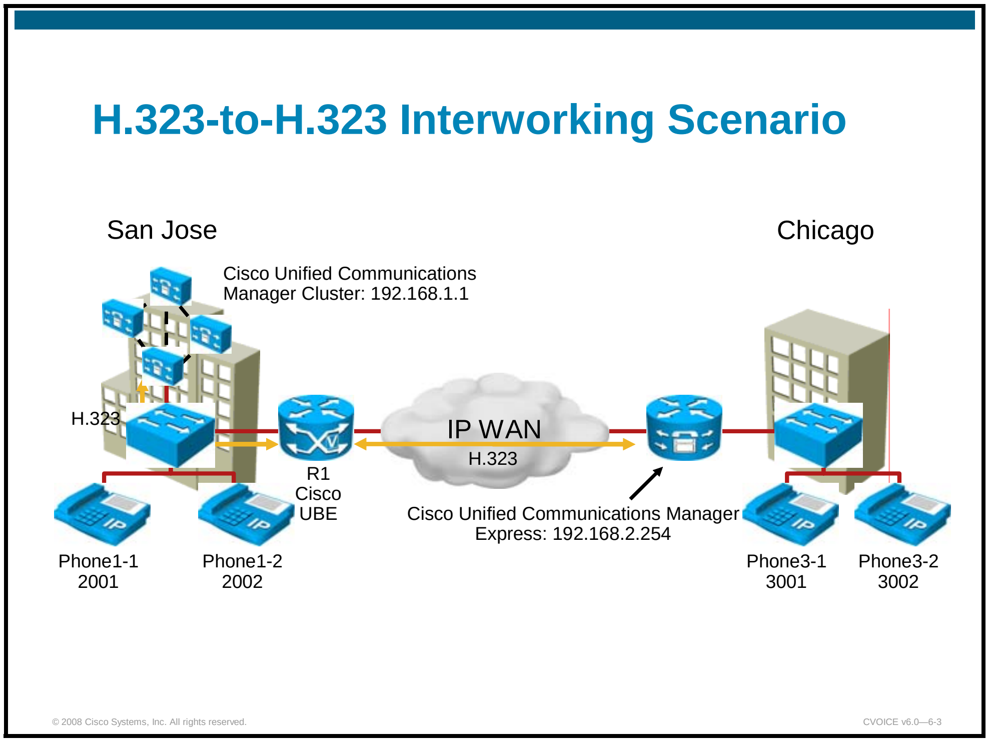
Syntax Description

from-type	Originating endpoint type. The following choices are valid: ■ **h323**—H.323 ■ **sip**—SIP
to	Indicates that the argument that follows is the connection target.
to-type	Terminating endpoint type. The following choices are valid: ■ **h323**—H.323 ■ **sip**—SIP

The configuration for H.323 and SIP interworking is unidirectional, thus if bidirectional interworking is required, you need to configure the mirror-matching statement as well. For example, if bidirectional H.323-to-SIP interworking is required, you need to configure **allow connections h323 to sip** as well as **allow connections sip to h323**.

Configuring H.323-to-H.323 Interworking

This topic describes how to configure H.323-to-H.323 interworking using a Cisco UBE.



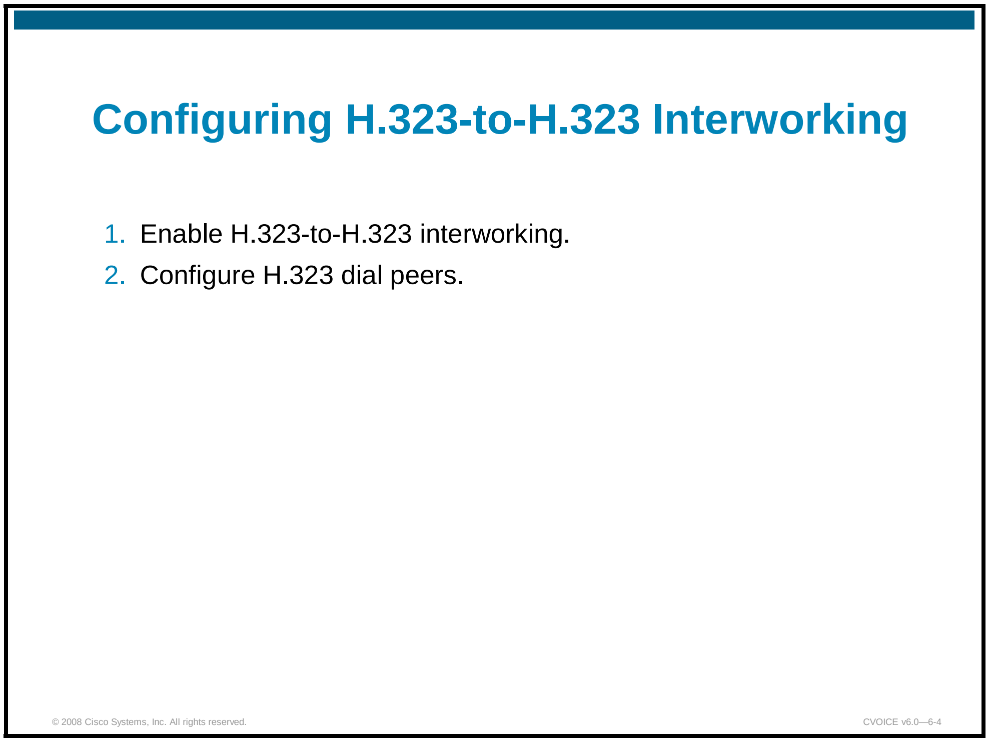
H.323-to-H.323 Interworking Scenario

San Jose
Chicago
Cisco Unified Communications Manager Cluster: 192.168.1.1
H.323
R1 Cisco UBE
IP WAN
H.323
Cisco Unified Communications Manager Express: 192.168.2.254
Phone1-1 2001
Phone1-2 2002
Phone3-1 3001
Phone3-2 3002

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—6-3

H.323-to-H.323 gateway configuration provides a network-to-network demarcation point between independent VoIP and video networks for billing, security, call-admission control, QoS, and signaling interworking. The Cisco UBE performs most of the functions of a PSTN-to-IP gateway but joins two H.323 VoIP call legs.

The figure shows an example scenario used to configure H.323-to-H.323 interworking for a Cisco UBE. The Cisco Unified Communications Manager cluster in San Jose is connected with the Cisco Unified Communications Manager Express in Chicago using a Cisco UBE.



Configuring H.323-to-H.323 Interworking

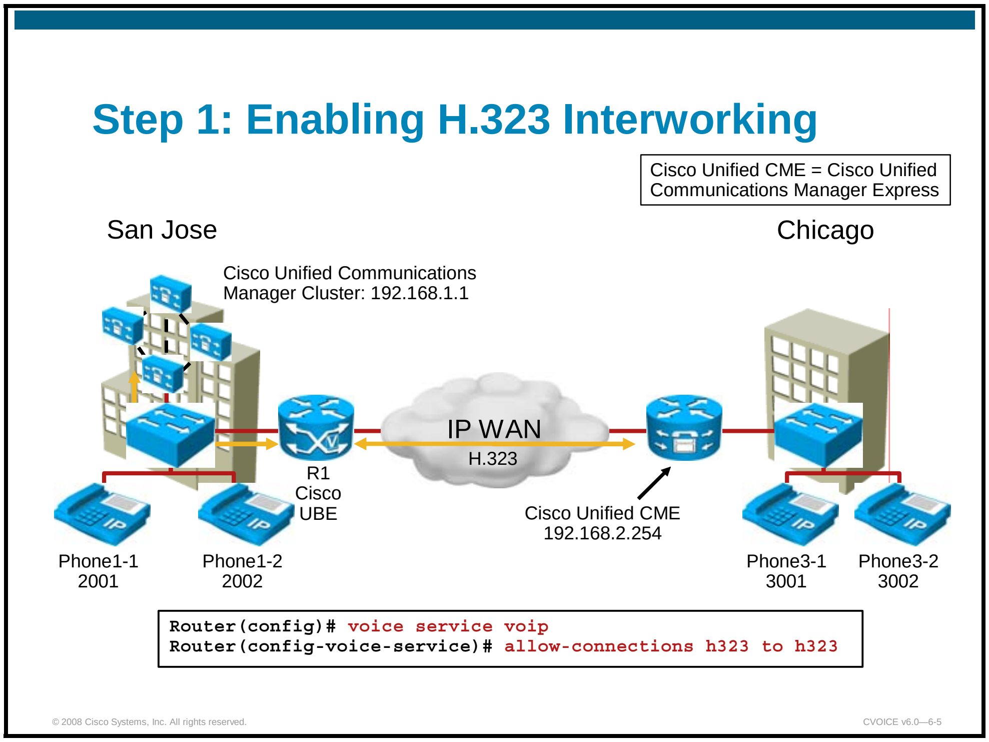
1. Enable H.323-to-H.323 interworking.
2. Configure H.323 dial peers.

