GWGK

Implementing Cisco Voice Gateways and Gatekeepers

Volume 2

Version 1.0

Student Guide

Text Part Number: 97-2223-01

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

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

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.

Students, this letter describes important course evaluation access information!

Welcome to Cisco Systems Learning. Through the Cisco Learning Partner Program, Cisco Systems is committed to bringing you the highest-quality training in the industry. Cisco learning products are designed to advance your professional goals and give you the expertise you need to build and maintain strategic networks.

Cisco relies on customer feedback to guide business decisions; therefore, your valuable input will help shape future Cisco course curricula, products, and training offerings. We would appreciate a few minutes of your time to complete a brief Cisco online course evaluation of your instructor and the course materials in this student kit. On the final day of class, your instructor will provide you with a URL directing you to a short post-course evaluation. If there is no Internet access in the classroom, please complete the evaluation within the next 48 hours or as soon as you can access the web.

On behalf of Cisco, thank you for choosing Cisco Learning Partners for your Internet technology training.

Sincerely,

Cisco Systems Learning

Table of Contents

Volume 2

Module 3

Implementing Dial Plans

Overview

This module discusses what a dial plan is and describes the critical elements that are required for implementing a scalable voice network. This module discusses dial plan design and configuration. It discusses the various ways to manipulate dial plans through the use of Cisco IOS software commands. Understanding digital manipulation and the options that are available to do this when the need arises is very critical in scaling a dial plan. Implementing class of service (CoS) using Class of Restrictions (COR) also will be covered. This module concludes with an in-depth look at how digit manipulation can influence call routes and how to configure a gateway to influence call flow.

Module Objectives

Upon completing this module, you will be able to implement a dial plan on a Cisco gateway by using dial plans, number plans, and COR applications. This ability includes being able to meet these objectives:

- Design an effective, scaleable numbering and dial plan for H.323, MGCP, and SIP gateways
- Improve call flow by designing and using translation rules and translation profiles to manipulate digits on a gateway that uses CLI
- Identify where in the gateway COR is applied and describe the configuration and verifications steps
- Influence call routes to provide redundancy and cost efficiency

Lesson 1

Dial Plan Overview

Overview

This lesson discusses dial plans and number plans and how important it is to scale these plans. You will understand how automatic number identification (ANI) and digital number identification service (DNIS) are used by a gateway and how numbering plans are manipulated. Using this knowledge, you will be able to implement a scalable dial plan for your organization.

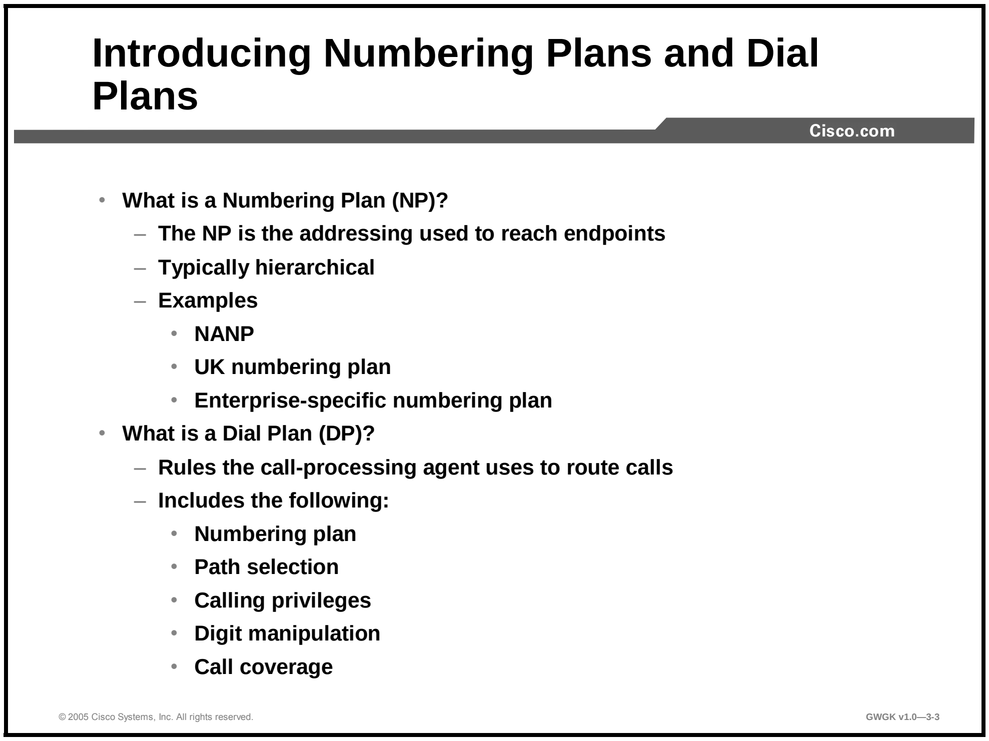
Objectives

Upon completing this lesson, you will be able to design an effective, scaleable numbering and dial plan for H.323, MGCP, and SIP gateways. This ability includes being able to meet these objectives:

- Define numbering plans and dial plans
- Given business and technical requirements, design a scaleable numbering plan
- Design a scaleable dial plan and explain why it is preferred to a static dial plan
- Identify the benefits and possible drawbacks of an overlapping dial plan

Introducing Numbering and Dial Plans

This topic describes numbering and dial plans and gives an overview of how and why each are used.



Introducing Numbering Plans and Dial Plans

Cisco.com

- What is a Numbering Plan (NP)?
  - The NP is the addressing used to reach endpoints
  - Typically hierarchical
  - Examples
    - NANP
    - UK numbering plan
    - Enterprise-specific numbering plan
- What is a Dial Plan (DP)?
  - Rules the call-processing agent uses to route calls
  - Includes the following:
    - Numbering plan
    - Path selection
    - Calling privileges
    - Digit manipulation
    - Call coverage

GWGK v1.0—3-3

A numbering plan is the addressing scheme that is used to reach voice endpoints. It consists of the digits that are dialed to reach a remote phone. For example, a company numbering plan might use four-digit extensions at each location and a three-digit site code. To call a phone at your own location, you would dial the four-digit extension. To call a phone at a remote company location, you would dial the site code and the extension.

The local public switched telephone network (PSTN) serving the company in this example also has a numbering plan. This numbering plan will vary from country to country. In North America, a typical number would include a three-digit area code, a three-digit prefix, and a four-digit subscriber number. Local calls can be 7 or 10 digits. Long distance calls are 11 digits, and international calls vary in length and are preceded by 011. The UK PSTN does not have a uniform structure like the North American Numbering Plan (NANP). Area codes can be 2 to 5 digits; subscriber numbers can be 5 to 8 digits; and service codes can be 3 to 6 digits. National numbers can be 10 or 11 digits (including the leading 0).

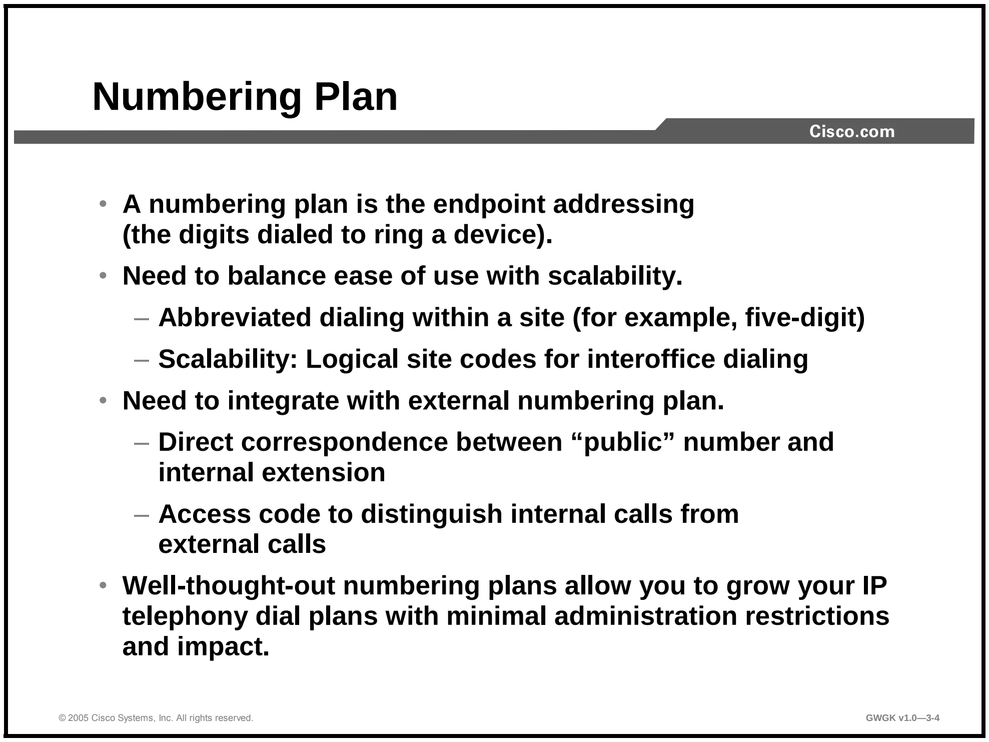
Conversely, a dial plan is more comprehensive and consists of the following:

- **Numbering plan (endpoint addressing):** Reachability of internal destinations is provided by assigning directory numbers (DNs) to all endpoints (such as IP phones, fax machines, and analog phones) and applications (such as voice-mail systems, auto attendants, and conferencing systems).
- **Path selection:** Depending on the calling device, different paths can be selected to reach the same destination. Moreover, a secondary path can be used when the primary path is not available (for example, a call can be transparently rerouted over the PSTN during an IP WAN failure).

- **Calling privileges or class of service (CoS):** Different groups of devices are assigned different classes of service based on granting or denying access to certain destinations. For example, lobby phones might be allowed to reach only internal and local PSTN destinations, while executive phones could have unrestricted PSTN access. The calling privileges assigned to a device are typically called class of service. In a Cisco voice gateway, class of service is implemented by assigning Class of Restrictions (COR) to dial peers. COR is discussed in detail in the “Class of Restrictions” lesson.
- **Digit manipulation:** In some cases, it is necessary to manipulate the dialed string before routing the call, for example, when you are rerouting over the PSTN a call originally dialed using the on-net access code, or when you are expanding an abbreviated code (such as 0 for the operator) to an extension.
- **Call coverage:** Special groups of devices can be created to handle incoming calls for a certain service according to different rules (top-down, circular hunt, longest idle, or broadcast).

Numbering Plans

This topic describes numbering plans.



Numbering Plan

Cisco.com

- **A numbering plan is the endpoint addressing (the digits dialed to ring a device).**
- **Need to balance ease of use with scalability.**
  - **Abbreviated dialing within a site (for example, five-digit)**
  - **Scalability: Logical site codes for interoffice dialing**
- **Need to integrate with external numbering plan.**
  - **Direct correspondence between “public” number and internal extension**
  - **Access code to distinguish internal calls from external calls**
- **Well-thought-out numbering plans allow you to grow your IP telephony dial plans with minimal administration restrictions and impact.**

GWGK v1.0—3-4

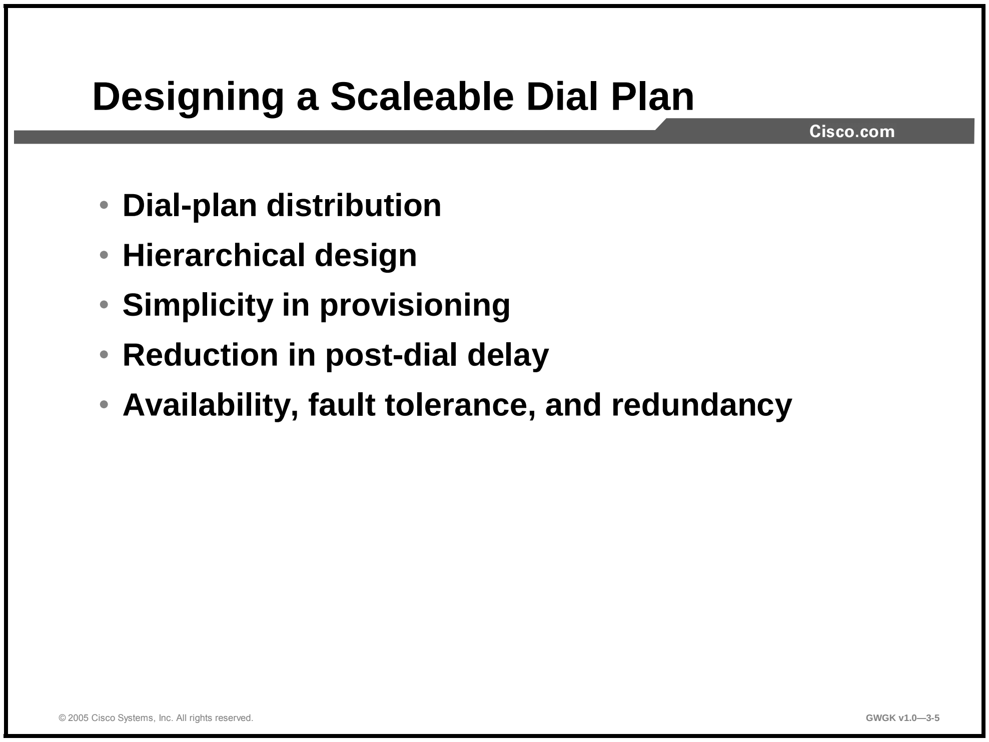
When deciding on a numbering plan, you must balance between ease of use and the ability to scale the numbering plan to accommodate both additional users and additional locations. It is typical to use a four- or five-digit extension for intraoffice dialing. For multisite facilities, a site code is often used along with an access code to indicate interoffice calling over the private network (VoIP or dedicated time-division multiplexing [TDM] circuits). A different access code is used to distinguish calls to the PSTN. Companies frequently try to match the extension to the publicly assigned number, referred to as Direct Inward Dialing (DID) or discard digits instruction (DDI) numbers (depending on location), but this is not always possible. For example, assume a company is using 9 as the PSTN access code and is using four-digit extensions internally. If the company is given a DID range of 555-8000–555-9999, some of the locally assigned four-digit extensions would begin with 9, making it difficult for the call-processing system to distinguish between internal and external calls. One solution to this issue would be to use five-digit extensions. This will result in all extensions beginning with a 5. You will to work with the service provider to determine if they can provide five incoming digits. If they are unable to provide five digits, the dial plan will need to manipulate the incoming digits to allow calls to be routed to the correct endpoint.

The following example shows how the company Span Engineering could implement their number plan.

All locations use a PSTN access code of 9 and an interoffice access code of 8. To accommodate a larger user base, Chicago uses five-digit extensions corresponding to the DID assigned to the device. All other locations use four-digit extensions. Chicago uses a two-digit site code. Other locations use a three-digit site code, resulting in eight-digits (access code [8] + site code + extension) interoffice calls. Span Engineering already uses a three-character office code for internal voice mail. For example, the Chicago site code is CHI and the San Francisco site code is SFO. Using the corresponding keypad digits, the site code for Chicago is 24, and the site code for San Francisco is 726. So, a caller in Chicago would dial 87264000 to reach extension 4000 in the San Francisco office.

Designing a Scaleable Dial Plan

This topic describes how to design scaleable dial plans.



Designing a Scaleable Dial Plan

Cisco.com

- Dial-plan distribution
- Hierarchical design
- Simplicity in provisioning
- Reduction in post-dial delay
- Availability, fault tolerance, and redundancy

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—3-5

This figure shows high-level considerations to keep in mind when you are designing, maintaining, and expanding a dial plan. These are some things you should consider when you are designing a scaleable dial plan:

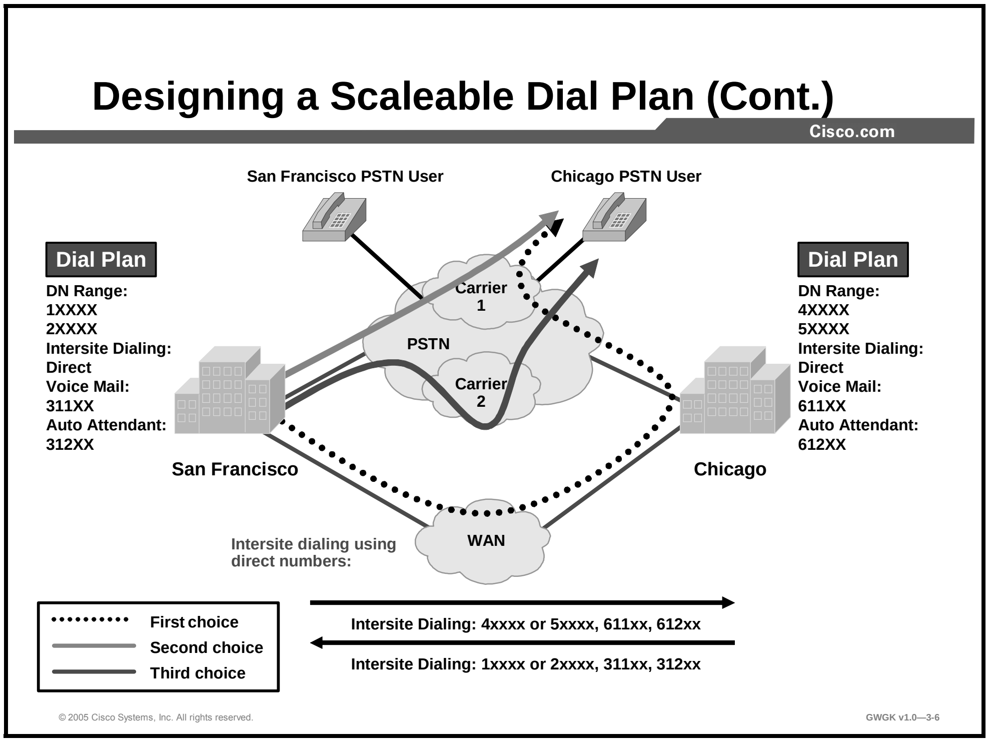
- **Dial-Plan Distribution:** Good dial-plan architecture relies on effectively distributing the dial-plan logic among the gateway and gatekeeper components. Isolating H.323 devices to a specific portion of the dial plan reduces the complexity of the configuration. Each component can focus on accomplishing specific tasks. Generally, local PSTN-specific details are handled at the local gateway; higher-level routing decisions are passed along to the gatekeepers and directory gatekeepers. A well-designed network places the majority of the dial-plan logic at the gatekeeper and directory gatekeeper devices.

- **Hierarchical Design:** Strive to keep the majority of the dial-plan logic (routing decision-making and failover) at the highest component level. For example, directory gatekeeper is generally considered the highest-level device. By maintaining a hierarchical design, you make the addition and deletion of zones more manageable. For example, scaling of the overall network is much easier when configuration changes need to be made only to a directory gatekeeper instead of to every zone gatekeeper. The size of the network dictates the level of hierarchy needed. A small business may have a single gateway while a medium-sized business may have multiple gateways and a single gatekeeper. As the company grows, the levels of hierarchy should also grow.

- **Simplicity in Provisioning:** You should keep the dial plan on the gateways and gatekeepers as simple and as symmetrical as possible when you are designing a network. Try to keep consistent dial plans on the gateways by using translation rules to manipulate the local-digit dialing patterns. These number patterns can be normalized into a standard format or pattern before the digits enter the VoIP core. Putting digits into a standard format simplifies gatekeeper zone-prefix provisioning and gateway dial-peer management.

This methodology helps reduce the number of dial peer configurations on the outgoing plain old telephone service (POTS) interface. If the gatekeeper can be provisioned to direct only calls of a certain area code to a particular gateway, then you would not need to provision all of the individual gateways with their respective area codes. Instead, you might be able to generalize the gateway configurations. By normalizing the number, you also reduce the zone-prefix search length, reducing the time required to search for a zone prefix match. For example, if you have the 0118943xxxx digit pattern, you can send the number as 8943xxxx and have the gatekeeper search on 89 as opposed to 01189.

- **Reducing Postdial Delay:** When you design a large-scale dial plan, you should consider the effects of postdial delay in the network. Postdial delay is the time from when the last digit is dialed to the moment the phone rings at the receiving location. Gateways, gatekeeper zone design, translation rules, and sequential Locate Request (LRQs) all affect post dial delay. Strive to use these tools most efficiently to reduce postdial delay.
- **Availability and Fault Tolerance:** During your dial-plan design, you should consider overall network availability and call success rate. Fault tolerance and redundancy within VoIP networks are most important at the gatekeeper level. Use of an alternate gatekeeper, sequential Location Requests (LRQs), and Hot Standby Routing Protocol (HSRP) help provide redundancy and fault tolerance in the H.323 network.