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—6-4

To configure H.323-to-H.323 interworking between a Cisco Unified Communications Manager cluster and a Cisco Unified Communications Manager Express gateway, follow these steps:

Step 1 Enable H.323-to-H.323 interworking.

Step 2 Configure the H.323 dial peers on the Cisco UBE to allow call routing between the Cisco Unified Communications Manager cluster and Cisco Unified Communications Manager Express.



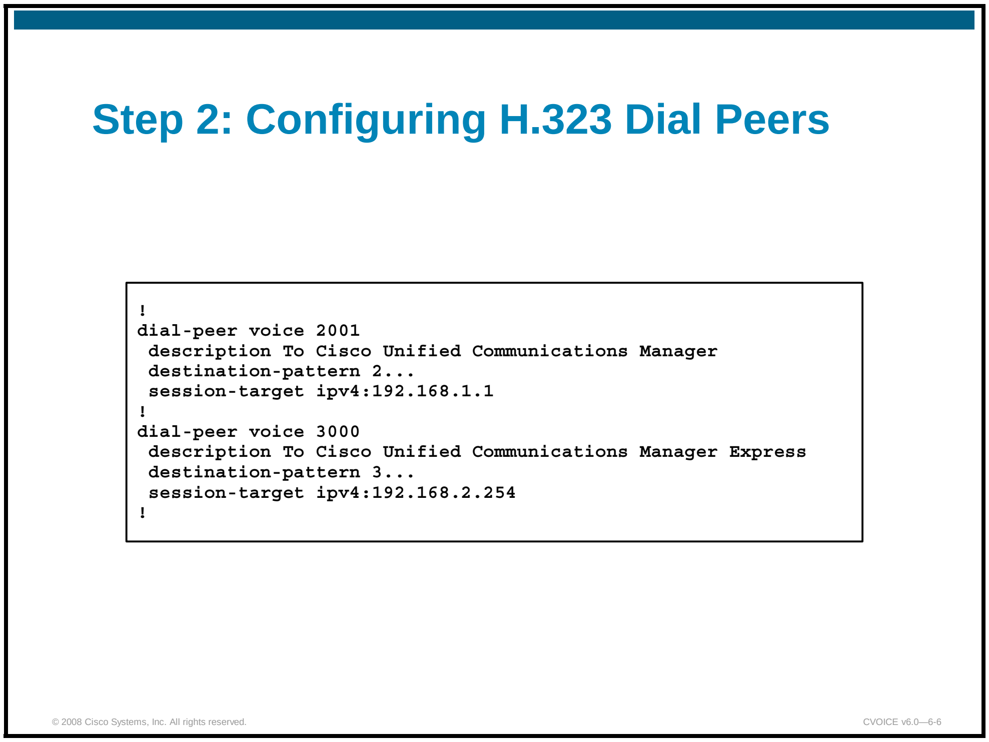
Step 1: Enabling H.323 Interworking

Cisco Unified CME = Cisco Unified Communications Manager Express

```
Router(config)# voice service voip
Router(config-voice-service)# allow-connections h323 to h323
```

CVOICE v6.0—6-5

By default, a Cisco IOS gateway will not allow connections between two VoIP dial peers. To change this behavior and allow H.323-to-H.323 connections, use the **allow-connections h323 to h323** command in voice service configuration mode.



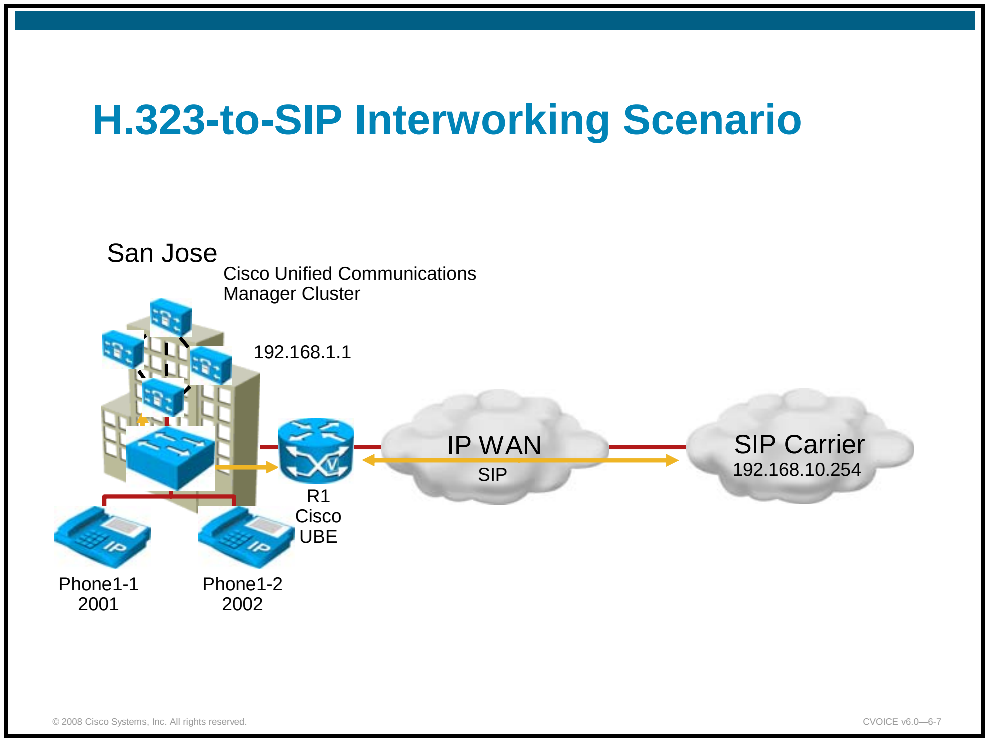
Step 2: Configuring H.323 Dial Peers

```
!
dial-peer voice 2001
 description To Cisco Unified Communications Manager
 destination-pattern 2...
 session-target ipv4:192.168.1.1
!
dial-peer voice 3000
 description To Cisco Unified Communications Manager Express
 destination-pattern 3...
 session-target ipv4:192.168.2.254
!
```

After H323-to-H323 calls have been allowed, configure the appropriate dial peers to route between the Cisco Unified Communications Manager cluster and the Cisco Unified Communications Manager Express cluster by setting the session target address. No special configuration on the dial peers is required.

Configuring H.323-to-SIP Interworking

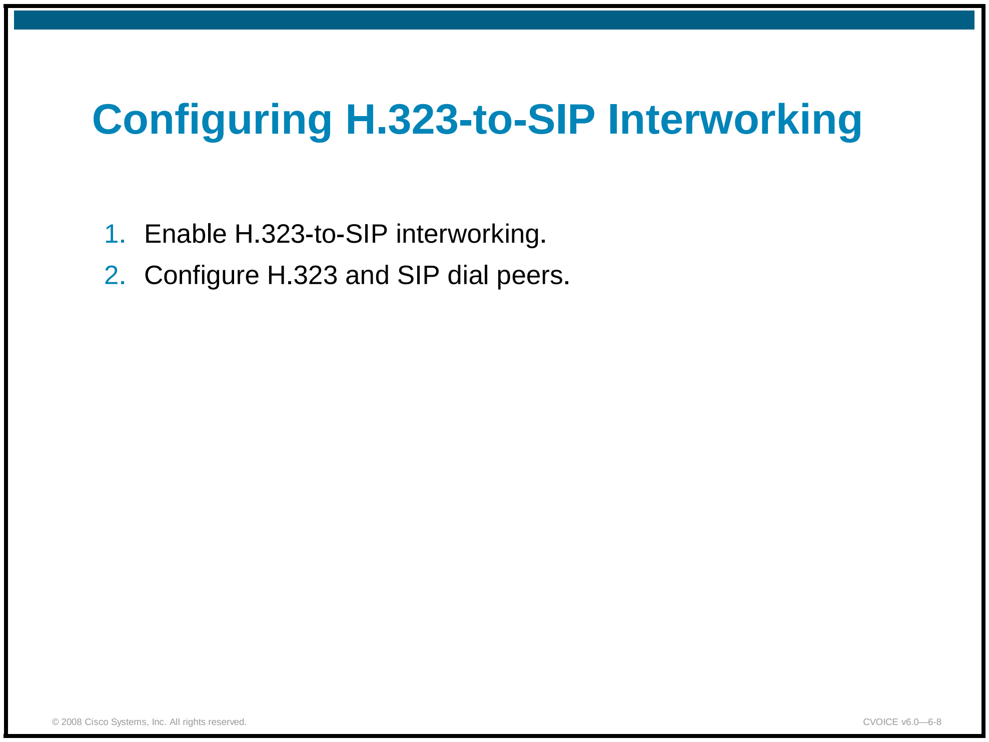
This topic describes how to configure H.323-to-SIP interworking.



H.323-to-SIP Interworking Scenario

CVOICE v6.0—6-7

The figure shows an example scenario used to configure H.323-to-SIP interworking with a Cisco UBE. The Cisco Unified Communications Manager cluster in San Jose routes calls to the SIP carrier via a Cisco UBE. The connection between the Cisco Unified Communications Manager and the Cisco UBE is H.323, and the connection between the Cisco UBE and the SIP carrier is SIP.



Configuring H.323-to-SIP Interworking

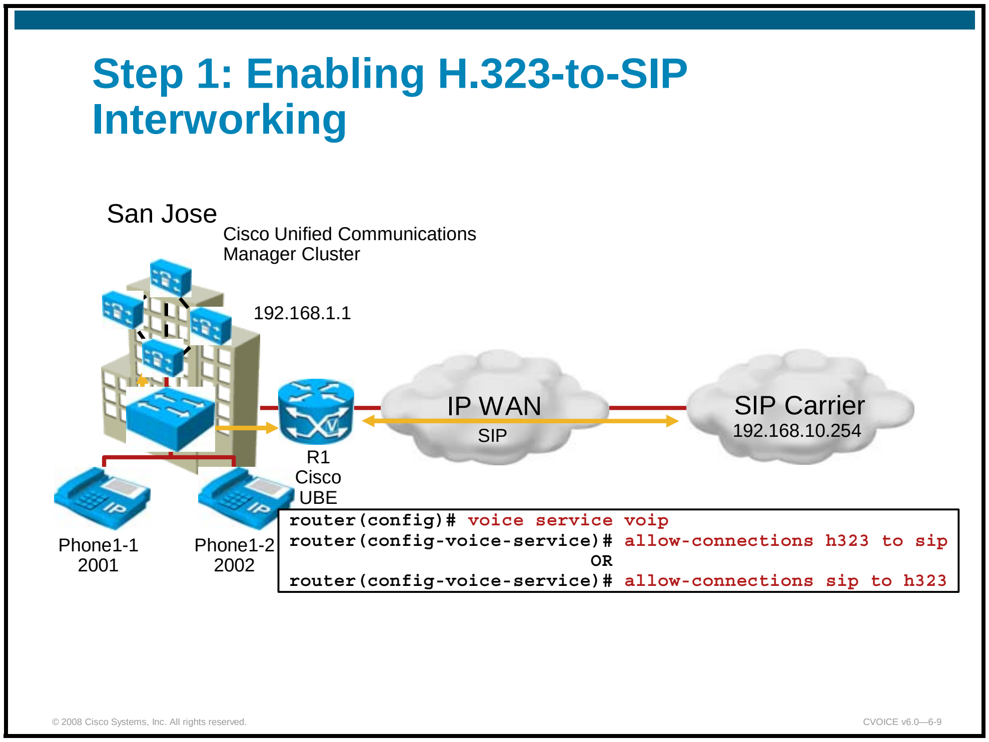
1. Enable H.323-to-SIP interworking.
2. Configure H.323 and SIP dial peers.

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—6-8

Follow these steps to configure H.323-to-SIP interworking:

Step 1 Enable H.323-to-SIP interworking.

Step 2 Configure H.323 and SIP dial peers to route international calls between the Cisco Unified Communications Manager cluster and the SIP carrier.

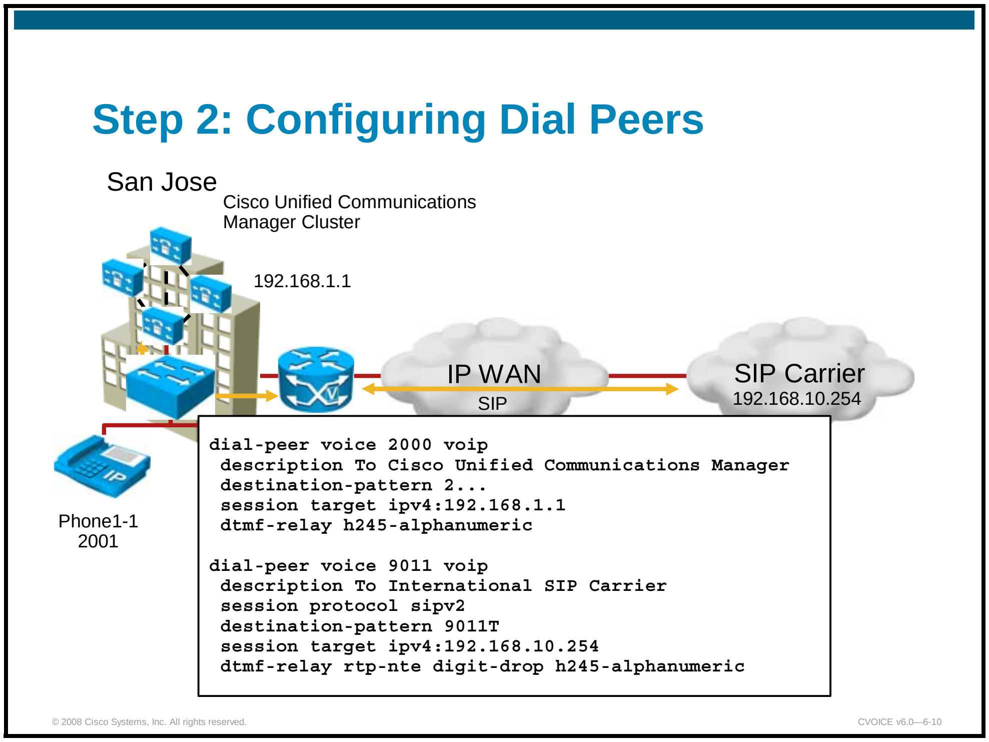


Step 1: Enabling H.323-to-SIP Interworking

```
router(config)# voice service voip
router(config-voice-service)# allow-connections h323 to sip
                                OR
router(config-voice-service)# allow-connections sip to h323
```

CVOICE v6.0—6-9

As with an H.323-to-H.323 connection, by default a Cisco IOS gateway will not allow connections between an H.323 and a SIP VoIP dial peer. To change this behavior and allow H.323-to-SIP connections, use the **allow-connections h323 to sip** command in voice service configuration mode. The last command enables SIP to H.323 calls.



Step 2: Configuring Dial Peers

```
dial-peer voice 2000 voip
 description To Cisco Unified Communications Manager
 destination-pattern 2...
 session target ipv4:192.168.1.1
 dtmf-relay h245-alphanumeric

dial-peer voice 9011 voip
 description To International SIP Carrier
 session protocol sipv2
 destination-pattern 9011T
 session target ipv4:192.168.10.254
 dtmf-relay rtp-nte digit-drop h245-alphanumeric
```

CVOICE v6.0—6-10

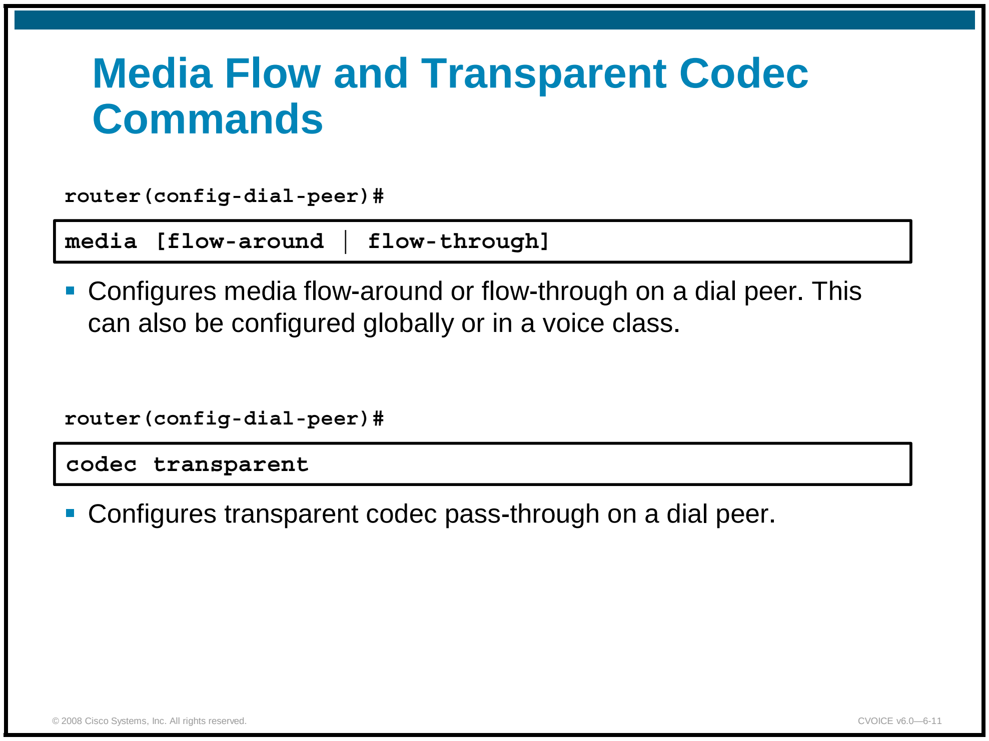
For a SIP-to-H.323 call (that is, **repented** to **h245-alphanumeric**) via a Cisco UBE, if any Real-Time Transport Protocol (RTP) named telephony event (NTE) packets are sent before the H.323 endpoint answers the call, the dual-tone multifrequency (DTMF) signal is not heard on a terminating gateway.