Designing a Scaleable Dial Plan (Cont.)

Dial Plan

DN Range:
1XXXX
2XXXX
Intersite Dialing:
Direct
Voice Mail:
311XX
Auto Attendant:
312XX

Dial Plan

DN Range:
4XXXX
5XXXX
Intersite Dialing:
Direct
Voice Mail:
611XX
Auto Attendant:
612XX

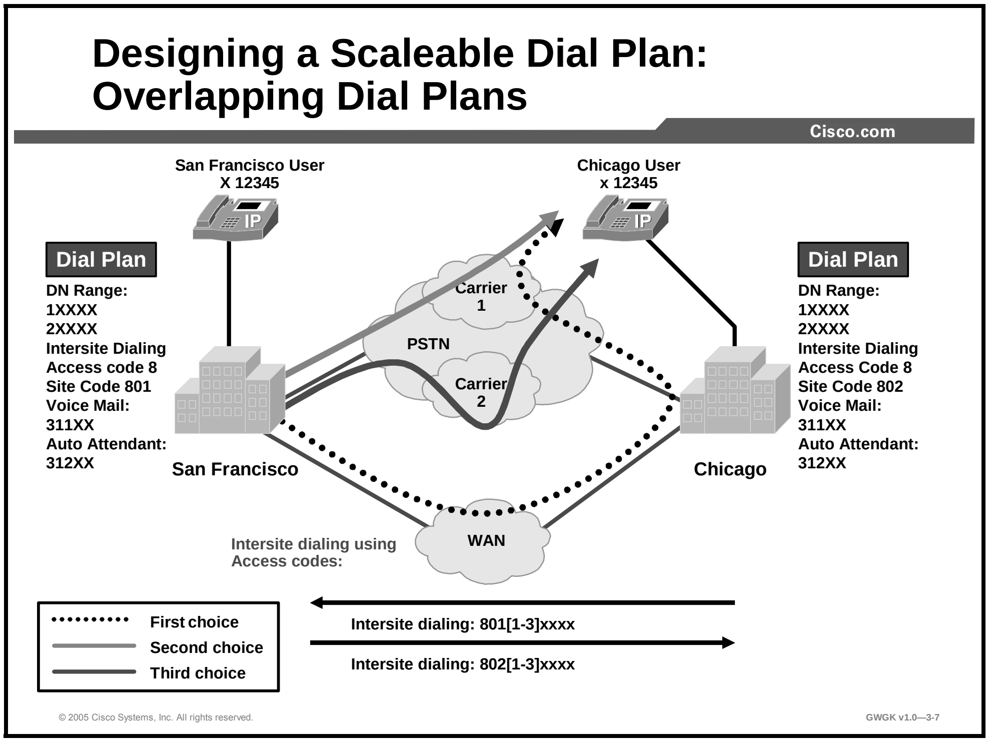
Intersite Dialing: 4xxxx or 5xxxx, 611xx, 612xx

Intersite Dialing: 1xxxx or 2xxxx, 311xx, 312xx

·········	First choice
▬	Second choice
▬	Third choice

GWGK v1.0—3-6

This and the next three figures show common dial-plan scenarios. This example shows a possible dial-plan scenario for the Chicago and San Francisco sites of Span Engineering. Each of the sites has unique, five-digit DNs, so direct DN dialing is possible. In addition, tail-end hop-off (TEHO) and least-cost routing are also deployed. If a user in Chicago dials a San Francisco PSTN number, the call will travel across the WAN and enter the San Francisco PSTN using a gateway located at the San Francisco site. If this is not possible, perhaps due to a congested WAN, the call will be placed using Carrier 1. If no trunks are available for Carrier 1, Carrier 2 would be used. This figure shows no overlapping dial plan.



Designing a Scaleable Dial Plan: Overlapping Dial Plans

Dial Plan

DN Range:
1XXXX
2XXXX
Intersite Dialing
Access code 8
Site Code 801
Voice Mail:
311XX
Auto Attendant:
312XX

Dial Plan

DN Range:
1XXXX
2XXXX
Intersite Dialing
Access Code 8
Site Code 802
Voice Mail:
311XX
Auto Attendant:
312XX

••••••••••	First choice
▬	Second choice
▬	Third choice

← Intersite dialing: 801[1-3]xxxx

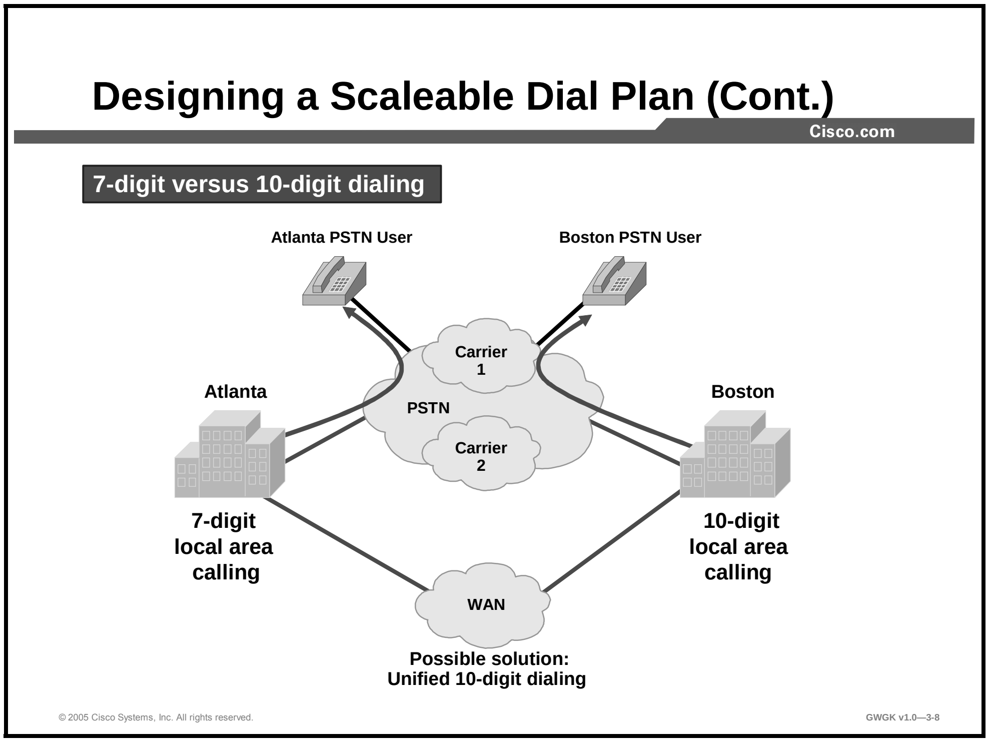
→ Intersite dialing: 802[1-3]xxxx

GWGK v1.0—3-7

Using the same topology as the previous figure, the dial plan in this figure has been changed so that dial plans of both sites overlap. A user in Chicago can no longer dial the five-digit extension of a user in San Francisco. The simplest solution to overlapping dial plans is to implement site codes. For intersite calling, users dial an access code followed by a site code and the extension. The call processing system or the gateway matches on this number, strips off the access code and site code, and routes the call to the appropriate destination. Additional digit manipulation may be required to use alternate routes.

The access code selected for intersite dialing should be different from the access code used for off-net calling. If you use the same access code, you will need to make sure your intersite calls can be distinguished from off-net calls. This can lead to a very complicated dial plan. In the United States, it is typical to use 9 as the access code for off-net dialing and 8 as the access code for inter-site dialing. The numbers used are not as important as making sure you that do not introduce complications to the dial plan.

In the figure, extension 12345 in Chicago wishes to call extension 12345 in San Francisco. The dial plan is configured for an intersite access code of 8 followed by a two-digit site code. The user dials 8-02-2345. The gateway matches this pattern to a dial peer and routes the call to Chicago. The gateway should translate both the called and the calling number. The called number should arrive in San Francisco as the five-digit extension so the call can be extended to the correct phone. If the calling number is not translated, the users in San Francisco will think the call is coming from their own phone.



Designing a Scaleable Dial Plan (Cont.)

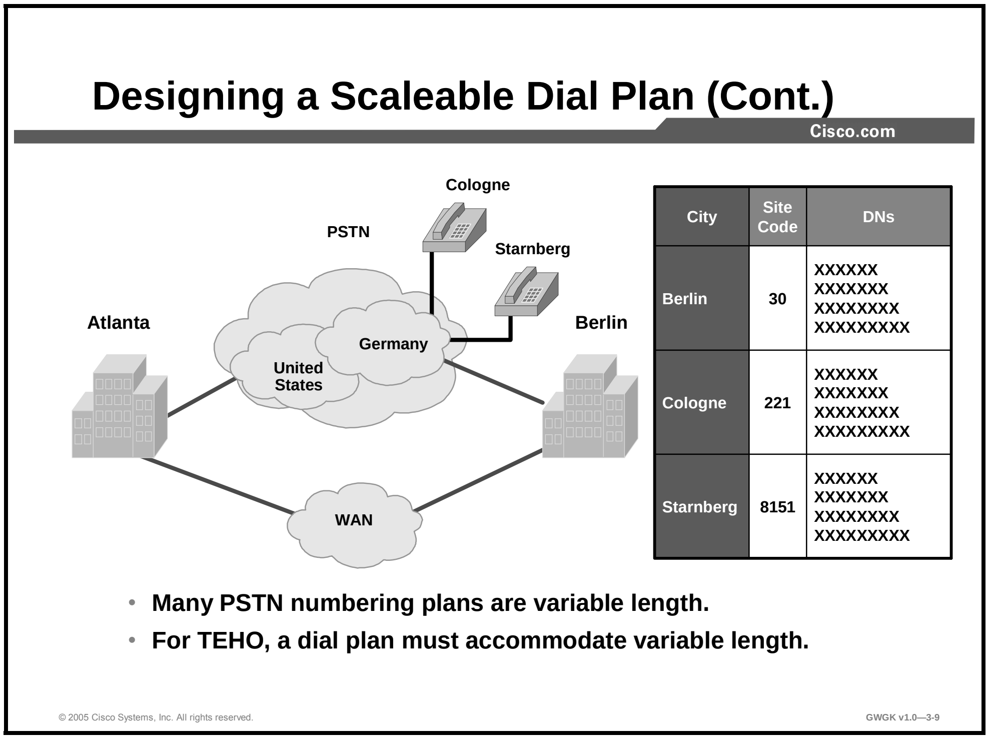
Cisco.com

7-digit versus 10-digit dialing

Possible solution:
Unified 10-digit dialing

GWGK v1.0—3-8

The network in this example has two sites: Atlanta and Boston. Atlanta uses 7-digit dialing, and Boston uses 10-digit dialing for local calls. The combination of these mixed dial plans is not advisable. A recommended solution would be to use a centralized dial plan with 10-digit dialing as the basis for all local calls. 7-digit dialing can still be supported using the appropriate voice translation rules and route patterns.



Designing a Scaleable Dial Plan (Cont.)

City	Site Code	DNs
Berlin	30	XXXXXX XXXXXXX XXXXXXXX XXXXXXXXX
Cologne	221	XXXXXX XXXXXXX XXXXXXXX XXXXXXXXX
Starnberg	8151	XXXXXX XXXXXXX XXXXXXXX XXXXXXXXX

- **Many PSTN numbering plans are variable length.**
- **For TEHO, a dial plan must accommodate variable length.**

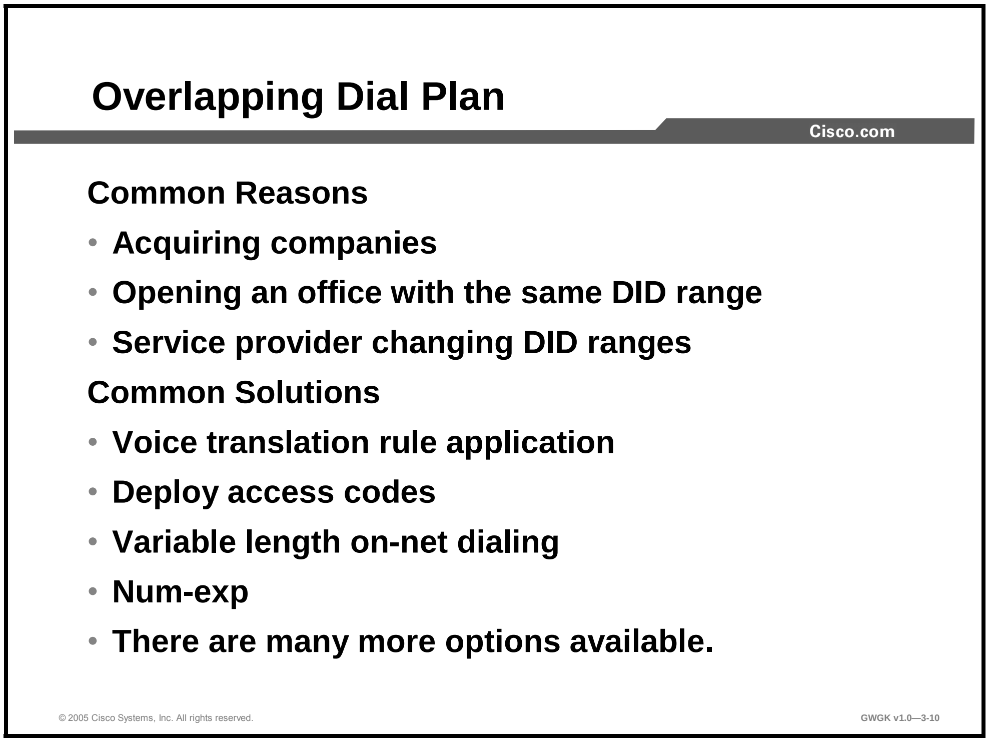
GWGK v1.0—3-9

Dial plans become more complex when you are considering country-specific dial plans for intersite calls, TEHO, or normal international calls. Having specific, fixed-length route patterns for international calls is impossible because every country has its own national numbering plan, which may even be variable length. For example, the German dial plan is a variable-length plan for access codes and DNs. Ideally, the dial plan would allow the user to dial the same number to reach the destination without worrying if the call was routed over the WAN or the PSTN. A solution to meet the requirements for this dial plan is to use access codes for the countries where TEHO is required.

This figure shows the complexities that exist when you are considering your international dialing dial plan.

Overlapping Dial Plans

This topic describes overlapping dial plans.



Overlapping Dial Plan

Cisco.com

Common Reasons

- **Acquiring companies**
- **Opening an office with the same DID range**
- **Service provider changing DID ranges**

Common Solutions

- **Voice translation rule application**
- **Deploy access codes**
- **Variable length on-net dialing**
- **Num-exp**
- **There are many more options available.**

GWGK v1.0—3-10

Overlapping dial plans can occur for various reasons. Besides the common causes for overlapping dial plans, there are possible solutions to overcome it. Overlapping dial plans may not be avoidable, so the following are some best practices for addressing overlapping dial plans:

- All on-net extension dialing must be globally unique. For instance, in a system using an abbreviated four-digit on-net dial plan, there cannot be an extension 1000 in site A and another extension 1000 in site B if the requirement is to reach either of them by dialing only four digits from site C.
- There cannot be any partial overlap between different dial strings.
  - For instance, if 9 is used as an off-net access code in a four-digit abbreviated dial plan (for example, for making PSTN calls), there cannot be any extensions in the 9XXX range. Attempting to do so would create situations where calls are not routed immediately. For example, if a user dialed 9141, the system would have to wait for either more digits (if the user were dialing 9 1 415 555 1234, for example) or the expiration of the interdigit timeout before routing the call to extension 9141. Likewise, if an operator code is used (for example, 0), the entire 0XXX extension range would have to be excluded from a four-digit uniform dial plan.
  - There cannot be overlapping strings of different length. For example, a system with extensions 1000 and 10000 would force users to wait for the interdigit timeout when they dial 1000.

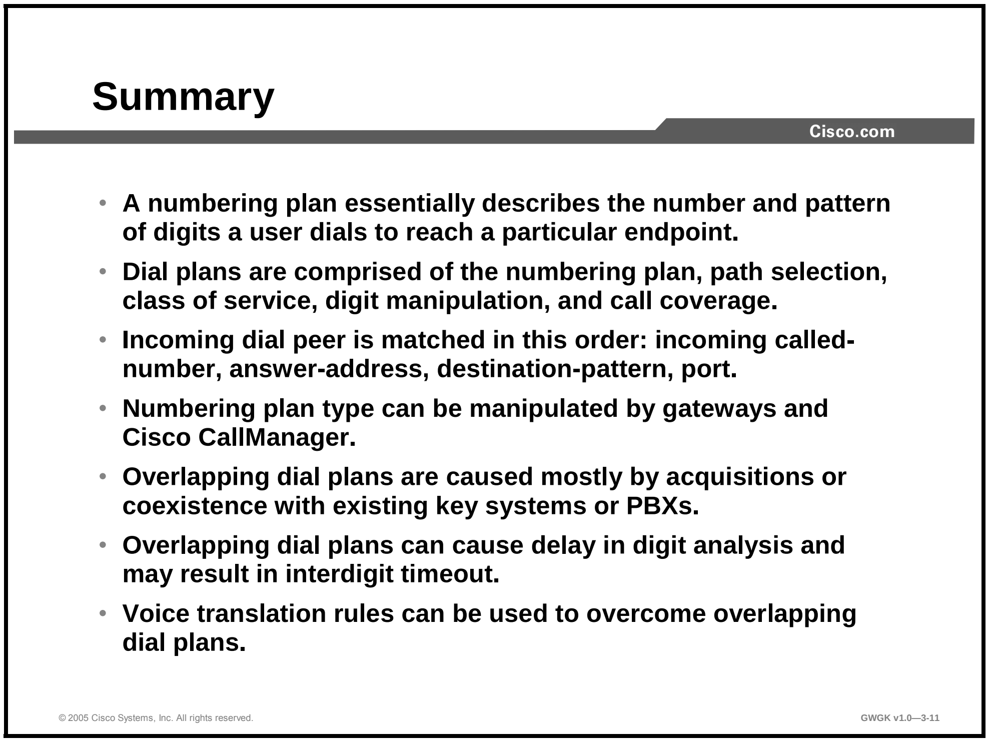
Variable-Length On-Net Dial Plan

Systems with many sites or overlapping site-extension ranges can benefit from the use of a variable-length dial plan with the following characteristics:

- Within a site, the system retains the use of abbreviated dialing for calls to on-net extensions (for example, four-digit dialing).
- Between sites, users dial an access code followed by a site code and the on-net extension of the destination.
- Off-net calls require an access code followed by a PSTN number.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

Cisco.com

- A numbering plan essentially describes the number and pattern of digits a user dials to reach a particular endpoint.
- Dial plans are comprised of the numbering plan, path selection, class of service, digit manipulation, and call coverage.
- Incoming dial peer is matched in this order: incoming called-number, answer-address, destination-pattern, port.
- Numbering plan type can be manipulated by gateways and Cisco CallManager.
- Overlapping dial plans are caused mostly by acquisitions or coexistence with existing key systems or PBXs.
- Overlapping dial plans can cause delay in digit analysis and may result in interdigit timeout.
- Voice translation rules can be used to overcome overlapping dial plans.

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—3-11

References

For additional information, refer to these resources:

- http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_chapter09186a00802c37f9.html
- http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a0080080aec.html#wp1241391

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) Which statements best describe dial plans on H.323 and SIP gateways? (Choose two.) (Source:)

A) They are defined by the call agent and then uploaded to the gateways.
B) They are considered part of POTS and VoIP call legs.
C) They are defined by the use of dial peers.
D) They are defined by the call agent.

Q2) Which statement best describes a well thought-out numbering plan? (Source:)

A) It reflects NANP.
B) It allows a customer to grow their IP telephony dial pans with minimal administrative restrictions.
C) It helps with designing the dial plan.
D) It reflects NPA and NXX.

Lesson Self-Check Answer Key

Q1)	B, C
Q2)	B

Lesson 2

Digit Manipulation

Overview

This lesson discusses digit manipulation and the associated Cisco IOS commands that are used to achieve and improve voice traffic call flow through a gateway. It also discusses how to use translation rules to manipulate calling features.