Note The debug output will show that the H245 out-of-band messages are sent to the terminating gateway. However, the digits are not heard on the phone.

To avoid sending both in-band and out-of-band tones to the outgoing leg when sending Cisco UBE calls in-band (**rtp-nte**) to out-of-band (**h245-alphanumeric**), configure the **dtmf-relay rtp-nte digit-drop** command on the incoming SIP dial peer. On the H.323 side, configure either **dtmf-relay h245-alphanumeric** or **dtmf-relay h245-signal**. This may also be used for H.323-to-SIP calls.

Media Flow and Transparent Codec Commands

This topic describes the commands required to configure media flow-around, and media flow-through, and transparent coder-decoder (codec) pass-through.



Media Flow and Transparent Codec Commands

```
router(config-dial-peer)#
```

```
media [flow-around | flow-through]
```

- Configures media flow-around or flow-through on a dial peer. This can also be configured globally or in a voice class.

```
router(config-dial-peer)#
```

```
codec transparent
```

- Configures transparent codec pass-through on a dial peer.

CVOICE v6.0—6-11

media

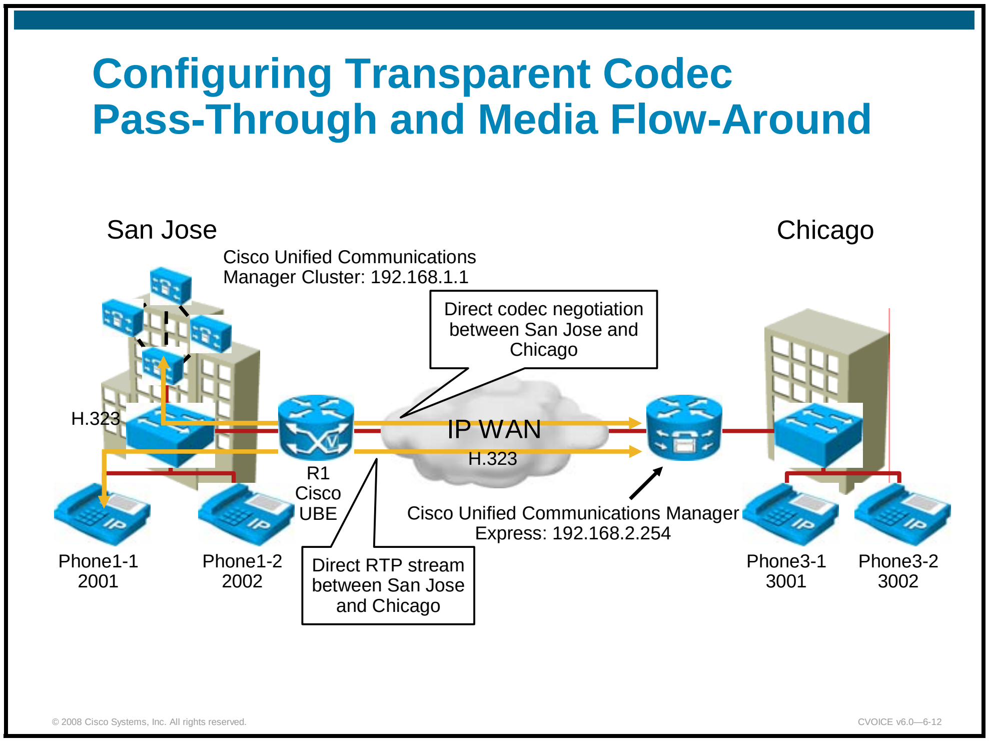
To configure media flow-through or media flow-around, use the **media** command. This can be done in dial-peer configuration mode or globally under the voice service configuration mode. The default is **media flow-through**.

codec transparent

To configure transparent codec pass-through, use the **codec transparent** command. This can be done in dial-peer configuration mode or via a codec class.

Configuring Transparent Codec Pass-Through and Media Flow-Around

This topic describes how to configure transparent codec pass-through and media flow-around.



Configuring Transparent Codec Pass-Through and Media Flow-Around

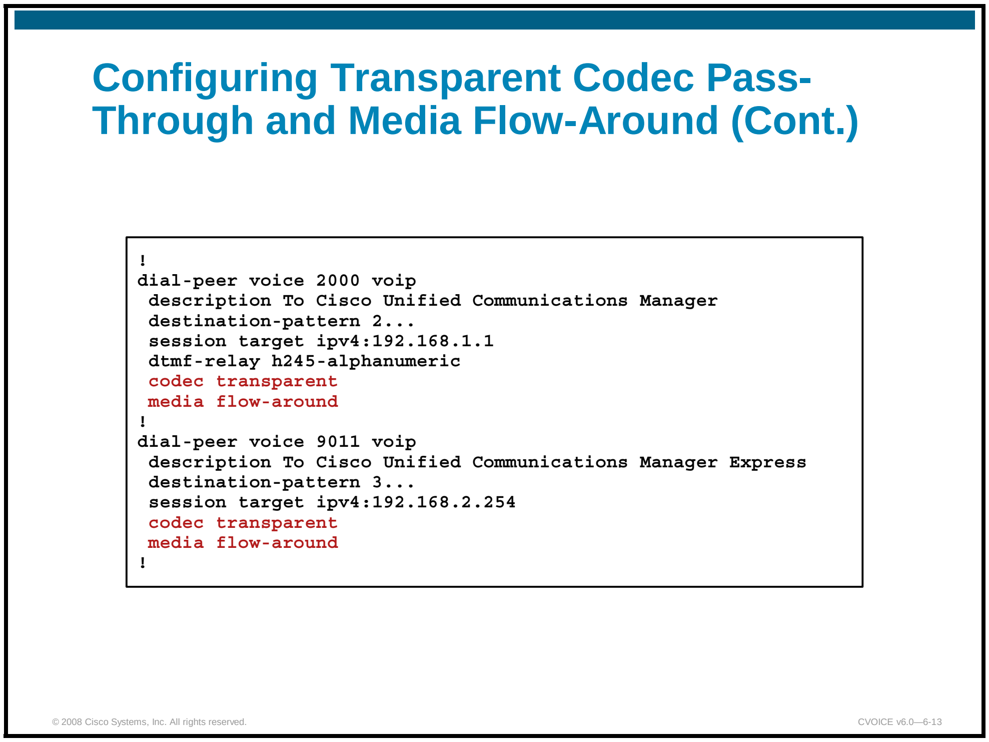
Direct codec negotiation between San Jose and Chicago

Direct RTP stream between San Jose and Chicago

San Jose
Chicago
Cisco Unified Communications Manager Cluster: 192.168.1.1
H.323
IP WAN
H.323
R1 Cisco UBE
Cisco Unified Communications Manager Express: 192.168.2.254
Phone1-1 2001
Phone1-2 2002
Phone3-1 3001
Phone3-2 3002

CVOICE v6.0—6-12

The figure shows an example scenario used to configure H.323-to-H.323 interworking, including transparent codec pass-through and media flow-around, using a Cisco UBE. The Cisco Unified Communications Manager cluster in San Jose is connected with the Cisco Unified Communications Manager Express in Chicago using a Cisco UBE. Codec negotiation is performed directly between the Cisco Unified Communications Manager and the Cisco Unified Communications Manager Express, and RTP streams flow directly between the endpoints.



Configuring Transparent Codec Pass-Through and Media Flow-Around (Cont.)

```
!
dial-peer voice 2000 voip
 description To Cisco Unified Communications Manager
 destination-pattern 2...
 session target ipv4:192.168.1.1
 dtmf-relay h245-alphanumeric
 codec transparent
 media flow-around
!
dial-peer voice 9011 voip
 description To Cisco Unified Communications Manager Express
 destination-pattern 3...
 session target ipv4:192.168.2.254
 codec transparent
 media flow-around
!
```

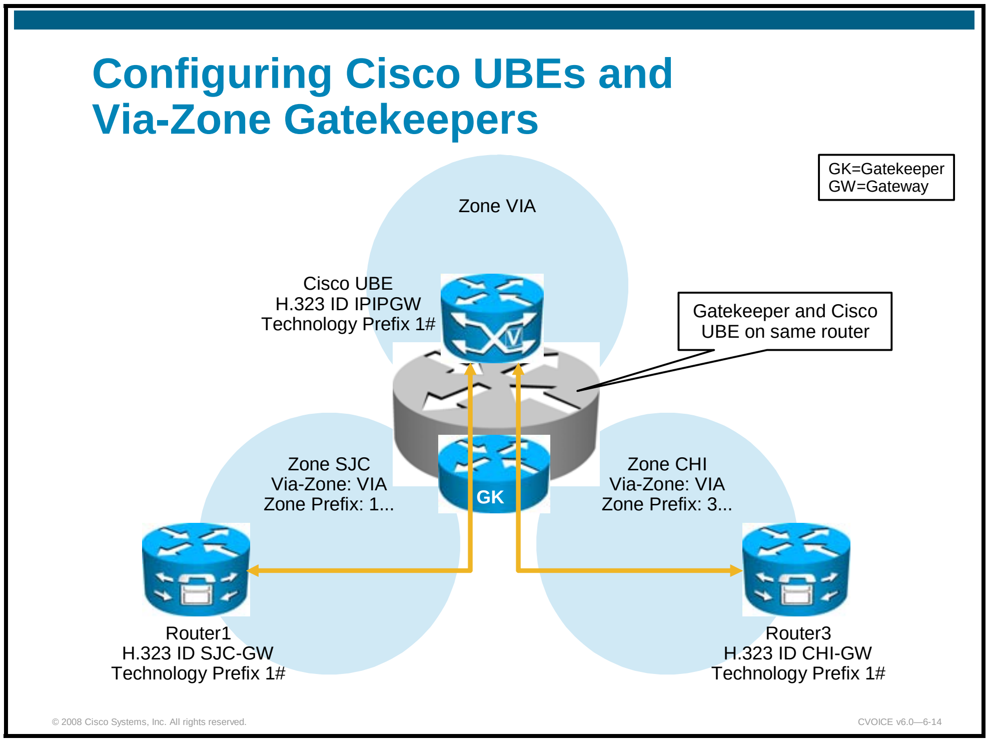
CVOICE v6.0—6-13

Codec transparency enables the Cisco UBE to pass codec capabilities between endpoints. If you configure transparency, the Cisco UBE uses the codec that was specified by the endpoints for setting up a call. To enable endpoint-to-endpoint codec negotiation without the Cisco UBE, use the **codec transparent** command.

With the default configuration, the Cisco UBE receives media packets from the inbound call leg, terminates them, and then reoriginates the media stream on an outbound call leg. Media flow-around enables media packets to be passed directly between the endpoints, without the intervention of the Cisco UBE. The Cisco UBE continues to handle routing and billing functions. Media flow-around for SIP-to-SIP calls is not supported. Use the **media flow-around** command to enable media flow-around.

Configuring Cisco UBEs and Via-Zone Gatekeepers

This topic describes how to configure a Cisco UBE to register with a via-zone gatekeeper.



Configuring Cisco UBEs and Via-Zone Gatekeepers

GK=Gatekeeper
GW=Gateway

Zone VIA

Cisco UBE
H.323 ID IPIPGW
Technology Prefix 1#

Gatekeeper and Cisco UBE on same router

Zone SJC
Via-Zone: VIA
Zone Prefix: 1...

GK

Zone CHI
Via-Zone: VIA
Zone Prefix: 3...

Router1
H.323 ID SJC-GW
Technology Prefix 1#

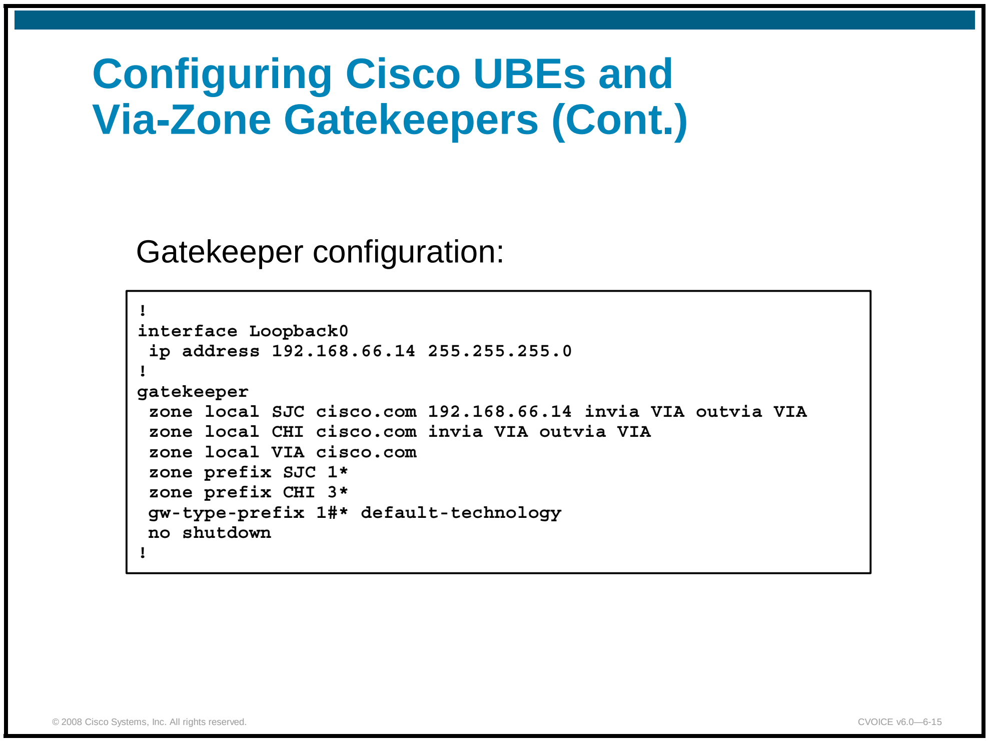
Router3
H.323 ID CHI-GW
Technology Prefix 1#

The figure shows an example scenario used to configure a Cisco UBE and a via-zone gatekeeper. A gatekeeper is configured with two standard local zones: San Jose (SJC) and Chicago (CHI). The Cisco Unified Communications Manager Express Router1 is registered in the SJC zone, and the Cisco Unified Communications Manager Express Router3 is registered in the CHI zone. Calls between Chicago and San Jose should be routed by the gatekeeper. Instead of routing calls directly between the two zones, the gatekeeper should route the calls through the via-zone (VIA), which includes a Cisco UBE.

Note	The Cisco UBE and the gatekeeper reside on the same router.

Configure the Gatekeeper

This subtopic covers configuration of the gatekeeper.



Configuring Cisco UBEs and Via-Zone Gatekeepers (Cont.)

Gatekeeper configuration:

```
!
interface Loopback0
 ip address 192.168.66.14 255.255.255.0
!
gatekeeper
 zone local SJC cisco.com 192.168.66.14 invia VIA outvia VIA
 zone local CHI cisco.com invia VIA outvia VIA
 zone local VIA cisco.com
 zone prefix SJC 1*
 zone prefix CHI 3*
 gw-type-prefix 1#* default-technology
 no shutdown
!
```

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—6-15

Complete these steps to configure the Cisco UBE.

Step 1 Create a loopback interface to use for the gatekeeper.

Step 2 Create local, remote, and VIA zones.