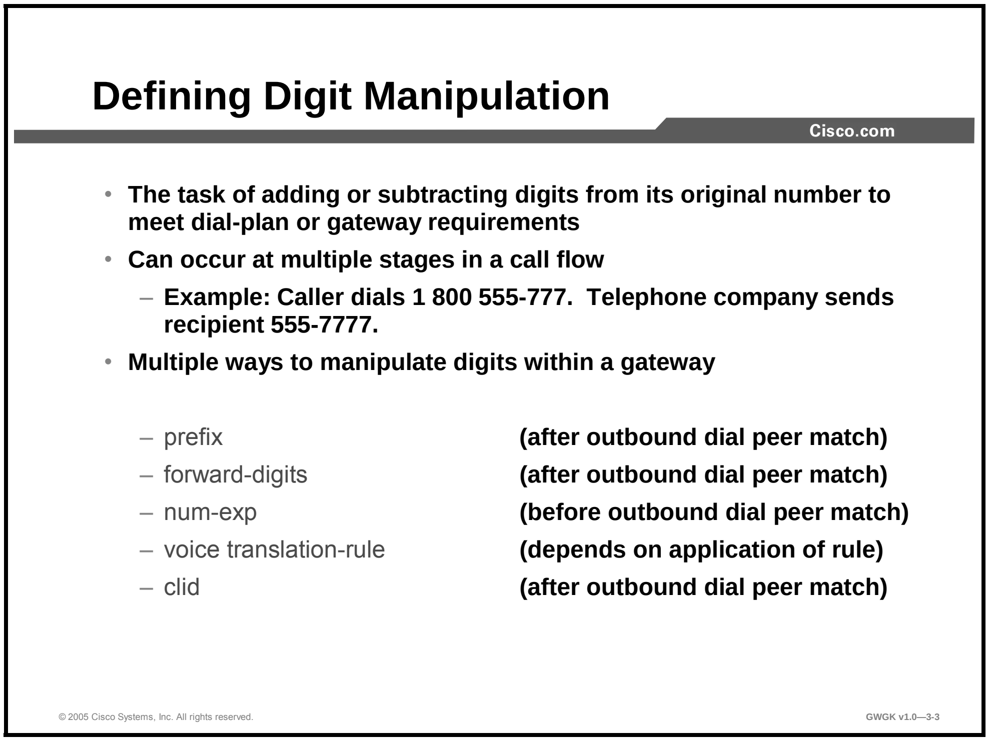
Objectives

Upon completing this lesson, you will be able to improve call flow by designing and using translation rules and translation profiles to manipulate digits on a gateway that uses CLI. This ability includes being able to meet these objectives:

- Define digit manipulation
- Describe how a dial peer matches digits
- Define the regular expressions used by a translation rule
- Describe the configuration steps for implementing translation rules
- Use translation rules to manipulate ANI and DNIS
- Manipulate ISDN numbering types
- Troubleshoot translation rules
- Define the order of operation for digit manipulation through a gateway

Defining Digit Manipulation

This topic defines digit manipulation and describes the methods of manipulating digits in a gateway.



Defining Digit Manipulation

Cisco.com

- **The task of adding or subtracting digits from its original number to meet dial-plan or gateway requirements**
- **Can occur at multiple stages in a call flow**
  - **Example: Caller dials 1 800 555-777. Telephone company sends recipient 555-7777.**
- **Multiple ways to manipulate digits within a gateway**

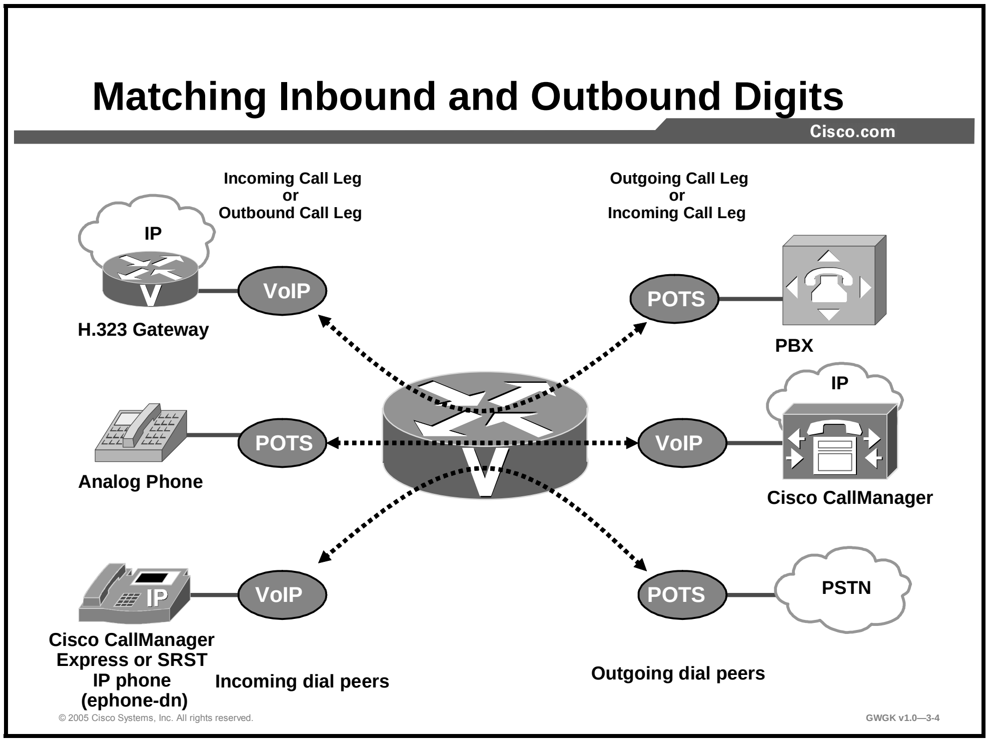
– prefix	**(after outbound dial peer match)**
– forward-digits	**(after outbound dial peer match)**
– num-exp	**(before outbound dial peer match)**
– voice translation-rule	**(depends on application of rule)**
– clid	**(after outbound dial peer match)**

GWGK v1.0—3-3

Digit manipulation is used typically to hide dial plan complexity from the caller. For example, Span Engineering uses an access code of “8” and a site code to place interoffice calls. If the call is routed over the IP WAN, the originating gateway strips the access code and sends the seven digits that represent the site code and extension to the terminating gateway. The terminating gateway strips the site code from the called number and sends the four- or five-digit extension to the CallManager or PBX so the call can be extended to the correct device. If the IP WAN is unavailable or congested, the originating gateway strips the access code and site code and prefixes the digits that the PSTN requires to route the call.

Matching Inbound and Outbound Digits

This topic describes how a gateway matches inbound and outbound dialed digits.



Matching Inbound and Outbound Digits

Cisco.com

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—3-4

Every VoIP call has an inbound and outbound call leg associated with it. The inbound and outbound element is from the perspective of the router. The router can originate a call or terminate a call. A router can be an originating and terminating gateway, and therefore, the router performs an incoming dial-peer match to an outbound dial-peer match within the same the device. The router matches dial peers in the same way whether the matching is done on the same device or the router is forwarding the call onto the next hop.

Call routing in Cisco IOS software is controlled by a list of configuration structures called dial peers. A dial peer can be defined as either a plain old telephone service (POTS) dial peer or one of several VoIP dial peers.

The following are examples of a POTS and VoIP dial peers:

```
dial-peer voice 111 pots
  destination-pattern 9T
  direct-inward-dial
  port 0/1/0:23


dial-peer voice 99 voip
 incoming called-number 9
 destination-pattern 1…
 session target ipv4:172.16.1.1
 dtmf-rely h245-alphanumeric
 codec g711ulaw
 no vad
```

POTS dial peers define the characteristics of a traditional telephony network connection. This dial peer maps a dial string to a specific voice port on a local gateway. Normally, this voice port connects the gateway to the local PSTN, a PBX, or analog telephone.

When you are determining how inbound dial peers are matched on a gateway, it is important to understand whether the inbound call leg is matched to a POTS or VoIP dial peer.

How a Gateway Matches Inbound Dial Peers

As is shown in the configuration example presented previously, when a call arrives from a PBX, the gateway must select an inbound dial peer. Suppose that the called number was 95551212 and the calling party number is 1001. In this case, the gateway matches the incoming dial peer 99 because the **incoming called-number** command matches the calling number 9.

Next, the gateway must select the outbound peer and uses the destination pattern as the criteria for matching. So, the gateway matches dial peer 111 for the outbound portion of the call leg.

If there is no incoming called number configured on a dial peer, the next possibility for matching an inbound peer involves **answer-address**. The **answer-address** command tries for a match using the calling number information instead of the called number criteria. For example, if **answer-address** was configured under a VoIP dial peer with the configuration of "1…", a call with the calling number of 1001 would match that VoIP dial peer for the incoming dial peer call leg.

If no peer matches based on **incoming called-number** or **answer-address**, then the calling party information is matched against the destination pattern that is configured on the dial peer. The focus here is on matching for the inbound peer characteristics, not for any routing information. The following is an example of using the **destination-pattern** command as the criteria for inbound peer matching:

```
dial-peer voice 111 pots
  destination-pattern 9T
  direct-inward-dial
  port 0/1/0:23

dial-peer voice 99 voip
 destination-pattern 1…
 session target ipv4:172.16.1.1
 dtmf-rely h245-alphanumeric
 codec g711ulaw
 no vad
```

Suppose that a call comes in with a called party number 95551212, and the calling party number is 1001. No peer matches the incoming called number for 95551212, and there is no peer with an answer address that matches 1001. The last resort is to look for a destination pattern that matches 1001. Dial peer 99 matches 1001 because of the **destination-pattern 1…**. The gateway still needs to select an outbound peer. That match is dial peer 111, which is based on the destination pattern match on the called party number 95551212.

For calls that originate on a POTS port, the same rules for dial peer selection of an inbound dial peer apply, with one additional possibility. If an inbound peer cannot be matched using any of the three methods (incoming called number, answer address, or destination pattern), the inbound peer is matched based upon port configuration. In this case, the dial peer used would be the first dial peer in the configuration that specifies the port the call came in on.

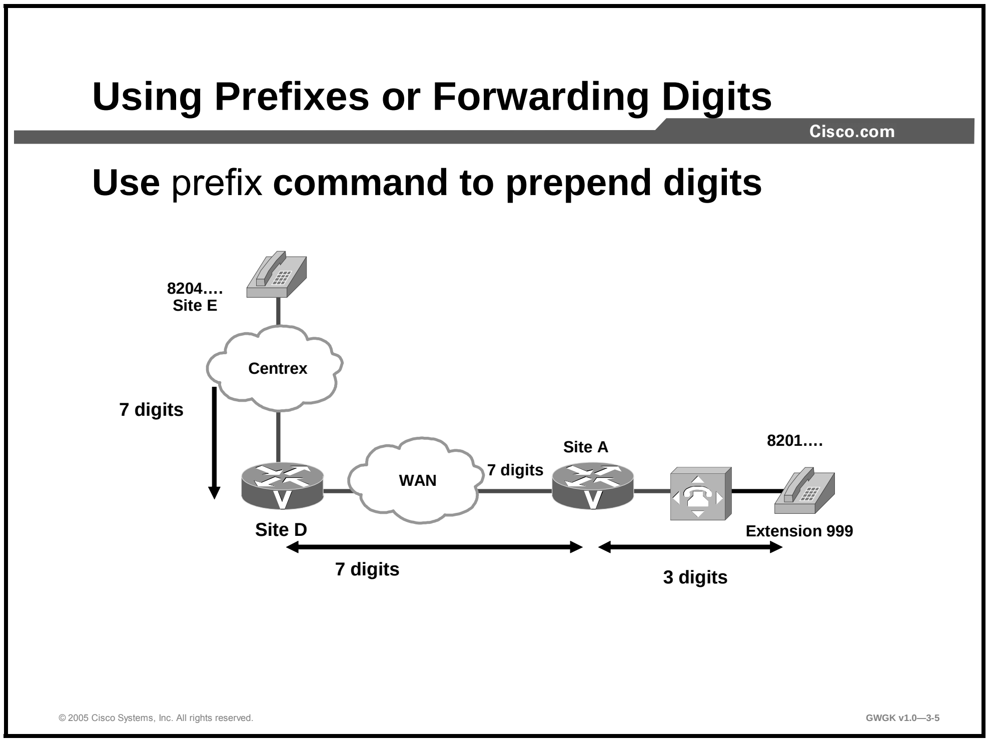
If no inbound peer can be matched using any of the criteria already listed, then the inbound peer is set to dial peer 0. The characteristics of dial peer 0, also seen as **peer ID = 0** in **debug voice ccapi inout**, is as follows:

- Any supported codec
- No dual tone multifrequency (DTMF) relay
- IP precedence 0
- VAD-enabled
- No Resource Reservation Protocol (RVSP)
- Fax-rate voice

It is not possible to modify dial peer 0. You should always have a peer with **incoming called-number** configured correctly to ensure that you always match a VoIP peer with the parameters you want when you are placing outbound calls through a Cisco IOS gateway.

Using Prefixes and No-Digit Stripping

This topic describes how to use prefixes and no-digit stripping.



Using Prefixes or Forwarding Digits

Cisco.com

Use prefix command to prepend digits

GWGK v1.0—3-5

In the figure, when Site E (with destination pattern “8204...”) dials the number 8201999, the full seven-digit dialed string is passed through the Centrex service to the router at Site D. This router matches the destination pattern “8201...” and forwards the seven-digit dial string to the router at Site A. This router matches the destination pattern “8201...”, strips off the matching 8201, and forwards the remaining three-digit dial string to the PBX. The PBX matches the correct station and completes the call to the proper extension.

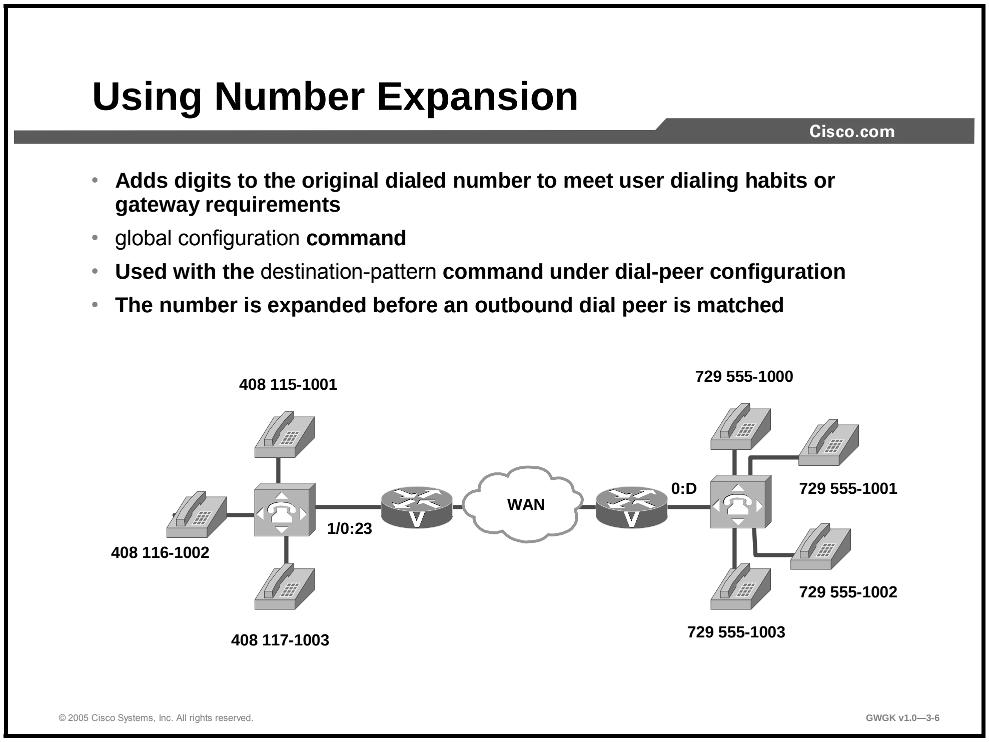
Calls in the reverse direction are handled similarly at Site A, but because the Centrex service requires the full seven-digit dial string to complete calls, the POTS dial peer at Site D is configured with no-digit stripping. Alternatively, digit stripping could be enabled and the dial peer could be configured with a four-digit prefix, in this case 8204, which would result in the router forwarding the full dial string to the Centrex service. Here are descriptions of the **prefix** and **forward-digits** dial-peer commands:

- **prefix:** This dial-peer command adds digits to the front of the dial string before the number is forwarded out of the gateway. The forwarding of the prefixed number occurs after the gateway matches an outbound dial peer but before the actual digits are sent out of the gateway telephony interface. Use the prefix command when the dialed digits leaving the gateway must be changed from the dialed number that had originally matched the dial peer. For example, a call is dialed using a four-digit extension such as 5000, but the call needs to be routed to the PSTN, which requires seven-digit dialing. If the four-digit extension matches the last four digits of the PSTN telephone number, then you could use the **prefix 527** command to prepend the three additional digits that are needed for the PSTN to route the call to 5275000.

- **forward-digits:** This dial-peer command specifies the number of digits that must be forwarded to the telephony interface, regardless of whether they are explicitly matched or wildcard matched. This command occurs after the outbound dial peer is matched, but before the digits are sent out of the gateway telephony interface. When a specific number of digits are configured for forwarding, the count is right justified. For example, if the port associated with the POTS dial peer is connected to a PBX and has a destination pattern configured to match all extensions in the 5000 range (**destination-pattern 5…**), by default, only the last three digits are forwarded. The gateway will strip the other five. If the PBX needs all four digits to route the call, you can use the command **forward-digits 4**. This commands tells the gateway that, when it finds an outbound dial-peer match, to make sure that the number forwarded is four digits in length starting from the right. To restore **forward-digits** to its default setting, use **default forward-digits** command.

Using Number Expansion

This topic describes number expansion.



Using Number Expansion

Cisco.com

- **Adds digits to the original dialed number to meet user dialing habits or gateway requirements**
- global configuration **command**
- **Used with the** destination-pattern **command under dial-peer configuration**
- **The number is expanded before an outbound dial peer is matched**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—3-6

This figure shows a network for a small company that wants to use VoIP to integrate its telephony network with its existing IP network. The destination patterns (or expanded telephone numbers) associated with Router A are 408 115-xxxx, 408 116-xxxx, and 408 117-xxxx, where xxxx identifies the individual dial peers for each extension. The destination pattern associated with router B is 729 555-xxxx.

Number expansion is a globally applied rule that enables you to define a set of digits for the gateway to prepend to the beginning of a dialed string before you pass it to the remote telephony device. This procedure reduces the number of digits that a user must dial to reach a remote location. Number expansion is similar to using a prefix, except that number expansion is applied globally to all dial peers and the expansion is applied before the outbound dial peer is matched. The "Sample Number Expansion Table" shows the number expansion table for the scenario shown in the figure.

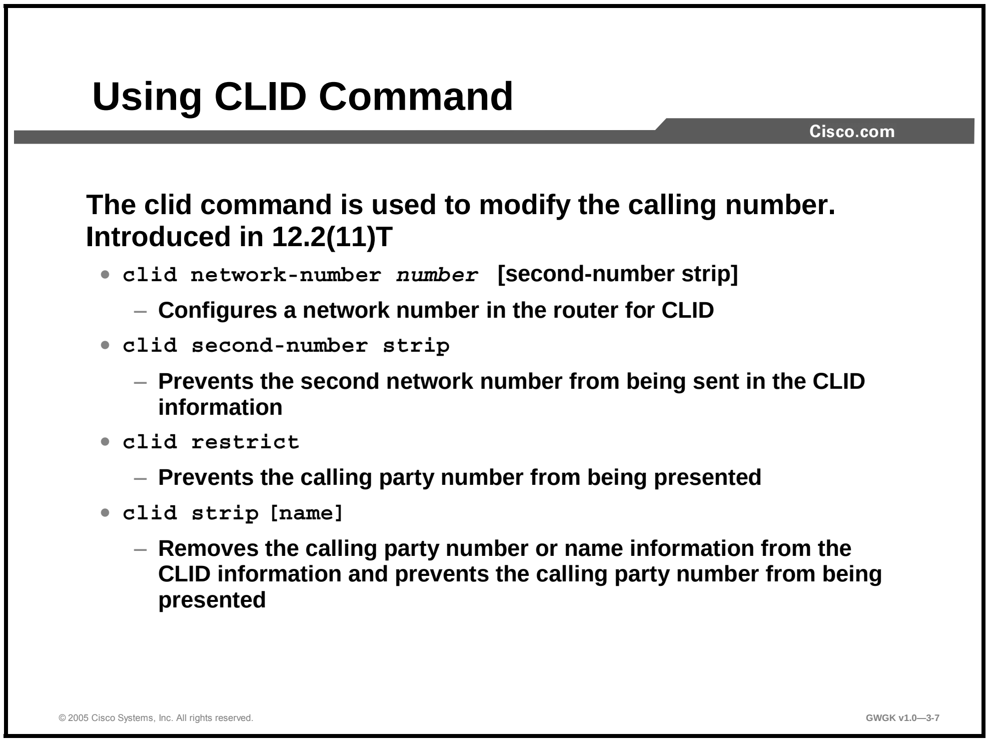
Note You must use the **show num-exp** command to view the configured number-expansion table. You must use the **show dialplan number** *number* command to confirm the presence of a valid dial peer to match the newly expanded number.