Two local zones, CHI and SJC, are configured, but instead of configuring a standard local zone, the **invia** and **outvia** options are used to route calls to and from the zones with the VIA zone:

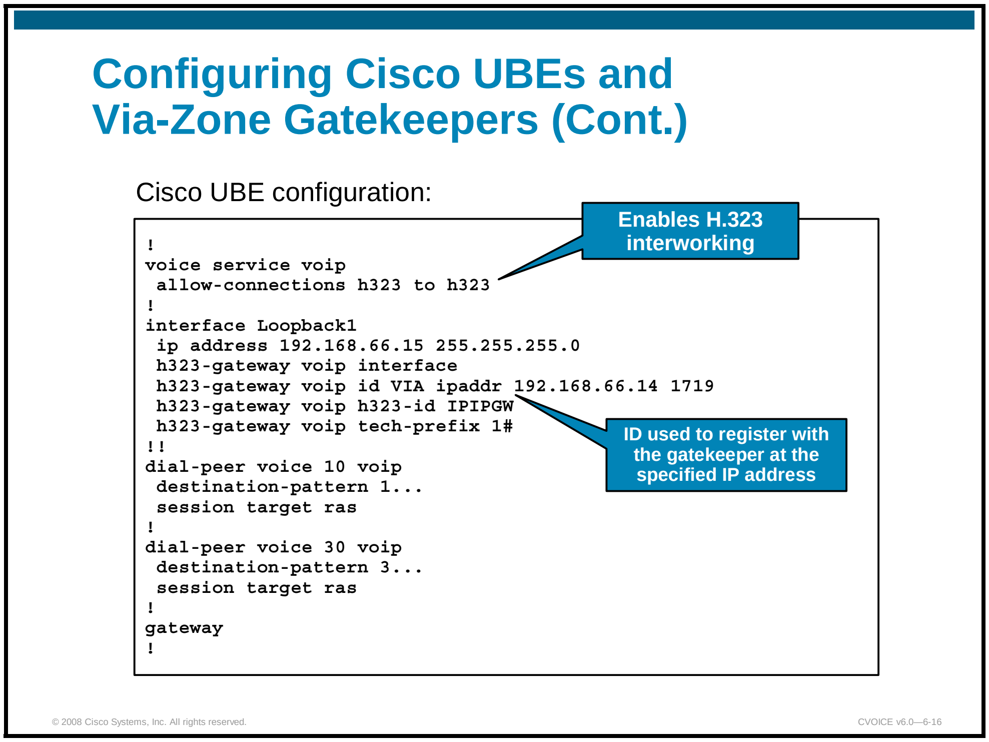
In addition to the SJC and CHI local zones, another local via-zone is configured. This zone will contain the Cisco UBE.

Step 3 Specify zone and technology prefixes.

Standard zone prefix routing is set up, and the default technology 1# is configured.

Configure the Cisco UBE

This subtopic covers configuration of the Cisco UBE.



Configuring Cisco UBEs and Via-Zone Gatekeepers (Cont.)

Cisco UBE configuration:

```
!
voice service voip
 allow-connections h323 to h323
!
interface Loopback1
 ip address 192.168.66.15 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id VIA ipaddr 192.168.66.14 1719
 h323-gateway voip h323-id IPIPGW
 h323-gateway voip tech-prefix 1#
!!
dial-peer voice 10 voip
 destination-pattern 1...
 session target ras
!
dial-peer voice 30 voip
 destination-pattern 3...
 session target ras
!
gateway
!
```

Enables H.323 interworking

ID used to register with the gatekeeper at the specified IP address

CVOICE v6.0—6-16

After the gatekeeper configuration is done, the Cisco UBE configuration is performed on the same router.

Complete these steps to configure the Cisco UBE.

Step 1 Enable H.323 interworking.

Step 2 Create a loopback interface to use as the source interface for the Cisco UBE to register with the gatekeeper.

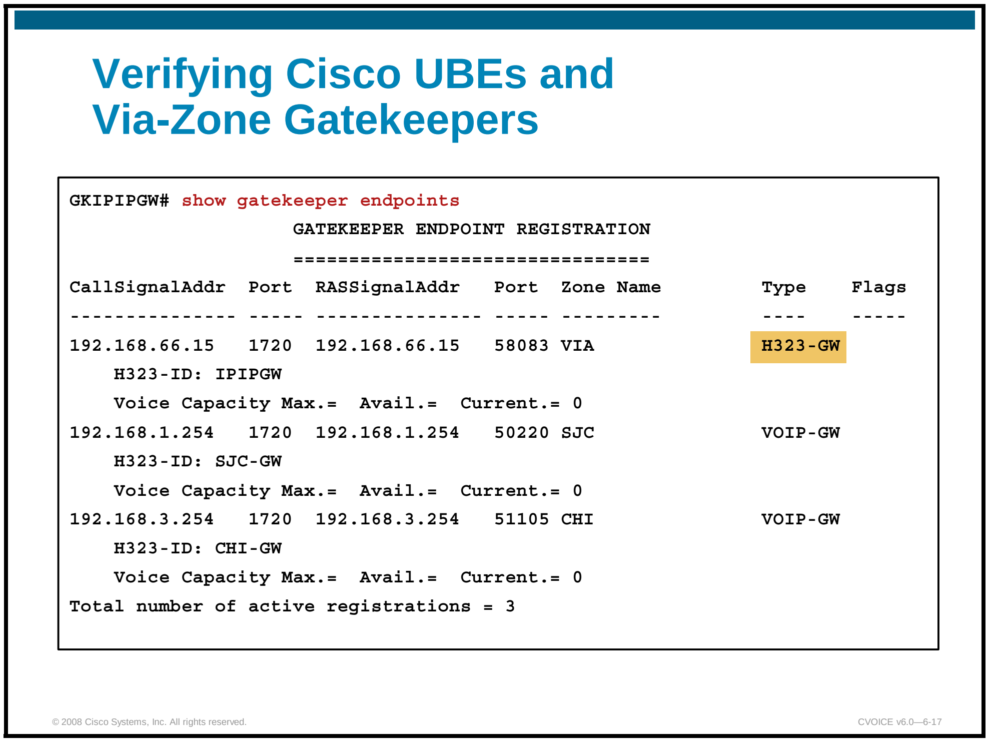
The Loopback1 interface is used as the H.323 gateway interface. The Cisco UBE will register in zone VIA, with the H.323 ID Cisco UBE and the technology prefix 1#

Step 3 Create two dial peers—one pointing to San Jose, and the other to Chicago.

Step 4 Enable the gateway process.

Verifying Cisco UBEs and Via-Zone Gatekeepers

This topic describes how to verify the Cisco UBE and via-zone gatekeeper operation.



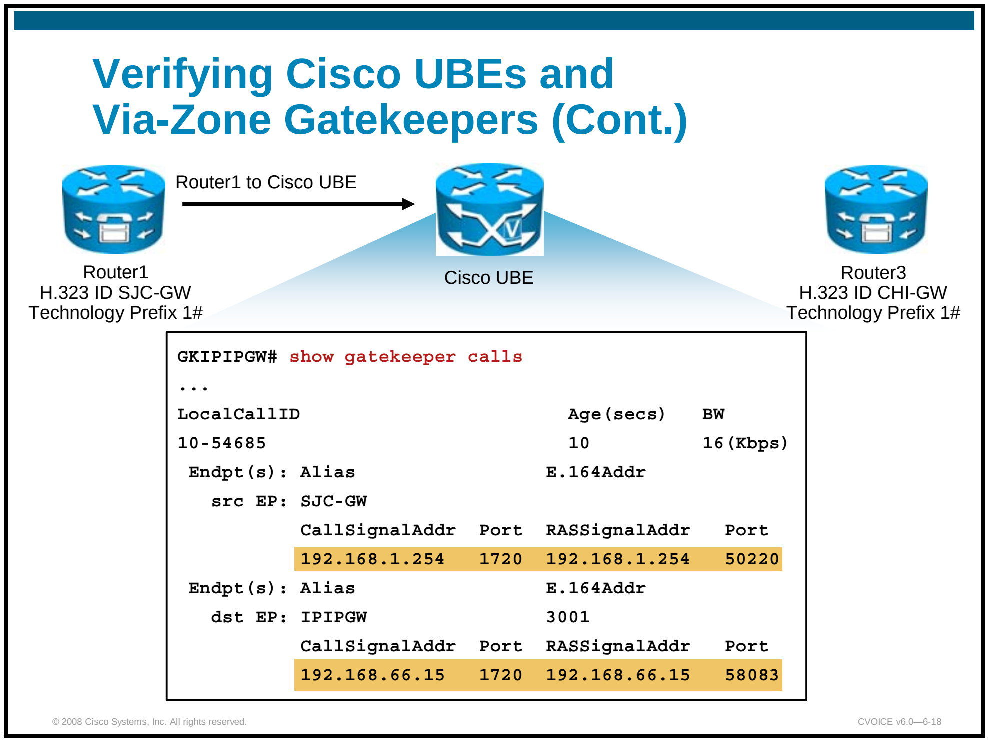
Verifying Cisco UBEs and Via-Zone Gatekeepers

```
GKIPIPGW# show gatekeeper endpoints
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type    Flags
--------------- ----- --------------- ----- ---------         ----    -----
192.168.66.15   1720  192.168.66.15   58083 VIA               H323-GW
    H323-ID: IPIPGW
    Voice Capacity Max.=  Avail.=  Current.= 0
192.168.1.254   1720  192.168.1.254   50220 SJC               VOIP-GW
    H323-ID: SJC-GW
    Voice Capacity Max.=  Avail.=  Current.= 0
192.168.3.254   1720  192.168.3.254   51105 CHI               VOIP-GW
    H323-ID: CHI-GW
    Voice Capacity Max.=  Avail.=  Current.= 0
Total number of active registrations = 3
```

© 2008 Cisco Systems, Inc. All rights reserved.