Sample Number Expansion Table

Extension	**Destination Pattern**	num-exp **Command Entry**
5....	408115....	num-exp 5.... 408115....
6....	408116....	num-exp 6.... 408116....
7....	408117....	num-exp 7.... 408117....
1....	729555....	num-exp 1... 729555....

Using CLID

This topic describes how to use calling line ID (CLID) to modify calling numbers.



Using CLID Command

Cisco.com

The clid command is used to modify the calling number. Introduced in 12.2(11)T

- `clid network-number` *`number`* **[second-number strip]**
  - **Configures a network number in the router for CLID**
- `clid second-number strip`
  - **Prevents the second network number from being sent in the CLID information**
- `clid restrict`
  - **Prevents the calling party number from being presented**
- `clid strip [name]`
  - **Removes the calling party number or name information from the CLID information and prevents the calling party number from being presented**

A Q.931 calling party number information element (IE) message is used to send the CLID information. This message can include two calling numbers: One “user provided, unscreened” and one “network provided”. The **clid** command can be used to modify the CLID information. The **clid network-number** command sets the network-provided number in the IE message and sets the presentation bit to allow the calling party number to be presented. Using the **second-number strip** option removes the user-provided number, or second number, from this IE message. It is also possible to leave the existing network number unaltered while removing the user-provided number from the IE.

The **clid restrict** command sets the presentation bit to prevent the display of the CLID information. This command does not remove the calling numbers from the IE message. It is possible to remove the numbers completely using the **clid strip** command. To remove both the calling number and the calling name, the **clid strip** command must be entered twice: Once with the name option and once without.

The **show dialplan number** *number* command can be used to determine what CLID information will be sent in an IE message.

This example shows the dial plan information with no CLID commands applied.

```
HQGW#sh dialplan number 914085551234
Macro Exp.: 914085551234
VoiceEncapPeer91
        peer type = voice, information type = voice,
        description = `',
        tag = 91, destination-pattern = `91..........',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        CLID Override RDNIS = disabled,
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-
label = `',
        numbering Type = `unknown'
```

This example shows the result of adding a **clid network-number** command to the dial peer.

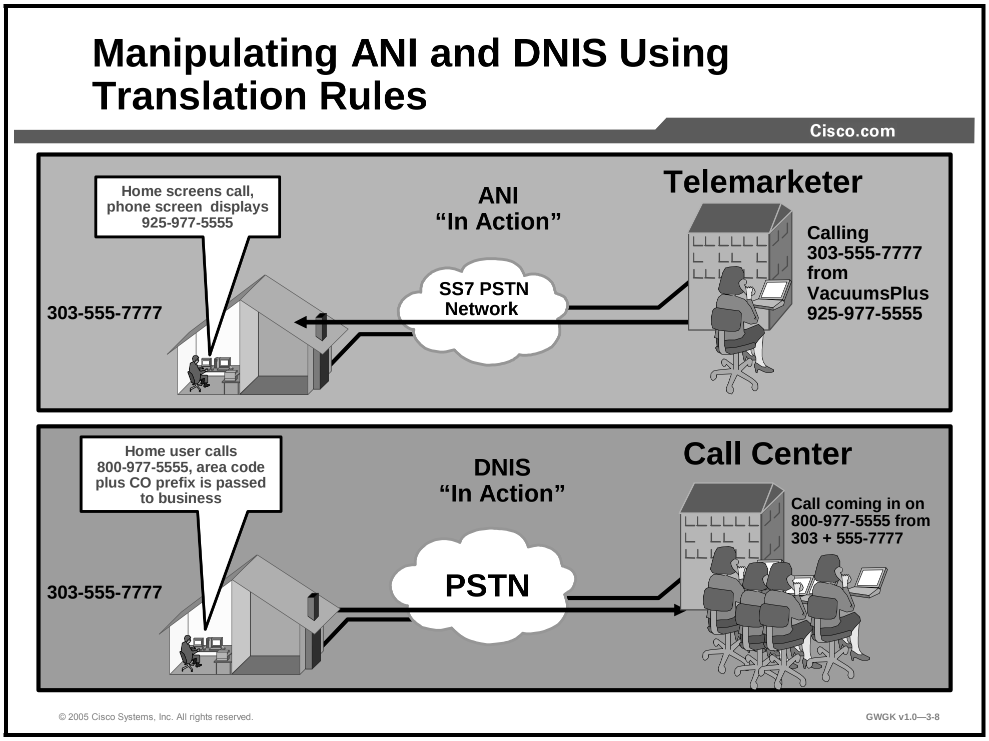
```
HQGW(config-dial-peer)#clid network-number 5551234

HQGW#show dialplan number 914085551234
Macro Exp.: 914085551234

VoiceEncapPeer91
        peer type = voice, information type = voice,
        description = `',
        tag = 91, destination-pattern = `91..........',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `5551234'
        CLID Second Number sent
        CLID Override RDNIS = disabled,
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-
label = `',
        numbering Type = `unknown'
```

This example shows the result of using the **clid restrict** command.

```
HQGW(config-dial-peer)#clid strip
HQGW#show dialplan number 914085551234
Macro Exp.: 914085551234

VoiceEncapPeer91
        peer type = voice, information type = voice,
        description = `',
        tag = 91, destination-pattern = `91..........',
        answer-address = `', preference=0,
        CLID Restriction = clid strip
        CLID Network Number = `'
        CLID Second Number sent
        CLID Override RDNIS = disabled,
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-
label = `',
        numbering Type = `unknown'
```

Manipulating ANI and DNIS

This topic describes automatic number identification (ANI) and dialed number identification service (DNIS).



Manipulating ANI and DNIS Using Translation Rules

Cisco.com

Telemarketer

ANI
“In Action”

Home screens call, phone screen displays 925-977-5555

303-555-7777

SS7 PSTN Network

Calling 303-555-7777 from VacuumsPlus 925-977-5555

Call Center

DNIS
“In Action”

Home user calls 800-977-5555, area code plus CO prefix is passed to business

303-555-7777

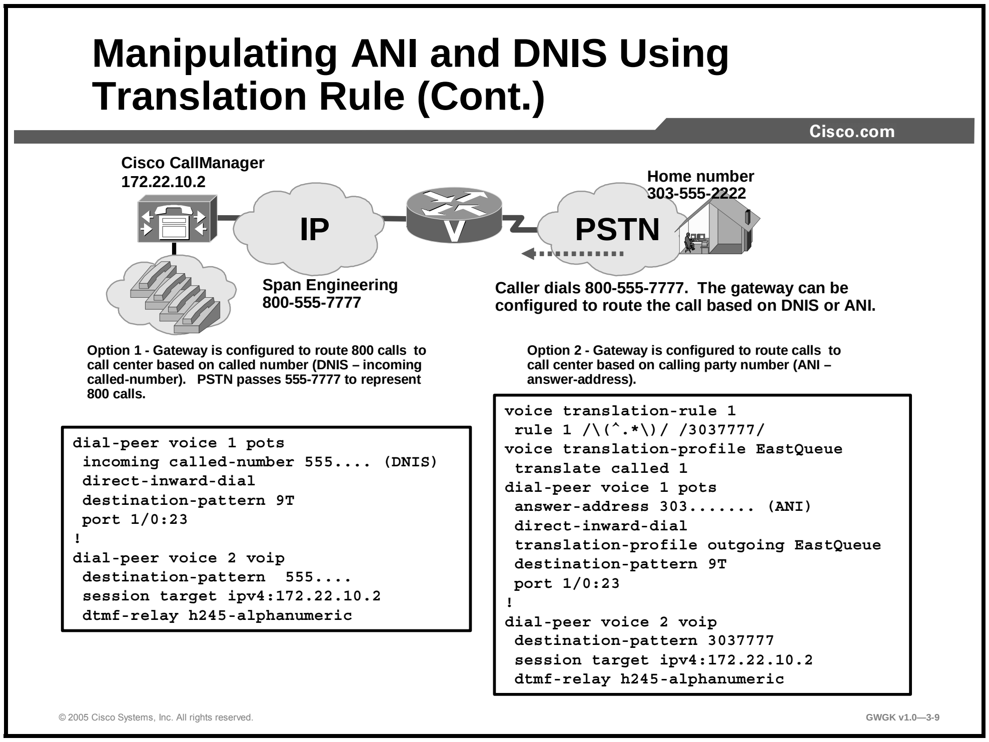
PSTN

Call coming in on 800-977-5555 from 303 + 555-7777

GWGK v1.0—3-8

ANI identifies the telephone number of the calling party. The service provider provides this information. In the example in the figure, a telemarketer calls a home number, and the resident screens the call. The resident can see where the number is coming from and can decide to answer the call or not. Another example of the use of ANI can be described from a call center environment. The ANI of an incoming call can be used to route the call to a specific queue based on the originating location of the call. Emergency call centers also use ANI to help locate callers. However, ANI only shows the number and not the caller name. Caller ID is an analog facility, typically provided to residential or business customers for an additional fee that provides both calling number (ANI) and caller name.

DNIS is a telephone service where the called number is identified. It is a common feature of toll-free services. If you have multiple toll-free numbers to the same destination, DNIS is used to route the call to the appropriate area within the destination to be answered. DNIS works by passing the touch-tone digits (DTMF or multifrequency [MF] digits) to the destination where a special facility can read and display them or make them available for call center programming. Here is an example of how a Cisco gateway would use the received DNIS digits. Suppose you have call center where customers dial 800-877-5555 for replacement parts and 800-877-7777 for service. The PSTN switch could be programmed to pass only a four-digit DNIS to the Cisco gateway. From the gateway, the call is sent to either Cisco CallManager or to a PBX where the call would route to a hunt group of agents. In this example, the Cisco gateway received 5555 and passed the digits appropriately to the hunt group for parts ordering. Basically, the call was routed to its destination by way of the DNIS digits.



Manipulating ANI and DNIS Using Translation Rule (Cont.)

Cisco.com

Cisco CallManager
172.22.10.2

Home number
303-555-2222

Span Engineering
800-555-7777

Caller dials 800-555-7777. The gateway can be configured to route the call based on DNIS or ANI.

Option 1 - Gateway is configured to route 800 calls to call center based on called number (DNIS – incoming called-number). PSTN passes 555-7777 to represent 800 calls.

```
dial-peer voice 1 pots
 incoming called-number 555.... (DNIS)
 direct-inward-dial
 destination-pattern 9T
 port 1/0:23
!
dial-peer voice 2 voip
 destination-pattern  555....
 session target ipv4:172.22.10.2
 dtmf-relay h245-alphanumeric
```

Option 2 - Gateway is configured to route calls to call center based on calling party number (ANI – answer-address).

```
voice translation-rule 1
 rule 1 /\(^.*\)/ /3037777/
voice translation-profile EastQueue
 translate called 1
dial-peer voice 1 pots
 answer-address 303....... (ANI)
 direct-inward-dial
 translation-profile outgoing EastQueue
 destination-pattern 9T
 port 1/0:23
!
dial-peer voice 2 voip
 destination-pattern 3037777
 session target ipv4:172.22.10.2
 dtmf-relay h245-alphanumeric
```

GWGK v1.0—3-9

Gateway Call Routing

The gateway can be configured to route calls based on the number that was dialed or the calling party number. In this figure, you can see two examples of how the gateway could be configured to route the voice call based on either by the 800 number that was dialed or by routing the call based on the home number of the user.

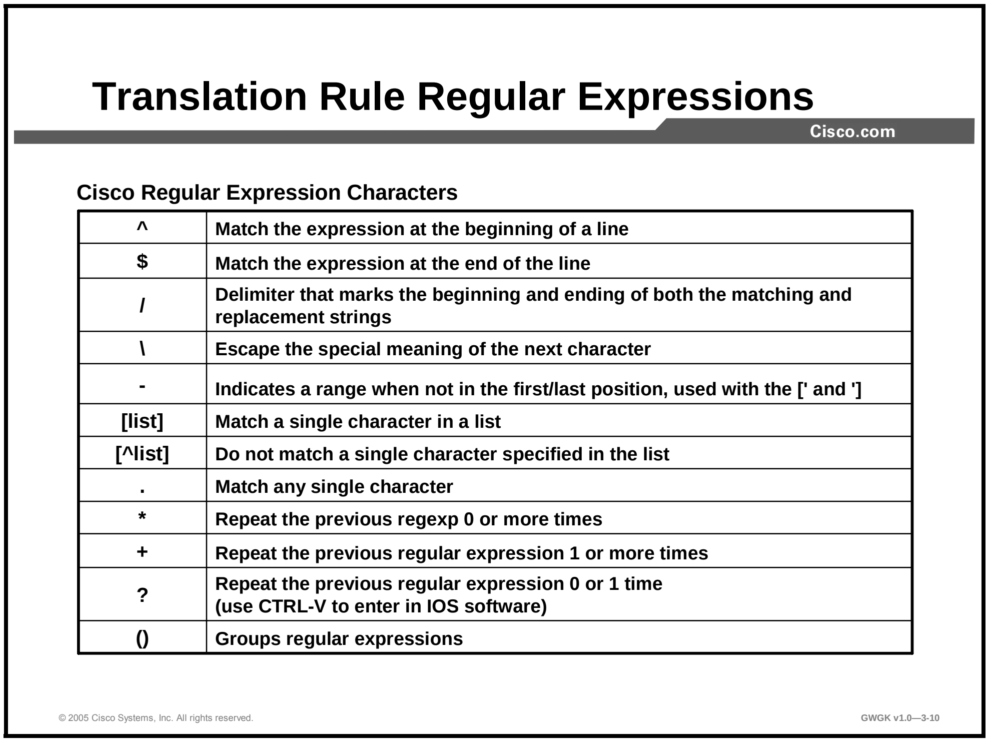
Option 1 takes the DNIS sent by the service provider and routes the call to the Cisco CallManager. The Cisco CallManager would need to be configured with a pilot number of 5557777 to place the calls in the queue.

Option 2 is used when you have different sets of agents answering calls based on where the call originated. This may be done to provide language support or to support multiple time zones. Because the service provider is still sending a DNIS of 5557777, you would use a voice translation rule to modify the DNIS so the call can be routed to a different queue.

Though not shown in the figure, the PSTN circuit would need to be configured to support ANI and DNIS. If the gateway was configured to route calls on calling party numbers and the PSTN circuit is not designed to pass the calling party number, then the gateway forwards the call based on a destination-pattern match, which could result in the call being misrouted.

Translation Rule Regular Expressions

This topic describes creating translation rule regular expressions.



Translation Rule Regular Expressions

Cisco.com

Cisco Regular Expression Characters

^	Match the expression at the beginning of a line
$	Match the expression at the end of the line
/	Delimiter that marks the beginning and ending of both the matching and replacement strings
\	Escape the special meaning of the next character
-	Indicates a range when not in the first/last position, used with the [' and ']
[list]	Match a single character in a list
[^list]	Do not match a single character specified in the list
.	Match any single character
*	Repeat the previous regexp 0 or more times
+	Repeat the previous regular expression 1 or more times
?	Repeat the previous regular expression 0 or 1 time (use CTRL-V to enter in IOS software)
()	Groups regular expressions

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—3-10

This figure shows the Cisco regular expression characters, which are the building blocks for creating powerful translation rules. Following is an example of a translation rule:

```
voice translation-rule 1
  rule 1 /^555\(....\)/ /444\1/

  rule 2 /^\(555\)\(....\)/ /444\2/
```

This is how to interpret rule 1:

- Matching Pattern /^555\(....\)/

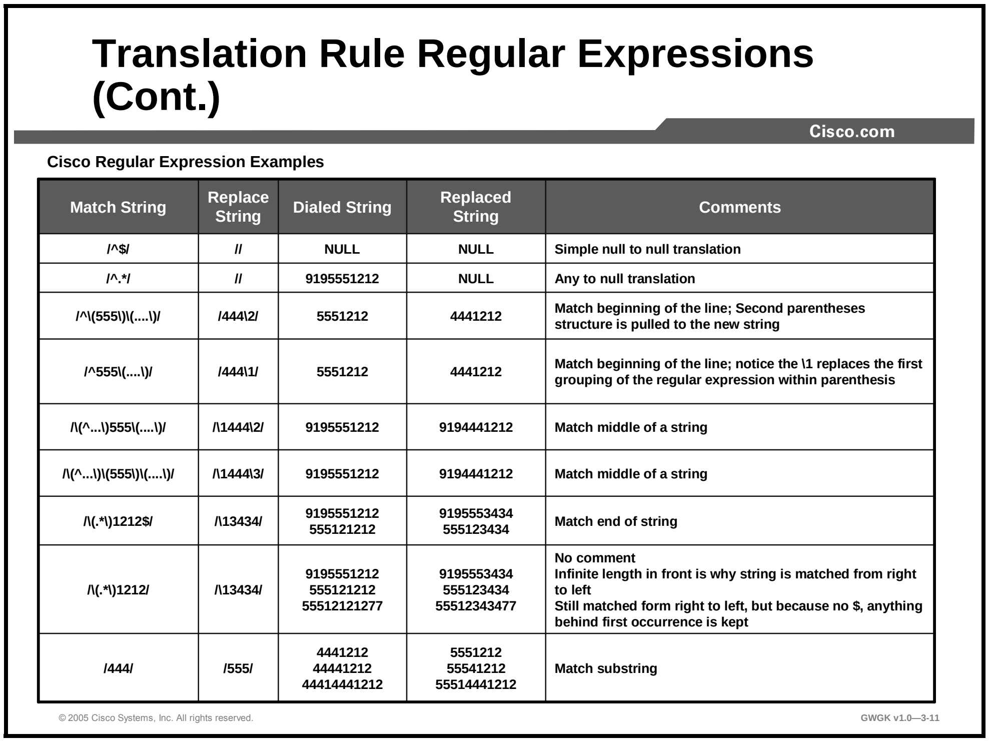
  Notice here that the parentheses are escaped out with the "\" character. If the "\" was not used, the parenthesis would be matched as part of the string instead of being used to group the expression. The parentheses are used to group portions of the expression into sets so we can manipulate it. Since the 555 is not in a set, it is ignored, and the first set consists of the four digits following 555.

- Replacement Pattern /444\1/

  This replacement pattern makes the new string start with 444 and then appends (\1). The \1 means that you take the first set from the matching pattern and put it here. For this replacement, the number will look like "444...."

If the dialed string was 5551212, then the replacement string would be 4441212.

Rule 2 is functionally equivalent to rule 1. The matching pattern in rule 2 is divided into two sets. The first set is 555 and the second set is the four digits following the 555. The replacement pattern starts with 444 and then appends the \2, which adds the second set from the matching pattern.



Translation Rule Regular Expressions (Cont.)

Cisco.com

Cisco Regular Expression Examples

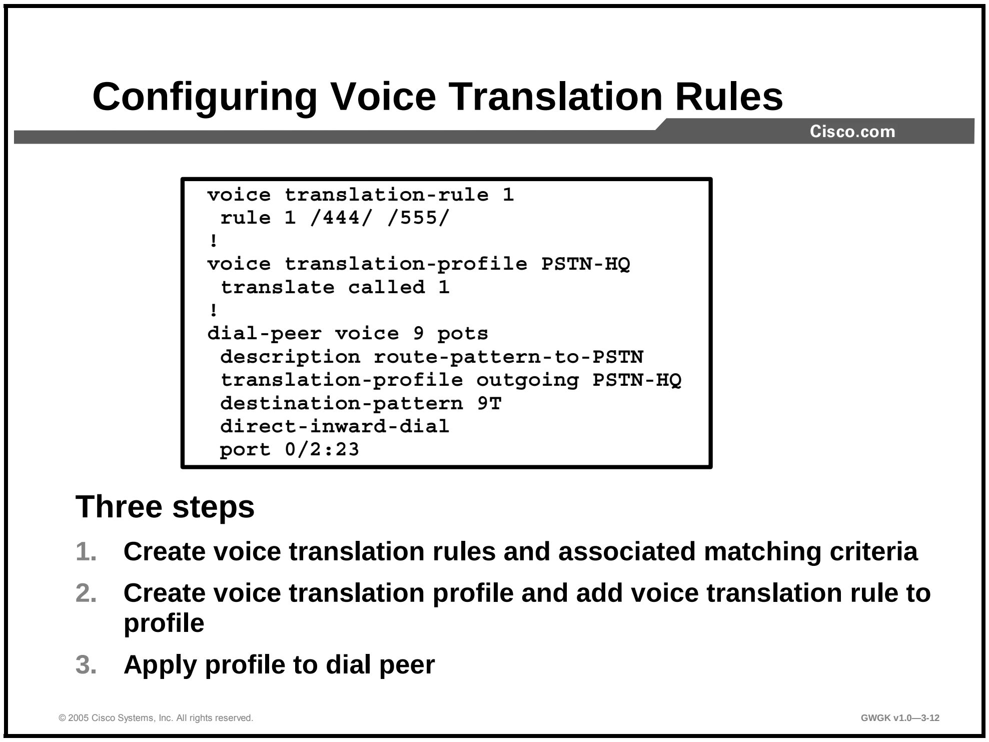
Match String	Replace String	Dialed String	Replaced String	Comments
/^$/	//	NULL	NULL	Simple null to null translation
/^.*/	//	9195551212	NULL	Any to null translation
/^\(555\)\(....\)/	/444\2/	5551212	4441212	Match beginning of the line; Second parentheses structure is pulled to the new string
/^555\(....\)/	/444\1/	5551212	4441212	Match beginning of the line; notice the \1 replaces the first grouping of the regular expression within parenthesis
/\(^...\)555\(....\)/	/\1444\2/	9195551212	9194441212	Match middle of a string
/\(^...\)\(555\)\(....\)/	/\1444\3/	9195551212	9194441212	Match middle of a string
/\(.*\)1212$/	/\13434/	9195551212 555121212	9195553434 555123434	Match end of string
/\(.*\)1212/	/\13434/	9195551212 555121212 55512121277	9195553434 555123434 55512343477	No comment Infinite length in front is why string is matched from right to left Still matched form right to left, but because no $, anything behind first occurrence is kept
/444/	/555/	4441212 44441212 44414441212	5551212 55541212 55514441212	Match substring

GWGK v1.0—3-11

This figure shows how to use the regular expressions to build your own translation rules. This is not an exhaustive list and is only presented to provide insight to how the expressions can be used.

Configuring Translation Rules

This topic describes how to configure translation rules.



Configuring Voice Translation Rules

Cisco.com

```
voice translation-rule 1
 rule 1 /444/ /555/
!
voice translation-profile PSTN-HQ
 translate called 1
!
dial-peer voice 9 pots
 description route-pattern-to-PSTN
 translation-profile outgoing PSTN-HQ
 destination-pattern 9T
 direct-inward-dial
 port 0/2:23
```

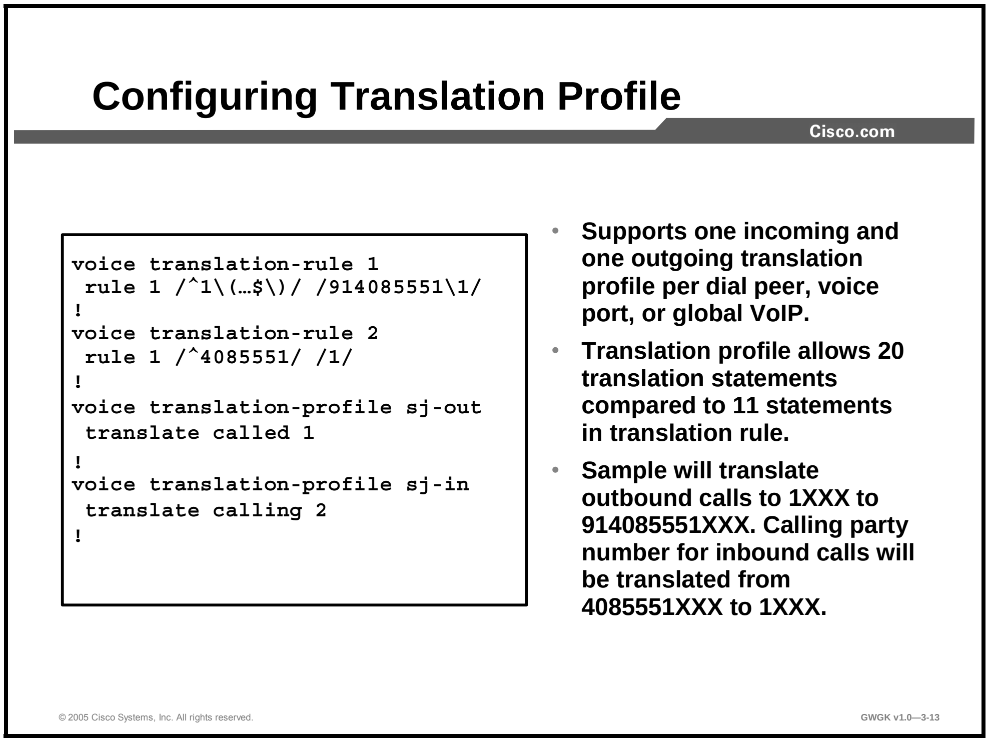
Three steps

1. **Create voice translation rules and associated matching criteria**
2. **Create voice translation profile and add voice translation rule to profile**
3. **Apply profile to dial peer**

GWGK v1.0—3-12

There are three steps involved in configuring voice translation rules:

- Create voice translation rules and their associated matching criteria
- Create voice a voice translation profile and add the voice translation rule to the profile
- Apply the profile to the dial peer



Configuring Translation Profile

Cisco.com

```
voice translation-rule 1
 rule 1 /^1\(…$\)/ /914085551\1/
!
voice translation-rule 2
 rule 1 /^4085551/ /1/
!
voice translation-profile sj-out
 translate called 1
!
voice translation-profile sj-in
 translate calling 2
!
```

- **Supports one incoming and one outgoing translation profile per dial peer, voice port, or global VoIP.**
- **Translation profile allows 20 translation statements compared to 11 statements in translation rule.**
- **Sample will translate outbound calls to 1XXX to 914085551XXX. Calling party number for inbound calls will be translated from 4085551XXX to 1XXX.**

GWGK v1.0—3-13

Translation profiles are used to scale translation rules. After defining the voice translation rule and applying the rule in a profile, you then apply the profile to a dial peer or voice port, or to both in some cases. Applying the translation profile in these three situations is described here:

- Dial peer
  - — The dial peer can have two different translation profiles, one for incoming calls and one for outgoing calls.
- Voice port
  - — A voice port can have a translation profile for incoming POTS calls. If the voice port is a member of a trunk group, the incoming translation profile of the voice port overrides the translation profile of the trunk group.
  - — A voice port can have a translation profile for outgoing POTS calls. If the voice port is a member trunk group, the outgoing translation profile of the voice port overrides the translation profile of the trunk group.
- VoIP incoming translation profile
  - — A global translation profile can be defined to translate all incoming VoIP calls by using the **voip-incoming translation-profile** command.
- Incoming call blocking

  The only option for call blocking is in the incoming direction. From the perspective of the gateway, the incoming direction can be either of the following:

  - — Incoming from a telephony device directly attached to a voice port on the gateway toward the gateway itself
  - — Incoming by the way of an inbound VoIP call from a peer gateway

The following is a call blocking configuration example:

1. To configure call blocking, define a translation rule with a **reject** keyword.

```
voice translation-rule 1
rule 1 reject /408252*/
```

2. Apply the rule to a translation profile for called, calling, or redirect-called numbers.

```
voice translation profile call_block_profile
  translate calling 1
```

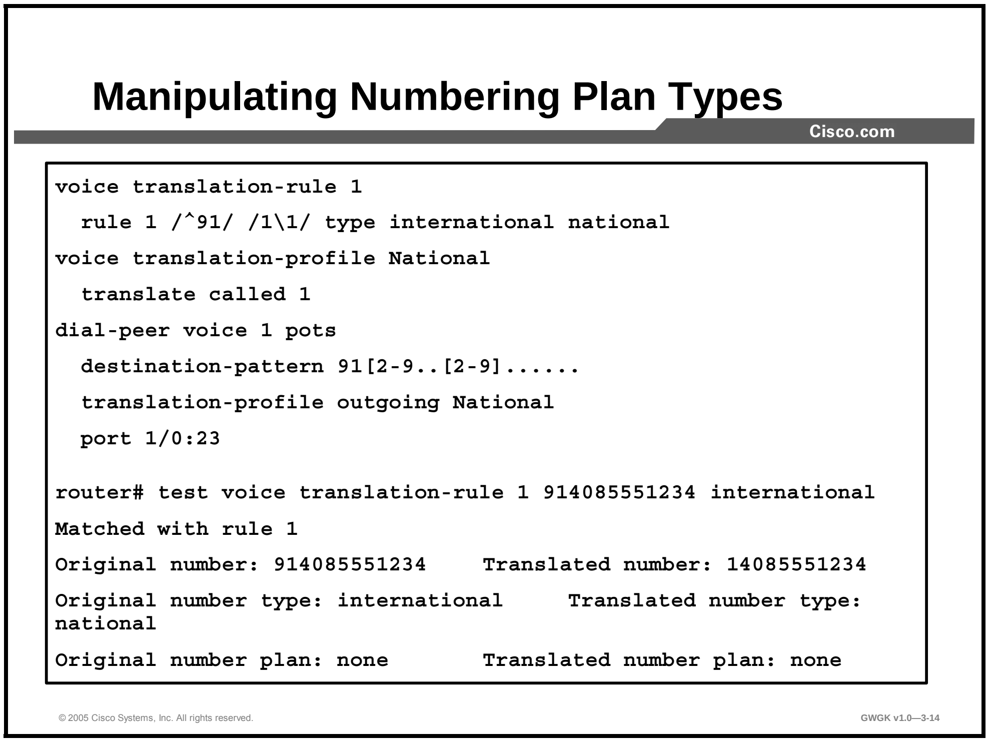
3. Include the translation profile within a dial peer definition.

```
Dial-peer voice 111 POTS
Call-block translation-profile incoming call_block_profile
Call-block disconnect-cause incoming invalid_number
```

In the call blocking example, the gateway blocks any incoming time-division multiplexing (TDM) call that successfully matches inbound dial peer 111 and has a calling number that starts with 408252. A component of the call block command is the ability to return a disconnect cause. These values include call-reject, invalid-number, unassigned-number, and user-busy. When dial peer 111 matches a dialed string starting with 408252, it will reject the call and return a disconnect cause of “invalid number” to the source of the call.

Manipulating Numbering Plan Types

This topic describes how to manipulate numbering plan types.



Manipulating Numbering Plan Types

Cisco.com

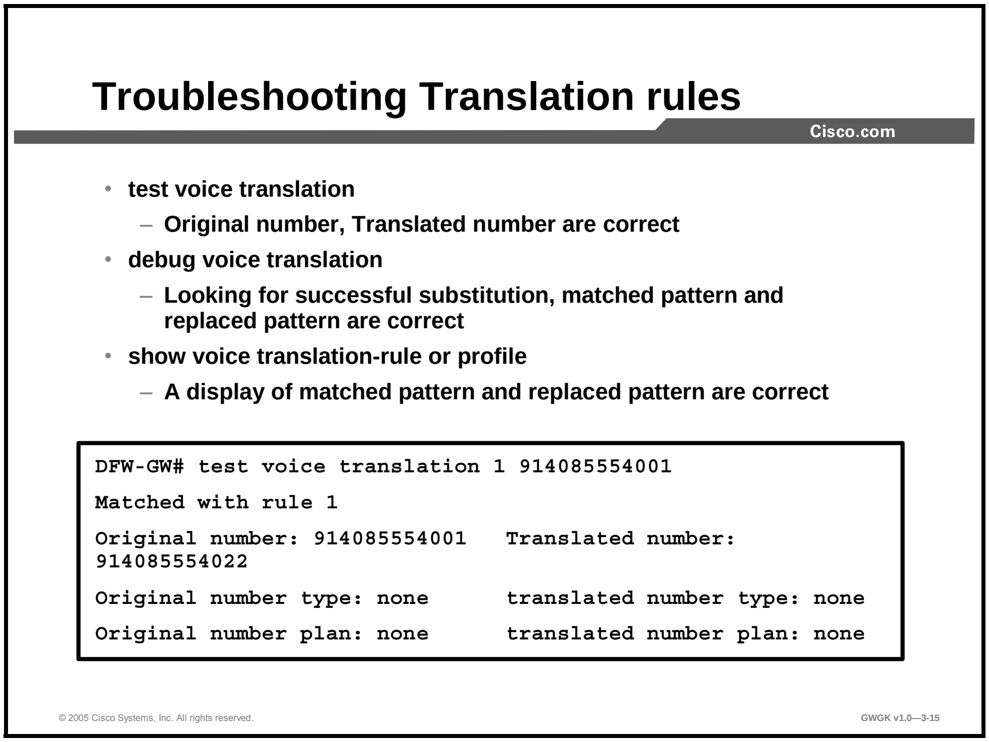
```
voice translation-rule 1
  rule 1 /^91/ /1\1/ type international national
voice translation-profile National
  translate called 1
dial-peer voice 1 pots
  destination-pattern 91[2-9..[2-9]......
  translation-profile outgoing National
  port 1/0:23

router# test voice translation-rule 1 914085551234 international
Matched with rule 1
Original number: 914085551234    Translated number: 14085551234
Original number type: international     Translated number type:
national
Original number plan: none       Translated number plan: none
```

GWGK v1.0—3-14

Translation rules can also be used to change the numbering type for a call. For example, some gateways may tag any number with more than 11 digits as an international number, even when the user must dial a 9 to reach an outside line. The example in the figure shows a translation rule that converts any called number that starts with 91 and that is tagged as an international number into a national number without the 9 before it sends it to the PSTN.

Troubleshooting Translation Rules

This topic describes how to troubleshoot translation rules.



Troubleshooting Translation rules

Cisco.com

- **test voice translation**
  - **Original number, Translated number are correct**
- **debug voice translation**
  - **Looking for successful substitution, matched pattern and replaced pattern are correct**
- **show voice translation-rule or profile**
  - **A display of matched pattern and replaced pattern are correct**

```
DFW-GW# test voice translation 1 914085554001
Matched with rule 1
Original number: 914085554001   Translated number:
914085554022
Original number type: none      translated number type: none
Original number plan: none      translated number plan: none
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—3-15

Use the t**est voice translation-rule** command when you are troubleshooting translation profiles and rules. The **debug voice translation** command is another useful tool.

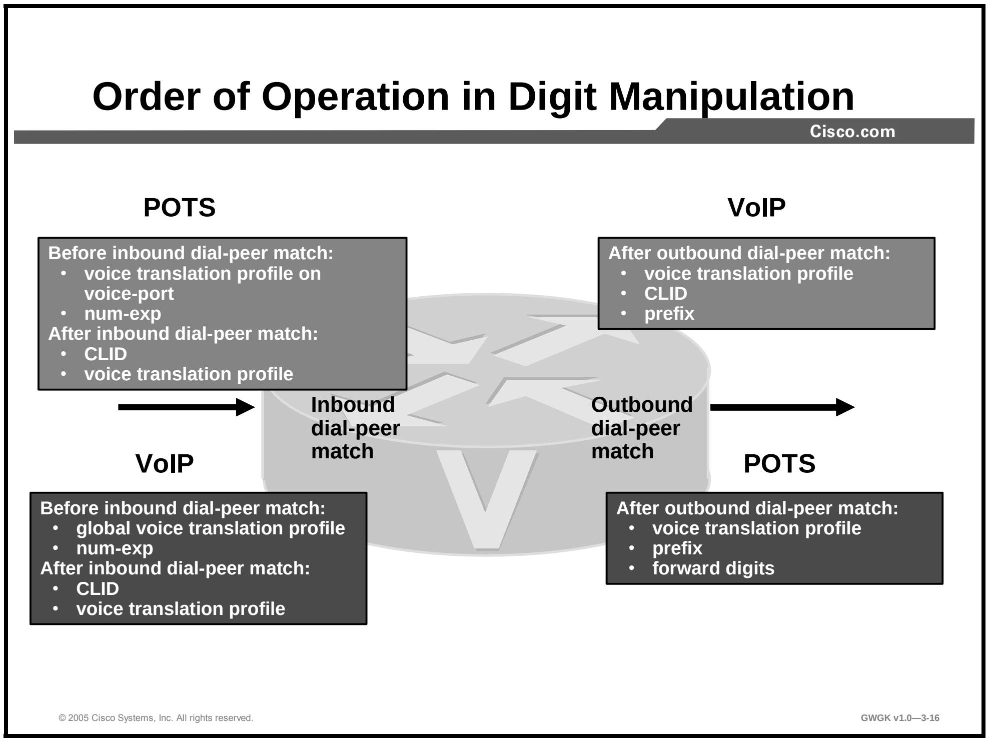
The following are examples of other show commands that can be used to troubleshoot problems with translation profiles and rules.

```
DFW-GW# test voice translation 1 914085554001
Matched with rule 1
Original number: 914085554001   Translated number:
914085554022
Original number type: none      translated number type: none
Original number plan: none      translated number plan: none


DFW-GW# debug voice translation
*Apr 25 19:40:47.507: //-1/xxxxxxxxxxxx/RXRULE/sed_subst:
Successful substitution; pattern=914085554001
matchPattern=4001 replacePattern=4022 replaced
pattern=914085554022
*Apr 25 19:40:47.507: //-
1/xxxxxxxxxxxx/RXRULE/regxrule_subst_num_type: Match Type =
none, Replace Type = none Input Type = none
*Apr 25 19:40:47.511: //-
1/xxxxxxxxxxxx/RXRULE/regxrule_subst_num_plan: Match Plan =
none, Replace Plan = none Input Plan = none
```