CVOICE v6.0—6-17

When you use the **show gatekeeper endpoints** command on the gatekeeper, a Cisco UBE will be displayed as an H323-GW type. In this output, the Cisco UBE is registered using the Loopback1 IP address 192.168.66.15.



Verifying Cisco UBEs and Via-Zone Gatekeepers (Cont.)

Router1 to Cisco UBE

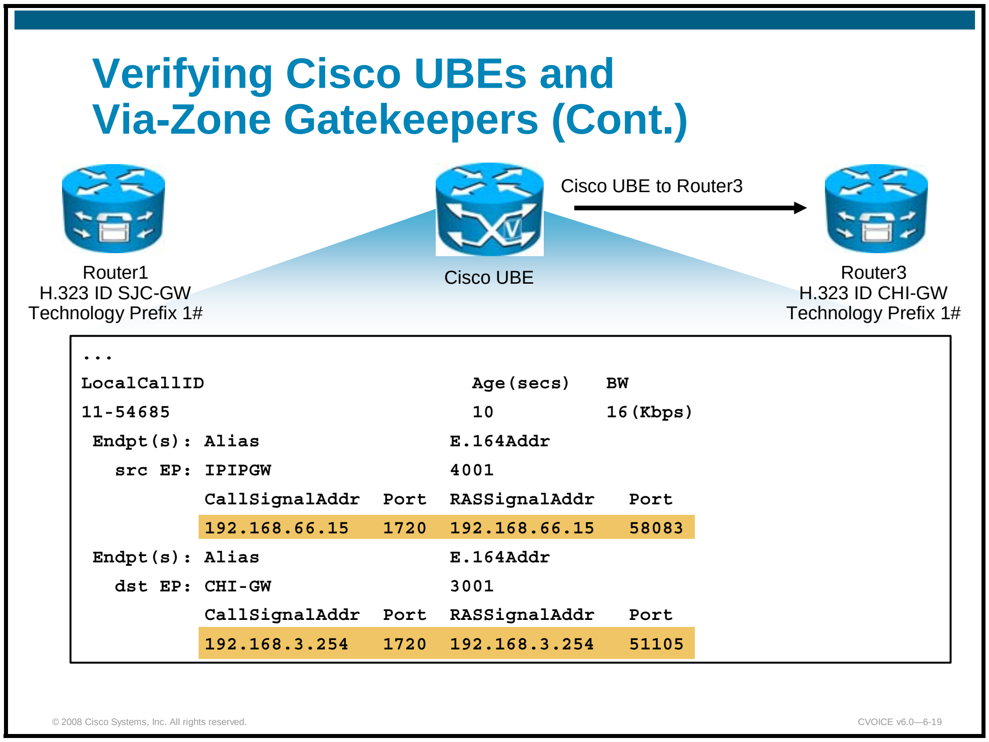
Router1
H.323 ID SJC-GW
Technology Prefix 1#

Cisco UBE

Router3
H.323 ID CHI-GW
Technology Prefix 1#

```
GKIPIPGW# show gatekeeper calls
...
LocalCallID                            Age(secs)   BW
10-54685                               10          16(Kbps)
 Endpt(s): Alias                     E.164Addr
   src EP: SJC-GW
           CallSignalAddr  Port  RASSignalAddr   Port
           192.168.1.254   1720  192.168.1.254   50220
 Endpt(s): Alias                     E.164Addr
   dst EP: IPIPGW                    3001
           CallSignalAddr  Port  RASSignalAddr   Port
           192.168.66.15   1720  192.168.66.15   58083
```

When a call is active, the **show gatekeeper calls** command will display two call legs. The first call leg is between the originating gateway (Router 1, in this case) and the Cisco UBE.



Verifying Cisco UBEs and Via-Zone Gatekeepers (Cont.)

Router1
H.323 ID SJC-GW
Technology Prefix 1#

Cisco UBE

Cisco UBE to Router3

Router3
H.323 ID CHI-GW
Technology Prefix 1#

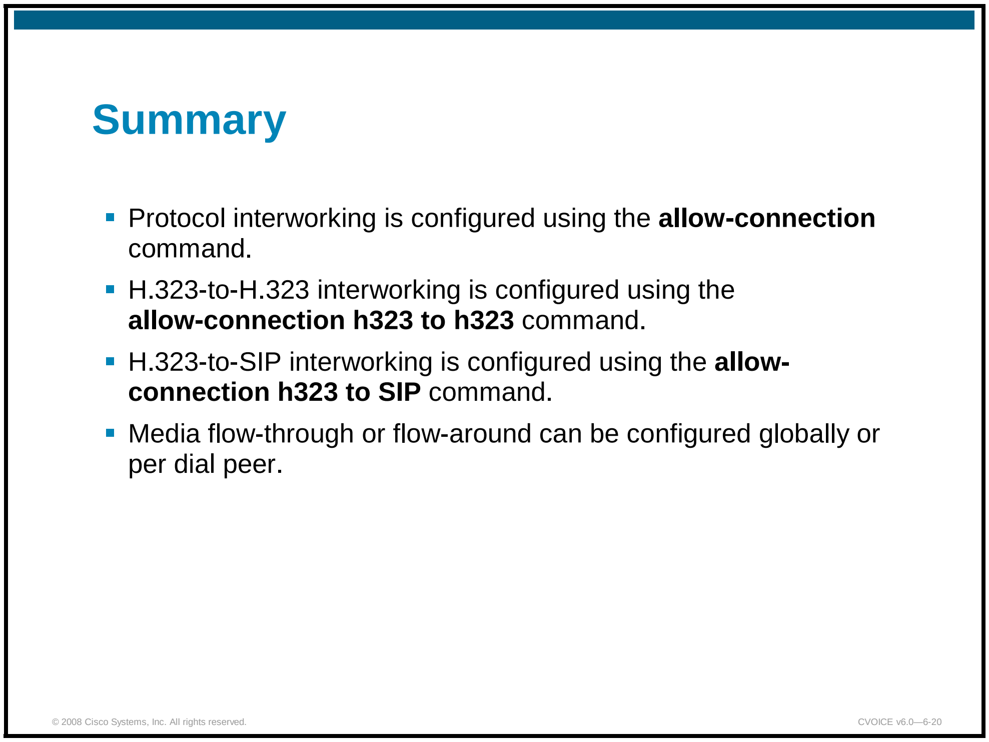
```
...
LocalCallID                         Age(secs)   BW
11-54685                            10          16(Kbps)
 Endpt(s): Alias                  E.164Addr
   src EP: IPIPGW                 4001
           CallSignalAddr  Port  RASSignalAddr   Port
           192.168.66.15   1720  192.168.66.15   58083
 Endpt(s): Alias                  E.164Addr
   dst EP: CHI-GW                 3001
           CallSignalAddr  Port  RASSignalAddr   Port
           192.168.3.254   1720  192.168.3.254   51105
```

CVOICE v6.0—6-19

The second call leg is between the Cisco UBE and the terminating gateway (Router 3, in this case).