```
DFW-GW# show voice translation-rule 1
Translation-rule tag: 1

        Rule 1:
        Match pattern: 4001
        Replace pattern: 4022
        Match type: none                Replace type: none
        Match plan: none                Replace plan: none
```

Order of Operation in Digit Manipulation

This topic describes the order of operation in digit manipulation.



Order of Operation in Digit Manipulation

Cisco.com

POTS

Before inbound dial-peer match:
- voice translation profile on voice-port
- num-exp

After inbound dial-peer match:
- CLID
- voice translation profile

VoIP

After outbound dial-peer match:
- voice translation profile
- CLID
- prefix

VoIP

Before inbound dial-peer match:
- global voice translation profile
- num-exp

After inbound dial-peer match:
- CLID
- voice translation profile

POTS

After outbound dial-peer match:
- voice translation profile
- prefix
- forward digits

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—3-16

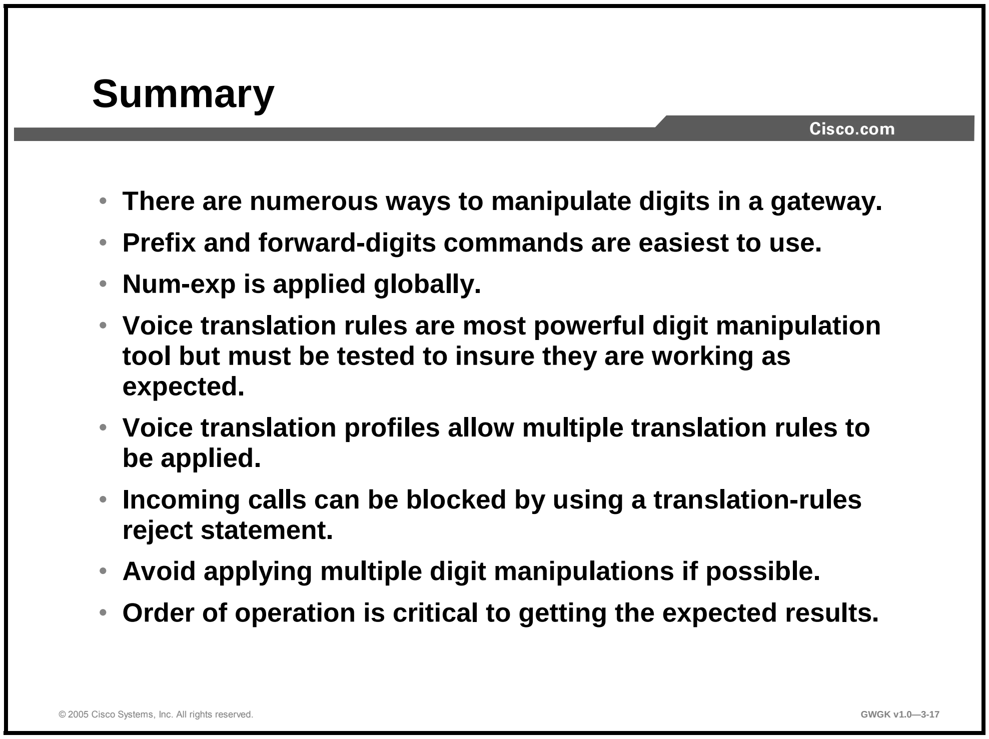
The order of operation in digit manipulation follows the call through the gateway. For inbound POTS calls, rules configured on the voice port are applied first, followed by the incoming dial peer and then the outgoing dial peer. For inbound VoIP calls, global voice translation profiles are applied first, followed by the incoming dial peer and then the outgoing dial peer. Note that the **num-exp** command is applied globally before any dial-peer matching.

It is recommended that, when possible, you use a single method of accomplishing the required digit manipulations. For example, do not use the **forward-digits** and the **prefix** commands in a dial peer configuration.

It is possible to use all of the digit manipulation methods in a gateway. A single dial peer can be configured with prefixes, voice translation rules, and CLID commands. A call can be modified by the voice port, number expansion, inbound dial peer, and outbound dial peer configuration commands in a single or multiple gateway. Understanding the order of operation in digit manipulation is important not only for configuration and test purposes but also for assisting in troubleshooting.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

Cisco.com

- There are numerous ways to manipulate digits in a gateway.
- Prefix and forward-digits commands are easiest to use.
- Num-exp is applied globally.
- Voice translation rules are most powerful digit manipulation tool but must be tested to insure they are working as expected.
- Voice translation profiles allow multiple translation rules to be applied.
- Incoming calls can be blocked by using a translation-rules reject statement.
- Avoid applying multiple digit manipulations if possible.
- Order of operation is critical to getting the expected results.

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—3-17

References

For additional information, refer to these resources:

- VoIP Gateway Trunk and Carrier Based Routing Enhancements:
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00800b5dbf.html#wp1032356
- Configuring Dial Plans, Dial Peers, and Digit Manipulation:
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a0080080aec.html
- Technical Support for Call Routing and Dial Plans:
  http://www.cisco.com/pcgi-bin/Support/browse/psp_view.pl?p=Technologies:Voice_Call_Routing_Dial_Plans&viewall=true
- Voice Translation Rule:
  http://www.cisco.com/en/US/tech/tk652/tk90/technologies_tech_note09186a0080325e8e.shtml

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) What do the **prefix** and **forward-digits** commands have in common? (Source:)

A) dial-peer matching occurs after an outbound peer is matched
B) dial-peer matching occurs after an inbound peer is matched
C) dial-peer matching occurs before the actual digits are sent out
D) dial-peer matching occurs before an outbound match

Q2) The task of adding or subtracting digits from a number to meet dial plan or gateway requirements defines which of the following terms? (Source:)

A) voice translation rules
B) the prefix command
C) number expansion
D) digit manipulation

Q3) Matching inbound and outbound dial peers is based on the perspective of which device? (Source:)

____

Q4) Inbound VoIP dial peers are associated with the incoming VoIP call leg of which device? (Source:)

____

Q5) Which element does the gateway use first when it attempts to match the calling number in the call setup request? (Source: Matching Inbound and Outbound Digits)

A) destination pattern
B) answer address
C) incoming called number
D) voice port

Q6) Which of the following statements describe CLID? (Choose two.) (Source:)

A) CLID can be used to send the main number of a company on outbound calls.
B) CLID sends caller ID information.
C) The CLID is the telephone number of the phone from which a call originates.
D) You can not restrict the calling number by inserting the **clid restrict** command.

Lesson Self-Check Answer Key

Q1)	A
Q2)	D
Q3)	Originating gateway
Q4)	Terminating gateway
Q5)	C
Q6)	A, C

Lesson 3

Class of Restrictions

Overview

Class of Restrictions (COR) is a Cisco voice gateway feature that enables class of service (CoS) or calling privileges to be assigned. It is most commonly used with Cisco Survivable Remote Site Telephony (SRST) and Cisco CallManager Express but can be applied to any dial peer. This feature is similar to the Cisco CallManager calling search spaces and partitions options and allows you to maintain control of calling patterns when the Cisco CallManager is not available or when Cisco CallManager Express is deployed. In this lesson, you will discover the power behind this technology and its ease of implementation. The lesson includes various configuration examples for your review. These examples should assist in your own deployment of COR within a Cisco SRST and Cisco CallManager Express environment.

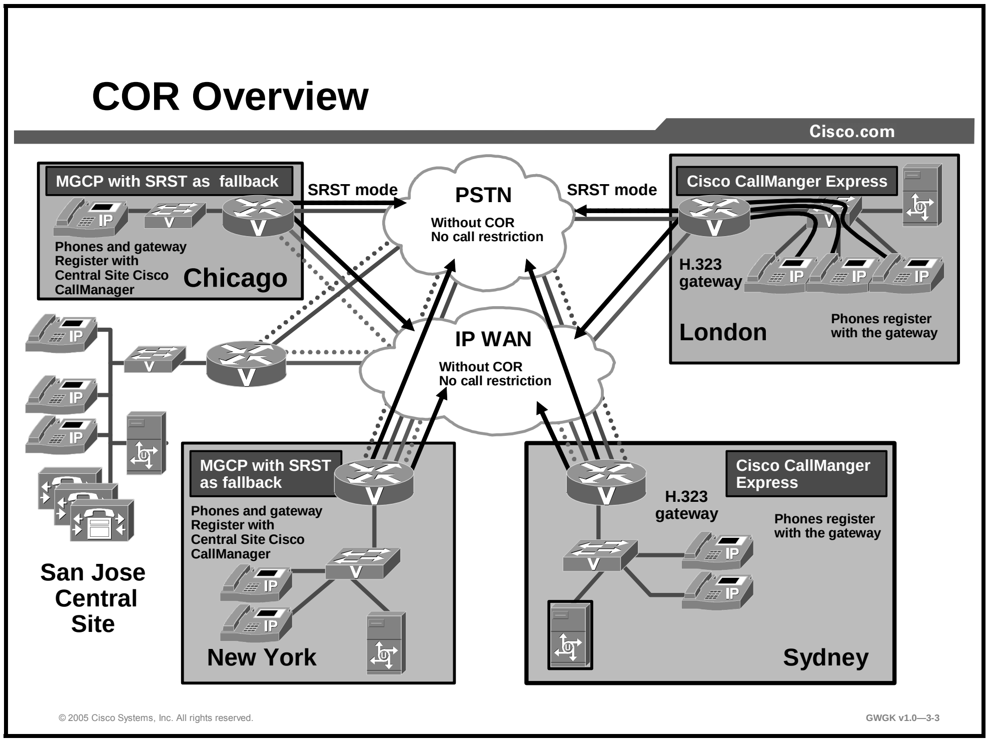
Objectives

Upon completing this lesson, you will be able to identify where in the gateway COR is applied and describe the configuration and verifications steps. This ability includes being able to meet these objectives:

- Describe why COR would be used
- Describe the components and operation of COR
- Compare and contrast COR with Cisco CallManager calling search spaces and partitions options
- Configure COR
- Use specific commands to verify COR on a network

COR Overview

This topic provides an overview of COR, its uses, and its functionality.



COR Overview

Cisco.com
MGCP with SRST as fallback
Phones and gateway Register with Central Site Cisco CallManager
Chicago
SRST mode
PSTN
Without COR
No call restriction
SRST mode
Cisco CallManger Express
H.323 gateway
London
Phones register with the gateway
IP WAN
Without COR
No call restriction
San Jose Central Site
MGCP with SRST as fallback
Phones and gateway Register with Central Site Cisco CallManager
New York
Cisco CallManger Express
H.323 gateway
Phones register with the gateway
Sydney
IP
V

GWGK v1.0—3-3

The figure shows a scenario in which COR could be used. Chicago and New York are Media Gateway Control Protocol (MGCP) sites with SRST as a backup. The gateways at these sites, along with their IP phones, are registered with the Cisco CallManager at the central site. Conversely, the London and Sydney sites use Cisco CallManager Express. Cisco CallManager Express gateways are Cisco IOS software-based H.323 gateways. The Cisco CallManager Express sites have their IP phones registered to their gateways and not to the Cisco CallManager at the central site.

In normal conditions, the MGCP site devices use the calling search space and partitions provided by Cisco CallManager at the central site. The Cisco CallManager Express sites and their devices do not use the calling search space and partitions at the central site.

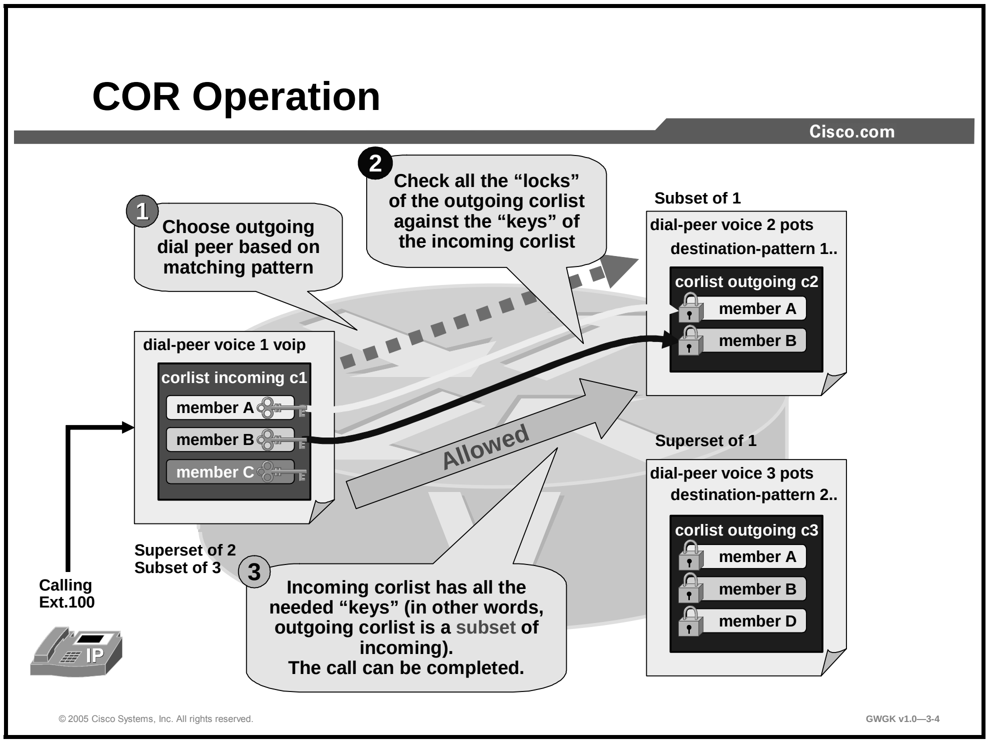
There are two potential problems to this configuration:

- One is when users at the MGCP lose communication with the Cisco CallManager at the central site and fall back to SRST mode. Without the central site CallManager managing their calling behavior, users can potentially have unlimited access to the PSTN.
- The other exists at the Cisco CallManager Express. The IP phones do not fall under the control of the Cisco CallManager but are managed by the Cisco CallManager Express gateway. Without any call behavior management at these sites, users can potentially have unlimited access to the PSTN, also.

COR can be used on Cisco IOS voice gateways for blocking or permitting a certain list of numbers based on incoming and outgoing dial-peer COR lists. Using COR, certain sets of subscribers can be blocked from making calls to other sets of subscribers and vice versa. This concept can be extended to enable a certain series of numbers (for example, 900 numbers) to be blocked from all or some sets of subscribers. Applications such as these are made possible by including incoming or outgoing COR lists, or both, on the dial plans in the gateways.

COR Operation

This topic describes COR operation and logic.



COR Operation

Cisco.com

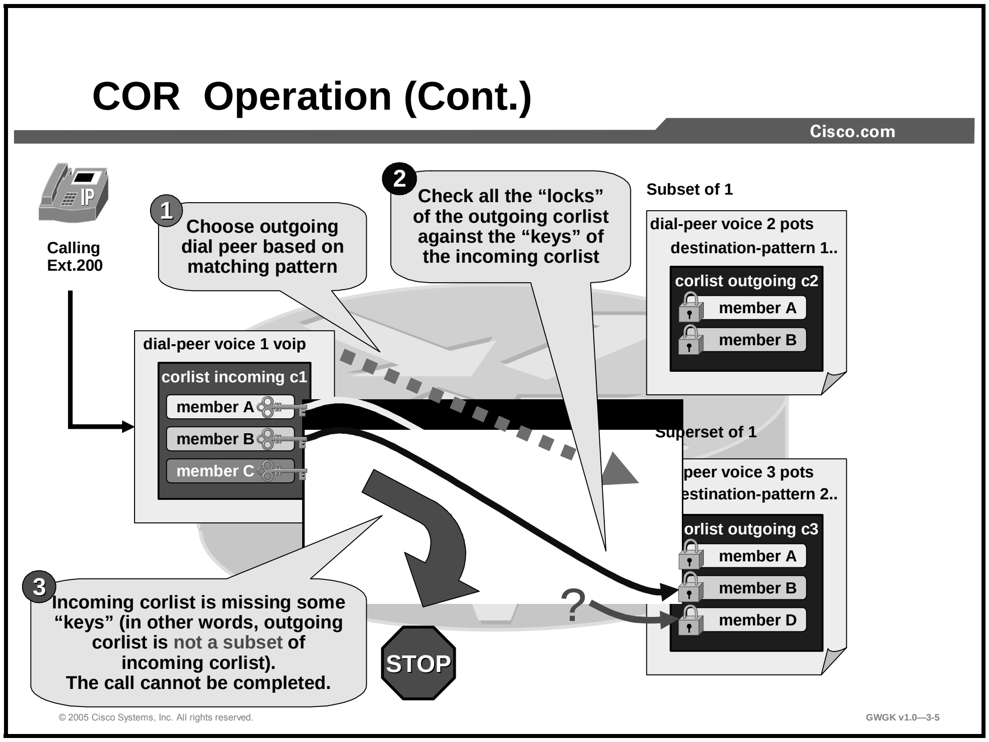
1 Choose outgoing dial peer based on matching pattern

2 Check all the "locks" of the outgoing corlist against the "keys" of the incoming corlist

3 Incoming corlist has all the needed "keys" (in other words, outgoing corlist is a subset of incoming). The call can be completed.

GWGK v1.0—3-4

This figure shows how dial peers are matched when COR is configured. This configuration applies to both Cisco SRST and to Cisco CallManager Express. For a call restriction to operate, the outgoing dial peer must be a subset of the incoming dial peer.



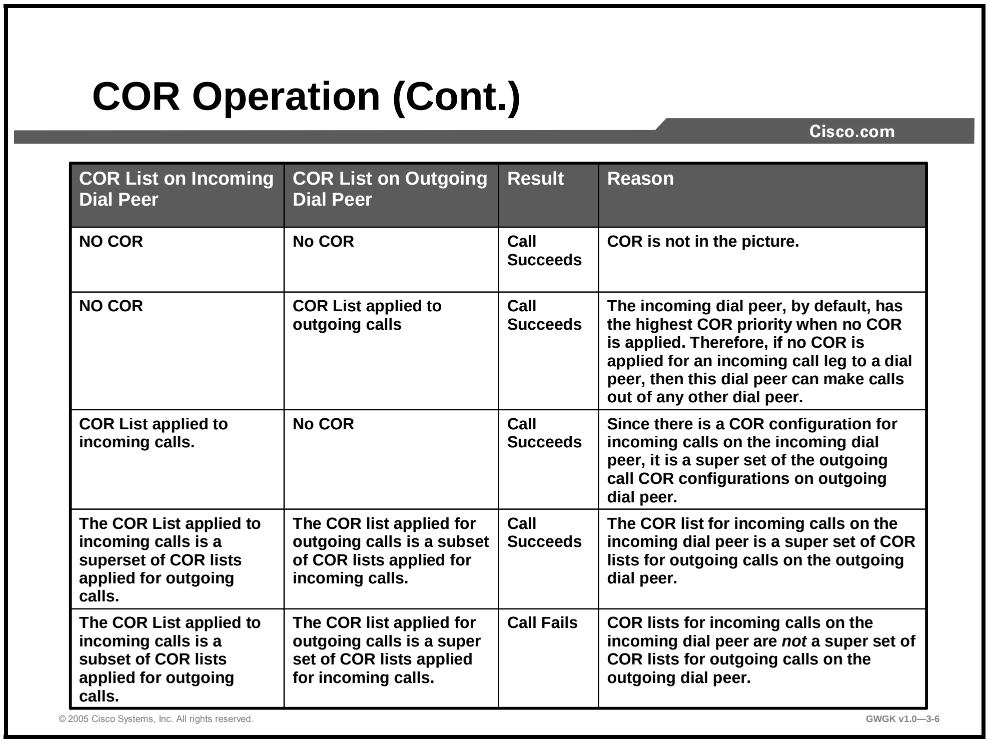
COR Operation (Cont.)

1 Choose outgoing dial peer based on matching pattern

2 Check all the “locks” of the outgoing corlist against the “keys” of the incoming corlist

3 Incoming corlist is missing some “keys” (in other words, outgoing corlist is not a subset of incoming corlist).
The call cannot be completed.

In this figure, plain old telephone service (POTS) dial peer 3 is not a subset of VoIP dial peer 1, and thus the call will not be allowed.



COR Operation (Cont.)

Cisco.com

COR List on Incoming Dial Peer	COR List on Outgoing Dial Peer	Result	Reason
NO COR	No COR	Call Succeeds	COR is not in the picture.
NO COR	COR List applied to outgoing calls	Call Succeeds	The incoming dial peer, by default, has the highest COR priority when no COR is applied. Therefore, if no COR is applied for an incoming call leg to a dial peer, then this dial peer can make calls out of any other dial peer.
COR List applied to incoming calls.	No COR	Call Succeeds	Since there is a COR configuration for incoming calls on the incoming dial peer, it is a super set of the outgoing call COR configurations on outgoing dial peer.
The COR List applied to incoming calls is a superset of COR lists applied for outgoing calls.	The COR list applied for outgoing calls is a subset of COR lists applied for incoming calls.	Call Succeeds	The COR list for incoming calls on the incoming dial peer is a super set of COR lists for outgoing calls on the outgoing dial peer.
The COR List applied to incoming calls is a subset of COR lists applied for outgoing calls.	The COR list applied for outgoing calls is a super set of COR lists applied for incoming calls.	Call Fails	COR lists for incoming calls on the incoming dial peer are *not* a super set of COR lists for outgoing calls on the outgoing dial peer.

GWGK v1.0—3-6

COR is used to specify which incoming dial peer can use which outgoing dial peer to make a call. Each dial peer can be provisioned with an incoming and an outgoing COR list. The **corlist** command sets the dial peer COR parameter for dial peers and sets the directory numbers that are created for Cisco IP phones associated with the Cisco CallManager Express or the Cisco SRST router. COR functionality provides the ability to deny certain call attempts on the basis of the incoming and outgoing COR lists that are provisioned on the dial peers. This functionality provides flexibility in network design, allows users to block calls (for example, calls to 900 numbers), and applies different restrictions to call attempts from different originators.

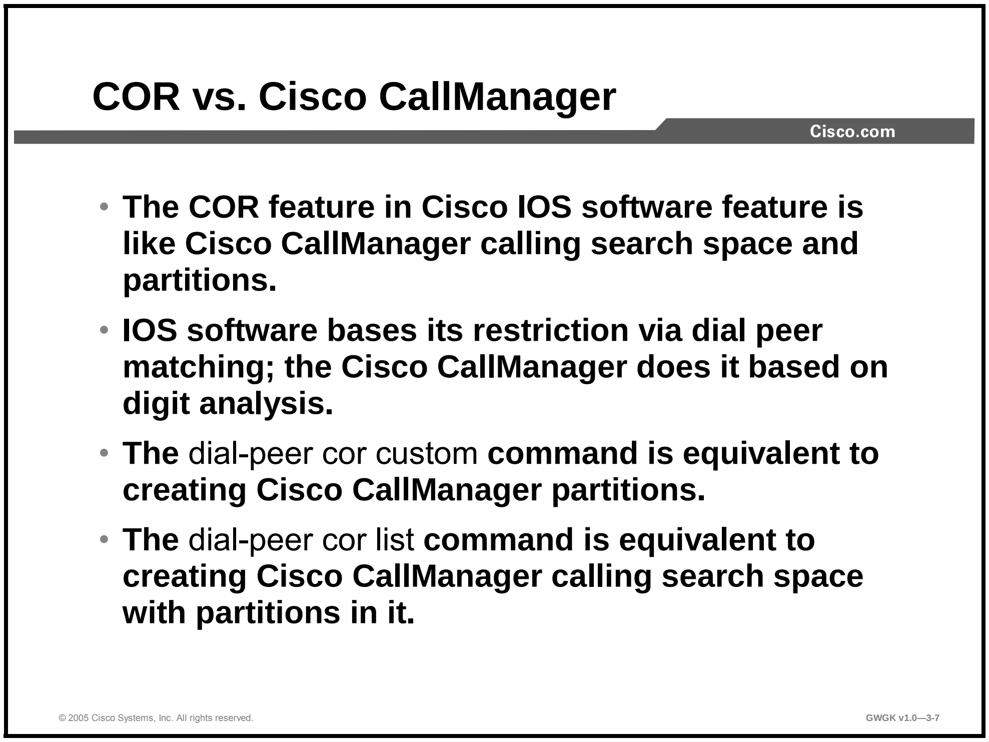
The figure shows how a call will proceed when COR is applied. If a COR is applied on an incoming dial peer (for incoming calls) and it is a superset of or is equal to the COR applied to the outgoing dial peer (for outgoing calls), the call will go through.

Voice ports determine whether a call is considered incoming or outgoing. For example, if you hook up a phone to a Foreign Exchange Station (FXS) port on a Cisco SRST router and try to make a call from that phone, the call will be considered an incoming call to the router and voice port. If you make a call to the FXS phone, the call will be considered outgoing.

By default, an incoming call leg has the highest COR priority, and the outgoing call leg has the lowest priority. If there is no COR configuration for incoming calls on a dial peer, you can make a call from a phone attached to the dial peer so that the call will go out of any dial peer regardless of the outgoing COR configuration on that dial peer. The figure describes call functionality based on how the COR lists are configured.

COR vs. Cisco CallManager

This topic describes COR versus Cisco CallManager.



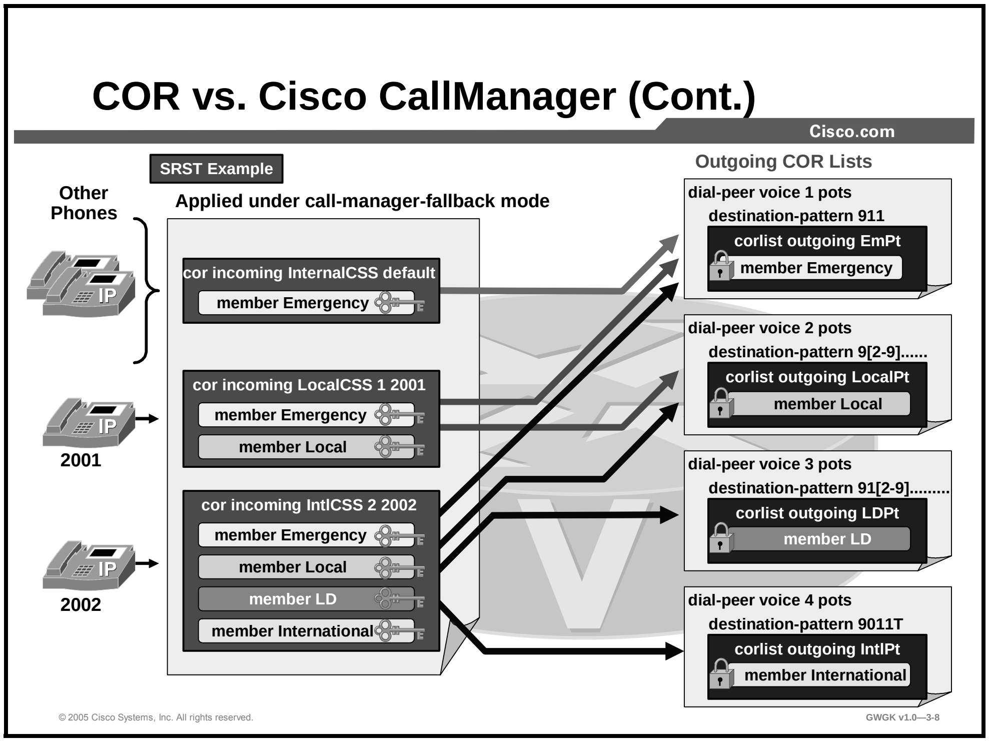
COR vs. Cisco CallManager

Cisco.com

- **The COR feature in Cisco IOS software feature is like Cisco CallManager calling search space and partitions.**
- **IOS software bases its restriction via dial peer matching; the Cisco CallManager does it based on digit analysis.**
- **The** dial-peer cor custom **command is equivalent to creating Cisco CallManager partitions.**
- **The** dial-peer cor list **command is equivalent to creating Cisco CallManager calling search space with partitions in it.**

GWGK v1.0—3-7

Partitions and calling search spaces provide the capability for implementing calling restrictions and creating closed dial plan groups on the same Cisco CallManager. There are resemblances between the COR operation and the Cisco CallManager calling search spaces and partitions feature. The one thing that COR cannot do is separate line and device calling search spaces and partitions like Cisco CallManager can.



COR vs. Cisco CallManager (Cont.)

Cisco.com

SRST Example

Applied under call-manager-fallback mode

Other Phones

2001

2002

cor incoming InternalCSS default
member Emergency

cor incoming LocalCSS 1 2001
member Emergency
member Local

cor incoming IntlCSS 2 2002
member Emergency
member Local
member LD
member International

Outgoing COR Lists

dial-peer voice 1 pots
destination-pattern 911
corlist outgoing EmPt
member Emergency

dial-peer voice 2 pots
destination-pattern 9[2-9]......
corlist outgoing LocalPt
member Local

dial-peer voice 3 pots
destination-pattern 91[2-9].........
corlist outgoing LDPt
member LD

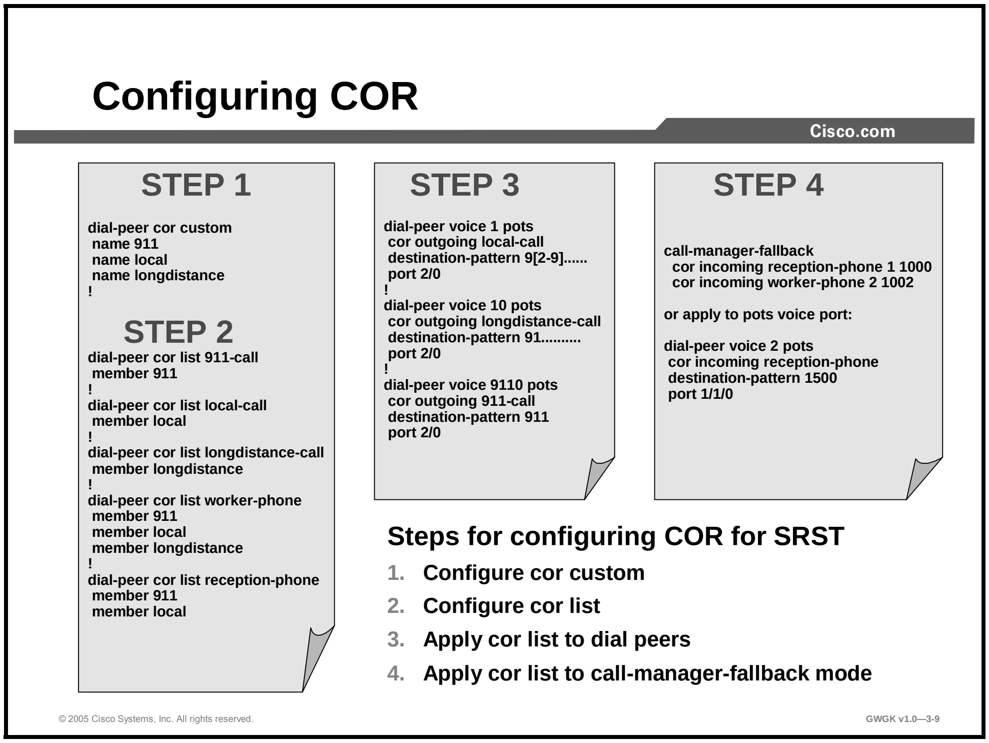
dial-peer voice 4 pots
destination-pattern 9011T
corlist outgoing IntlPt
member International

GWGK v1.0—3-8

To apply COR with Cisco SRST phones, COR is applied under the **call-manager-fallback** configuration mode. With Cisco CallManager Express, you apply COR to the phone under the **ephone-dn** configuration mode.

Configuring COR

This topic describes configuring COR for Cisco SRST and Cisco CallManager Express gateways.



Configuring COR

Cisco.com

STEP 1

```
dial-peer cor custom
 name 911
 name local
 name longdistance
!
```

STEP 2

```
dial-peer cor list 911-call
 member 911
!
dial-peer cor list local-call
 member local
!
dial-peer cor list longdistance-call
 member longdistance
!
dial-peer cor list worker-phone
 member 911
 member local
 member longdistance
!
dial-peer cor list reception-phone
 member 911
 member local
```

STEP 3

```
dial-peer voice 1 pots
 cor outgoing local-call
 destination-pattern 9[2-9]......
 port 2/0
!
dial-peer voice 10 pots
 cor outgoing longdistance-call
 destination-pattern 91..........
 port 2/0
!
dial-peer voice 9110 pots
 cor outgoing 911-call
 destination-pattern 911
 port 2/0
```

STEP 4

```
call-manager-fallback
  cor incoming reception-phone 1 1000
  cor incoming worker-phone 2 1002

or apply to pots voice port:

dial-peer voice 2 pots
 cor incoming reception-phone
 destination-pattern 1500
 port 1/1/0
```

Steps for configuring COR for SRST

1. **Configure cor custom**
2. **Configure cor list**
3. **Apply cor list to dial peers**
4. **Apply cor list to call-manager-fallback mode**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—3-9

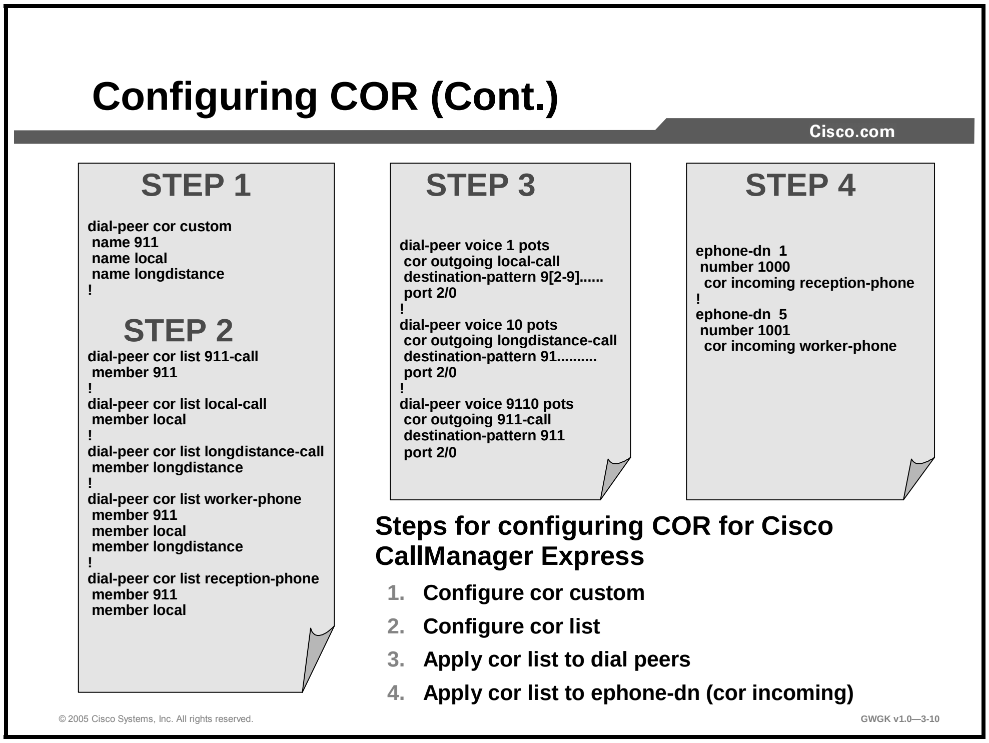
This figure shows the basic three steps in configuring COR on a Cisco SRST gateway. Before relating COR to a dial peer, COR members need to be named, and then a list of members needs to be defined in a COR list. COR is applied to dial peers through COR lists, which comprise a number of COR names that signify specific permissions. This process is similar to Cisco CallManager calling search spaces and partitions. Creating the COR names is similar to creating partitions, and creating the COR lists is similar to creating calling search spaces.

The following is a configuration example of COR applied on a Cisco SRST gateway. With this configuration, the Cisco CallManager phone has unlimited call access, and the employee phones can make local, emergency, and internal calls only. In this example, there is not a COR list specifically for internal calls. If you wish to restrict internal calls, assign an outgoing COR list to an extension or extension range in call-manager-fallback configuration mode.

```
Example Manager phone 2001

Example Employee phone 2003

---------------------------------------------------

!

dial-peer cor custom

 name Emergency

 name Local

 name LD

 name International
```

```
!
dial-peer cor list Emergency
 member Emergency
!
dial-peer cor list Local
 member Local
!
dial-peer cor list LD
 member LD
!
dial-peer cor list International
 member International
!
dial-peer cor list Manager
 member Emergency
 member Local
 member LD
 member International
!
dial-peer cor list Employee
 member Internal
 member Emergency
 member Local
!

!
dial-peer voice 1 pots
 corlist outgoing LD
 description National PSTN
 destination-pattern 91[2-9]..[2-9]......
 port 1/1:23
 forward-digits 11
!
dial-peer voice 2 pots
 corlist outgoing Emergency
 description 911 Emergency
 destination-pattern 911
 port 1/1:23
 forward-digits all
!
```

```
dial-peer voice 3 pots
 corlist outgoing Emergency
 description 911 Emergency
 destination-pattern 9911
 port 1/1:23
 forward-digits 3
!
dial-peer voice 4 pots
 corlist outgoing International
 description International dialing
 destination-pattern 9011T
 port 1/1:23
 prefix 011
!
dial-peer voice 5 pots
 corlist outgoing Local
 description Local Dialing
 destination-pattern 9[2-9]......
 port 1/1:23
!
dial-peer voice 6 pots
 incoming called-number .
 direct-inward-dial
 port 1/1:23
!
call-manager-fallback
 ip source-address 10.10.1.11 port 2000
 max-ephones 8
 max-dn 16
 transfer-pattern 2...
 voicemail 917327518000
 call-forward busy 917327518000
 call-forward noan 917327518000 timeout 12
 cor incoming Manager 1 2001 - 2002
 cor incoming Employee 2 2003 - 2008
```



Configuring COR (Cont.)

STEP 1

```
dial-peer cor custom
 name 911
 name local
 name longdistance
!
```

STEP 2

```
dial-peer cor list 911-call
 member 911
!
dial-peer cor list local-call
 member local
!
dial-peer cor list longdistance-call
 member longdistance
!
dial-peer cor list worker-phone
 member 911
 member local
 member longdistance
!
dial-peer cor list reception-phone
 member 911
 member local
```

STEP 3

```
dial-peer voice 1 pots
 cor outgoing local-call
 destination-pattern 9[2-9]......
 port 2/0
!
dial-peer voice 10 pots
 cor outgoing longdistance-call
 destination-pattern 91..........
 port 2/0
!
dial-peer voice 9110 pots
 cor outgoing 911-call
 destination-pattern 911
 port 2/0
```

STEP 4

```
ephone-dn  1
 number 1000
  cor incoming reception-phone
!
ephone-dn  5
 number 1001
  cor incoming worker-phone
```

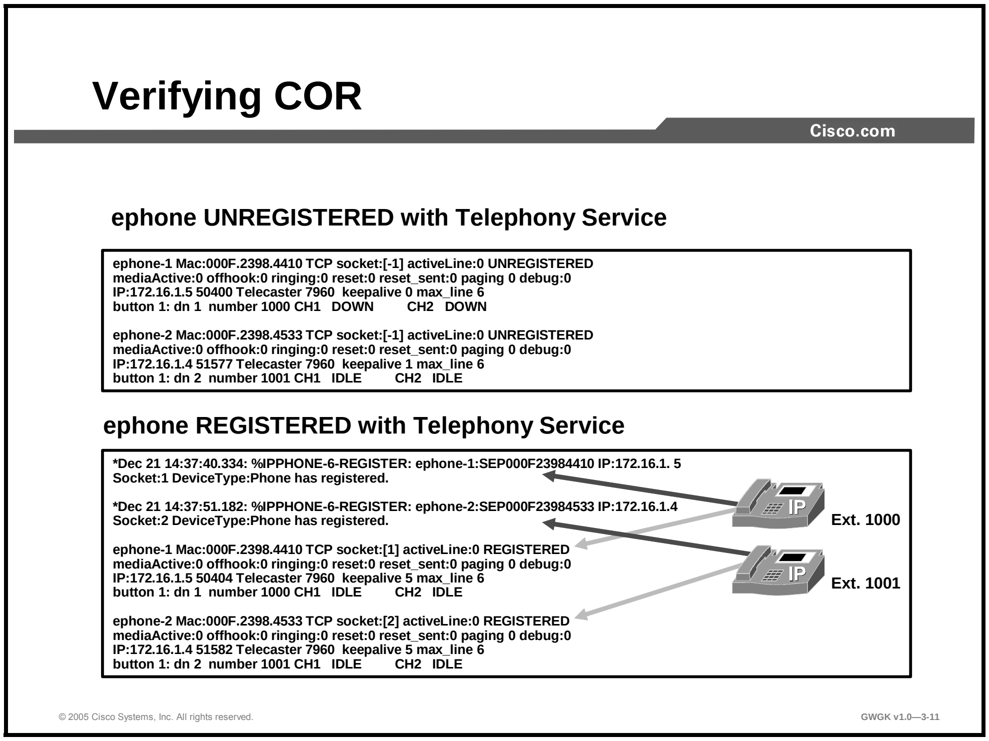
Steps for configuring COR for Cisco CallManager Express

1. Configure cor custom
2. Configure cor list
3. Apply cor list to dial peers
4. Apply cor list to ephone-dn (cor incoming)

This figure shows the steps in configuring COR on Cisco CallManager Express. Notice the first three steps are identical to configuring COR in Cisco SRST. This figure shows two phones: one with directory number (DN) 1000 and one with DN 1001. DN 1000 is the reception phone and DN 1001 is the employee phone. DN 1000 can only make emergency and local calls and is not permitted to make long-distance calls. DN 1001 can make emergency, local, and long-distance calls.

Verifying COR

This topic describes how to verify the COR configuration and verify that the configuration works.



Verifying COR

ephone UNREGISTERED with Telephony Service

```
ephone-1 Mac:000F.2398.4410 TCP socket:[-1] activeLine:0 UNREGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:172.16.1.5 50400 Telecaster 7960  keepalive 0 max_line 6
button 1: dn 1  number 1000 CH1   DOWN        CH2   DOWN

ephone-2 Mac:000F.2398.4533 TCP socket:[-1] activeLine:0 UNREGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:172.16.1.4 51577 Telecaster 7960  keepalive 1 max_line 6
button 1: dn 2  number 1001 CH1   IDLE        CH2   IDLE
```

ephone REGISTERED with Telephony Service

```
*Dec 21 14:37:40.334: %IPPHONE-6-REGISTER: ephone-1:SEP000F23984410 IP:172.16.1. 5
Socket:1 DeviceType:Phone has registered.