Summary

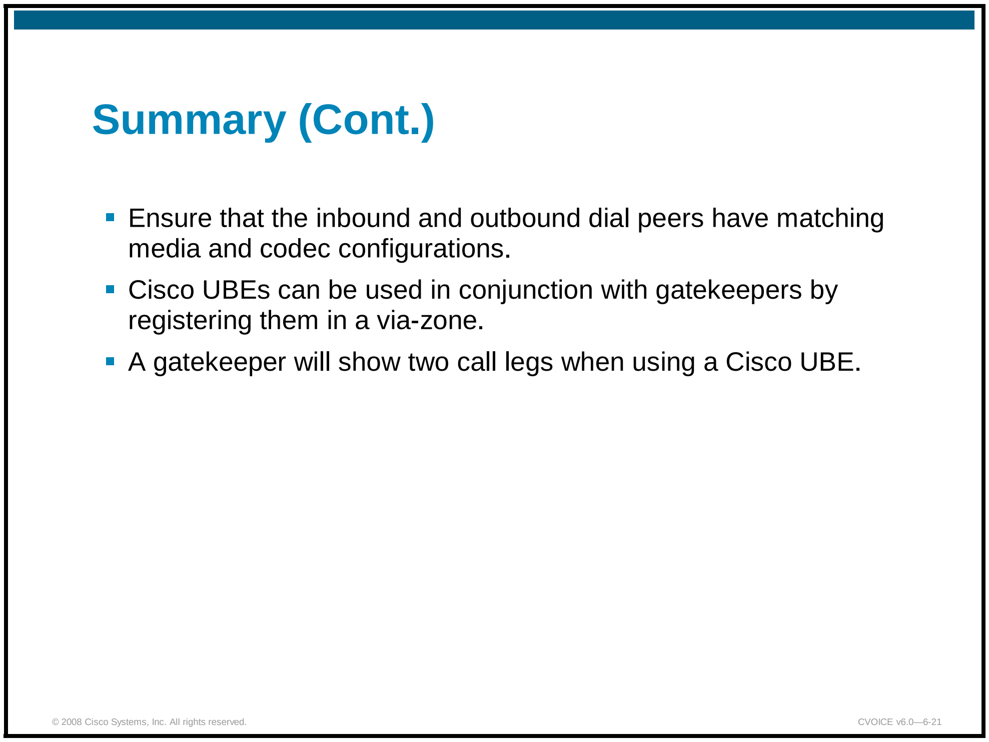
This topic summarizes the key points that were discussed in this lesson.



Summary

- Protocol interworking is configured using the **allow-connection** command.
- H.323-to-H.323 interworking is configured using the **allow-connection h323 to h323** command.
- H.323-to-SIP interworking is configured using the **allow-connection h323 to SIP** command.
- Media flow-through or flow-around can be configured globally or per dial peer.

CVOICE v6.0—6-20



Summary (Cont.)

- Ensure that the inbound and outbound dial peers have matching media and codec configurations.
- Cisco UBEs can be used in conjunction with gatekeepers by registering them in a via-zone.
- A gatekeeper will show two call legs when using a Cisco UBE.

CVOICE v6.0—6-21

Lesson Self-Check

Use the questions here to review what you learned in this lesson. The correct answers and solutions are found in the Lesson Self-Check Answer Key.

Q1) The configuration for H.323-to-SIP interworking is _________________.

Relates to: Protocol Interworking Command

A) unilateral
B) bilateral
C) unidirectional
D) bidirectional

Q2) Choose the correct command to enable H.323-to-H.323 interworking.

Relates to: Configuring H.323-to-H.323 Interworking

A) **allow-connections h323 to sip**
B) **allow-connections h323 to h323 interworking**
C) **allow-connections h323 interworking**
D) **allow-connections h323 to h323**

Q3) A Cisco Unified Communications Manager cluster needs to route outbound calls using H.323 to a SIP carrier. Which configuration is required?

Relates to: Configuring H.323-to-SIP Interworking

A) allow-connections h323 to sip
B) allow-connections sip to h323
C) **allow-connections sip to sip**
D) **allow-connections h323 to sip** and **allow-connections sip to h323**

Q4) Two Cisco Unified CallManager 4.X clusters need to be interconnected using RSVP-based CAC. Which requirements exist?

Relates to: Media Flow and Transparent Codec Commands

A) two IP-to-IP gateways, media flow-through
B) one IP-to-IP gateway, media flow-through
C) two IP-to-IP gateways, media flow around
D) one IP-to-IP gateway, media flow-around

Q5) Use the ________________ command to configure codec pass-through.

Relates to: Configuring Transparent Codec Pass-Through and Media Flow-Around

A) **transparent codec**
B) **codec transparent**
C) **codec auto**
D) **codec preference**

Q6) A gatekeeper should be configured to route calls between local zones via an IP-to-IP gateway. How can this be achieved?

Relates to: Configuring Cisco UBEs and Via-Zone Gatekeepers

A) The gatekeeper should route calls directly via an IP-to-IP gateway.
B) The gatekeeper should route calls via a local zone that contains an IP-to-IP gateway.
C) The gateways should route calls to the IP-to-IP gateway instead of the gatekeeper.
D) The gateway should register with a technology prefix that matches the technology prefix of an IP-to-IP gateway.

Q7) When you use the **show gatekeeper endpoints** command on the gatekeeper, a Cisco UBE will be displayed as a(n) __________ type.

Relates to: Verifying Cisco UBEs and Via-Zone Gatekeepers

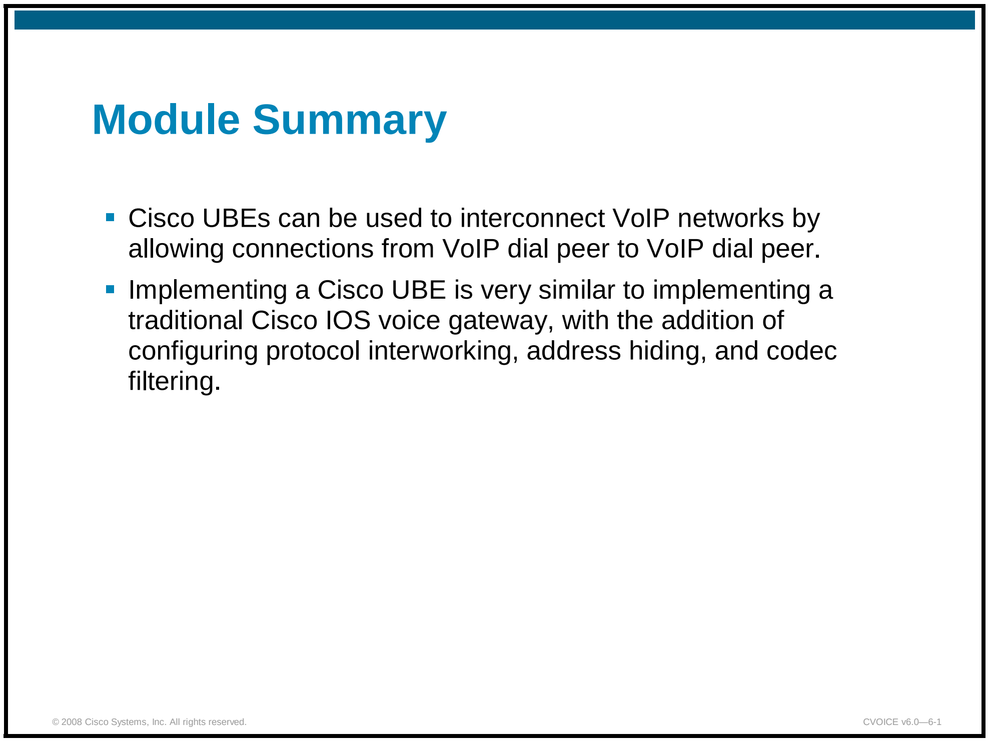
A) VOIP-GW
B) POTS-GW
C) H323-GW
D) TDM-GW

Lesson Self-Check Answer Key

Q1)	C
Q2)	D
Q3)	A
Q4)	A
Q5)	B
Q6)	B
Q7)	C

Module Summary

This topic summarizes the key points that were discussed in this module.



Module Summary

- Cisco UBEs can be used to interconnect VoIP networks by allowing connections from VoIP dial peer to VoIP dial peer.
- Implementing a Cisco UBE is very similar to implementing a traditional Cisco IOS voice gateway, with the addition of configuring protocol interworking, address hiding, and codec filtering.

CVOICE v6.0—6-1

This module discussed Cisco Unified Border Elements (Cisco UBEs), which interconnect voice and video over IP networks. Call routing is allowed between VoIP dial peers, enabling a Cisco UBE to interconnect an inbound VoIP call leg with an outbound VoIP call leg.

Implementing a Cisco UBE is very similar to implementing a standard Cisco IOS voice gateway. The same dial-plan components are used, but additional features are available for tuning the connections from VoIP dial peer to VoIP dial peer. This includes protocol interworking, address hiding, and codec filtering.

References

For additional information, refer to these resources:

- *Cisco Multiservice IP-to-IP Gateway:* http://www.cisco.com/en/US/products/sw/voicesw/ps5640/products_configuration_guide_book09186a0080409b6d.html
- *Cisco Multiservice IP-to-IP Gateway with Gatekeeper:* http://www.cisco.com/en/US/products/sw/voicesw/ps5640/products_configuration_guide_book09186a00806bed2d.html
- *Cisco Unified Border Element:* http://www.cisco.com/en/US/products/sw/voicesw/ps5640/products_data_sheet09186a00801da698.html
- *The Cisco Unified Border Element (CUBE) Configuration Application Note:* http://www.cisco.com/en/US/partner/products/sw/voicesw/ps5640/products_white_paper0900aecd8067937f.shtml
- *Cisco Voice Gateways and Gatekeepers, Cisco Press*