*Dec 21 14:37:51.182: %IPPHONE-6-REGISTER: ephone-2:SEP000F23984533 IP:172.16.1.4
Socket:2 DeviceType:Phone has registered.

ephone-1 Mac:000F.2398.4410 TCP socket:[1] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:172.16.1.5 50404 Telecaster 7960  keepalive 5 max_line 6
button 1: dn 1  number 1000 CH1   IDLE        CH2   IDLE

ephone-2 Mac:000F.2398.4533 TCP socket:[2] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:172.16.1.4 51582 Telecaster 7960  keepalive 5 max_line 6
button 1: dn 2  number 1001 CH1   IDLE        CH2   IDLE
```

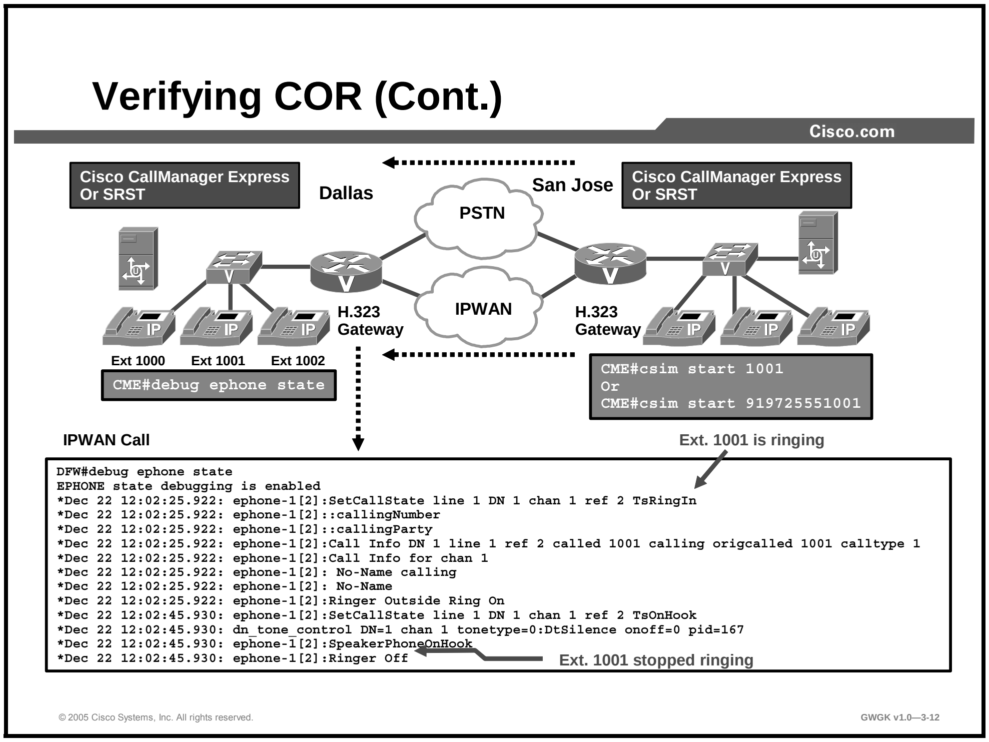
GWGK v1.0—3-11

To verify the COR configuration, you need to make sure all Ethernet phones (ephones) are registered with the Cisco SRST or Cisco CallManager Express gateway. You should not try verifying the operation until the phones completely register.

When Cisco CallManager Express is first configured or when the Cisco SRST mode is engaged, give the phones about 2 to 4 minutes to register with the gateway. Cisco CallManager Express usually takes longer for phones to register than Cisco SRST does.

The example in the figure was produced by the **debug ephone detail** command or the **debug ephone register** command.

Verifying COR (Cont.)



```
CME#debug ephone state
```

```
CME#csim start 1001
Or
CME#csim start 919725551001
```

```
DFW#debug ephone state
EPHONE state debugging is enabled
*Dec 22 12:02:25.922: ephone-1[2]:SetCallState line 1 DN 1 chan 1 ref 2 TsRingIn
*Dec 22 12:02:25.922: ephone-1[2]::callingNumber
*Dec 22 12:02:25.922: ephone-1[2]::callingParty
*Dec 22 12:02:25.922: ephone-1[2]:Call Info DN 1 line 1 ref 2 called 1001 calling origcalled 1001 calltype 1
*Dec 22 12:02:25.922: ephone-1[2]:Call Info for chan 1
*Dec 22 12:02:25.922: ephone-1[2]: No-Name calling
*Dec 22 12:02:25.922: ephone-1[2]: No-Name
*Dec 22 12:02:25.922: ephone-1[2]:Ringer Outside Ring On
*Dec 22 12:02:45.930: ephone-1[2]:SetCallState line 1 DN 1 chan 1 ref 2 TsOnHook
*Dec 22 12:02:45.930: dn_tone_control DN=1 chan 1 tonetype=0:DtSilence onoff=0 pid=167
*Dec 22 12:02:45.930: ephone-1[2]:SpeakerPhoneOnHook
*Dec 22 12:02:45.930: ephone-1[2]:Ringer Off
```

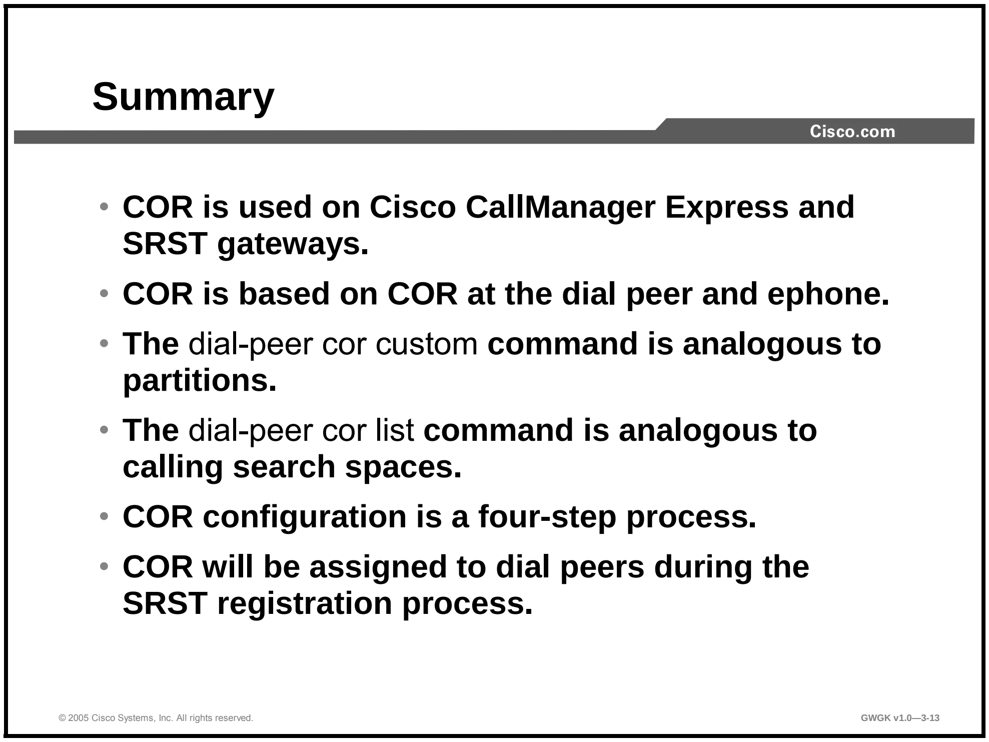
GWGK v1.0—3-12

You can verify that your configuration is correct by placing a few test calls over the gateways through the IP WAN or the PSTN. By running a debug on the target gateway, you can see if the call coming into the gateway is ringing. From the San Jose gateway shown in the figure, there was a test call placed using the **csim start 1001** command, where 1001 is a Cisco CallManager Express extension number on the Dallas gateway. At the Dallas gateway, a **debug ephone state** command was used. You can use this testing process for SIP, Cisco SRST, or Cisco CallManager Express gateways.

In this figure, the **debug ephone state** command shows that extension 1001 at the Dallas gateway is ringing. This is a valid test. However, someone physically needs to hear if the phone is actually ringing. If you want to test a call over the PSTN, you could use **csim start 919725551001** command. It is assumed that the operation of **csim start** is setup correctly on the dial peers. Any **debug ephone** commands that are used for PSTN testing will not produce an output. You will have to use the **debug voice ccapi inout** command for that information.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

Cisco.com

- COR is used on Cisco CallManager Express and SRST gateways.
- COR is based on COR at the dial peer and ephone.
- The dial-peer cor custom command is analogous to partitions.
- The dial-peer cor list command is analogous to calling search spaces.
- COR configuration is a four-step process.
- COR will be assigned to dial peers during the SRST registration process.

GWGK v1.0—3-13

References

For additional information, refer to these resources:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_administration_guide_book09186a00802d3ca5.html

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) COR is most commonly used with which device? (Choose two.) (Source:)

A) Cisco CallManager Express
B) SIP gateways
C) Cisco SRST
D) MGCP gateways

Q2) COR resembles which feature in Cisco CallManager? (Source:)

A) Calling search spaces and partitions
B) Digit translation and transformation masks
C) Trunk groups
D) Line groups

Q3) Which task has to be completed before you can apply outgoing COR to a POTS dial peer? (Source:)

A) **dial-peer cor list** needs to be configured
B) **dial-peer cor custom** has to be configured
C) dial-peer session targets need to be defined
D) codec complexity needs to be defined

Q4) By default, the incoming call leg has which priority over outgoing call legs? (Source:)

A) Higher priory
B) Lower priority
C) Equal priority

Q5) If the COR list of the incoming dial peer includes members A, B, and C, and the COR list of the outgoing dial peer includes members A and B but not C, what will happen to the call? (Source:)

A) The call goes through.
B) The user hears a reorder tone or a fast busy tone.
C) The call goes to the operator.
D) This is not a supported setup.

Q6) If the COR list of an incoming dial peer includes members A, and B, and the COR list of the outgoing dial peer has members A, B, and C, what will happen to the call? (Source:)

A) The call goes through.
B) The user hears a reorder tone or a fast busy tone.
C) The call goes to the operator.
D) This is not a supported setup.

Q7) In **dial-peer cor custom** configuration, what are you defining? (Choose two.) (Source:)

A) partition-like names
B) calling search space-like members
C) names so that you can associate them as members under the COR list configuration
D) POTS dial peers

Q8) Which two commands would be entered to apply the same COR to all phones registered to a Cisco SRST gateway? (Choose two.) (Source:)

A) **telephony-service**
B) **cor incoming <corlist> default**
C) **call-manager-fallback**
D) **Cisco CallManager device pool**

Lesson Self-Check Answer Key

Q1)	A, C
Q2)	A
Q3)	B
Q4)	A
Q5)	A
Q6)	B
Q7)	A, C
Q8)	B, C

Lesson 4

Influencing Call Routes

Overview

This lesson discusses the technologies that are used to influence call routes on a Cisco gateway and the various common configurations that are used to achieve this.

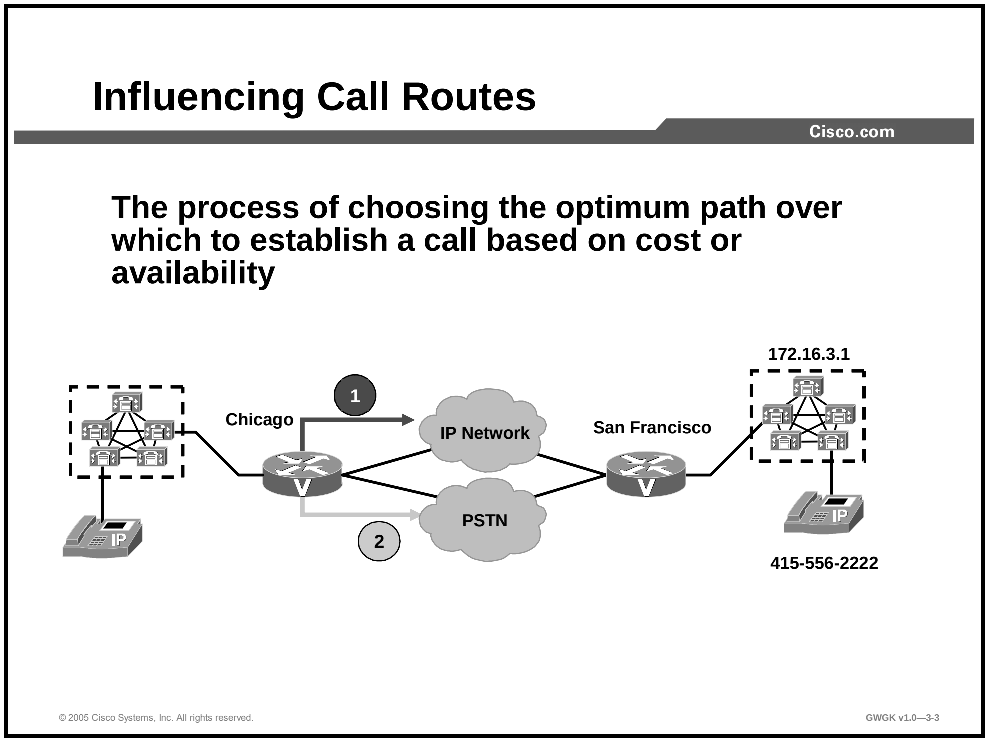
Objectives

Upon completing this lesson, you will be able to influence call routes to provide redundancy and cost efficiency. This ability includes being able to meet these objectives:

- Describe the technologies that are used to influence call routing
- Configure hunt groups to determine call route selection
- Manipulate ISDN cause codes to enable reroute
- Implement CAC
- Configure TEHO to determine call route selection

Influencing Call Routes

This topic describes how to influencing call routes.



Influencing Call Routes

Cisco.com

The process of choosing the optimum path over which to establish a call based on cost or availability

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—3-3

There are many ways to influence call routes on Cisco gateways to provide redundancy or to reduce costs. For example, the primary path for a call may be through the IP WAN, but the call should be routed across the public switched telephone network (PSTN) in the event of an IP-WAN failure or if you anticipate bandwidth constraints.

The following are some design considerations when you are planning for call rerouting:

1. What calls are routed across the IP WAN? Are there internal only or internal and external calls?

2. What is the bandwidth availability for calls across the IP WAN?

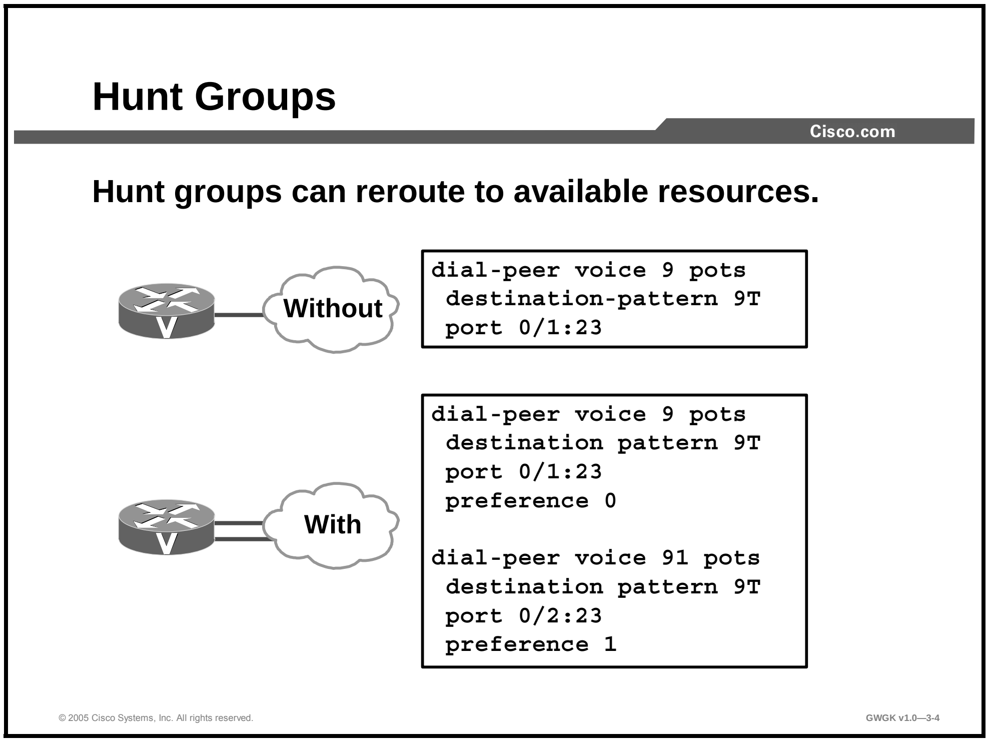
3. What digit manipulations are required to reroute calls?

4. Do you have multiple service providers or dedicated circuits for long distance? Are there different billing charges based on the time of day?

5. In case of a PSTN outage, what are the call reroute requirements? Should local PSTN calls be routed across the IP WAN and placed as long-distance calls?

Hunt Groups

This topic describes the hunt Group and its configuration.



Hunt Groups

Cisco.com

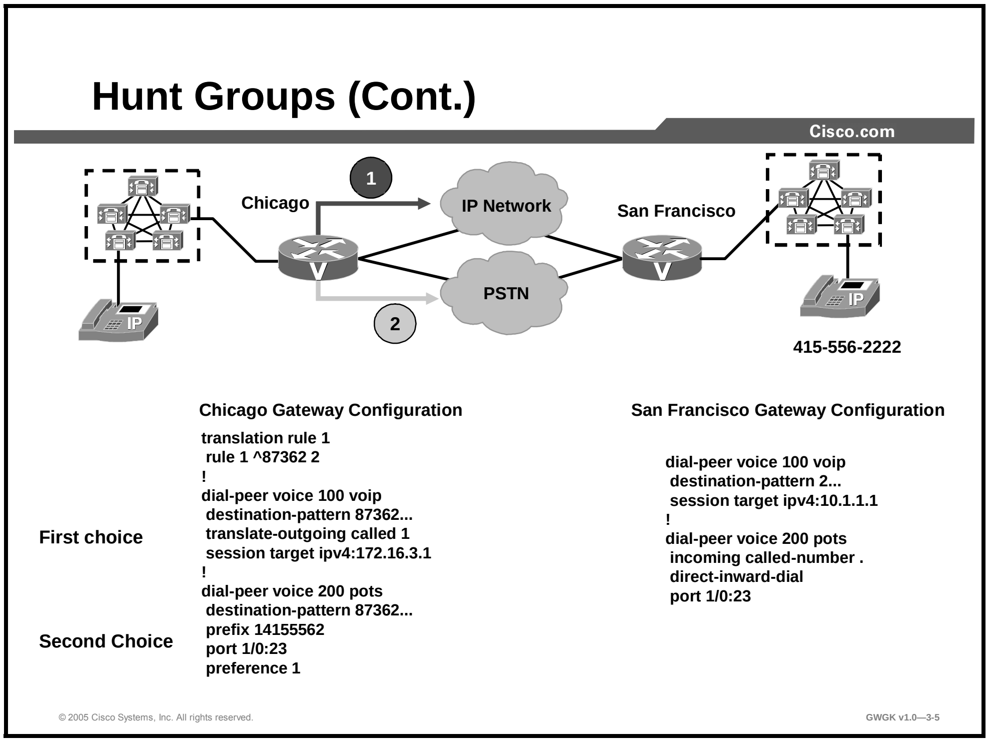
Hunt groups can reroute to available resources.

```
dial-peer voice 9 pots
 destination-pattern 9T
 port 0/1:23
```

```
dial-peer voice 9 pots
 destination pattern 9T
 port 0/1:23
 preference 0

dial-peer voice 91 pots
 destination pattern 9T
 port 0/2:23
 preference 1
```

GWGK v1.0—3-4

The simplest method of rerouting calls is to configure a hunt group using the preference command. Dial-peer hunting is used to ensure that when either a primary route or service is down or resources are fully utilized, there is a second route to send calls. Consider this to be an overflow method. As shown in the example in the figure, if voice port 0/1:23 was 100 percent utilized, meaning all DS0s were in use, dial peer 91 would be used and calls would be sent to voice port 0/2:23.



Hunt Groups (Cont.)

Chicago Gateway Configuration

```
translation rule 1
 rule 1 ^87362 2
!
dial-peer voice 100 voip
 destination-pattern 87362...
 translate-outgoing called 1
 session target ipv4:172.16.3.1
!
dial-peer voice 200 pots
 destination-pattern 87362...
 prefix 14155562
 port 1/0:23
 preference 1
```

San Francisco Gateway Configuration

```
dial-peer voice 100 voip
 destination-pattern 2...
 session target ipv4:10.1.1.1
!
dial-peer voice 200 pots
 incoming called-number .
 direct-inward-dial
 port 1/0:23
```

GWGK v1.0—3-5

This figure shows how a hunt group can be applied to achieve alternate call routing based on resource availability. When a call is placed from Chicago to San Francisco, the first choice is to route the call across the IP WAN. The second choice is to send it out the PSTN. This configuration requires digit manipulation for both dial peers.

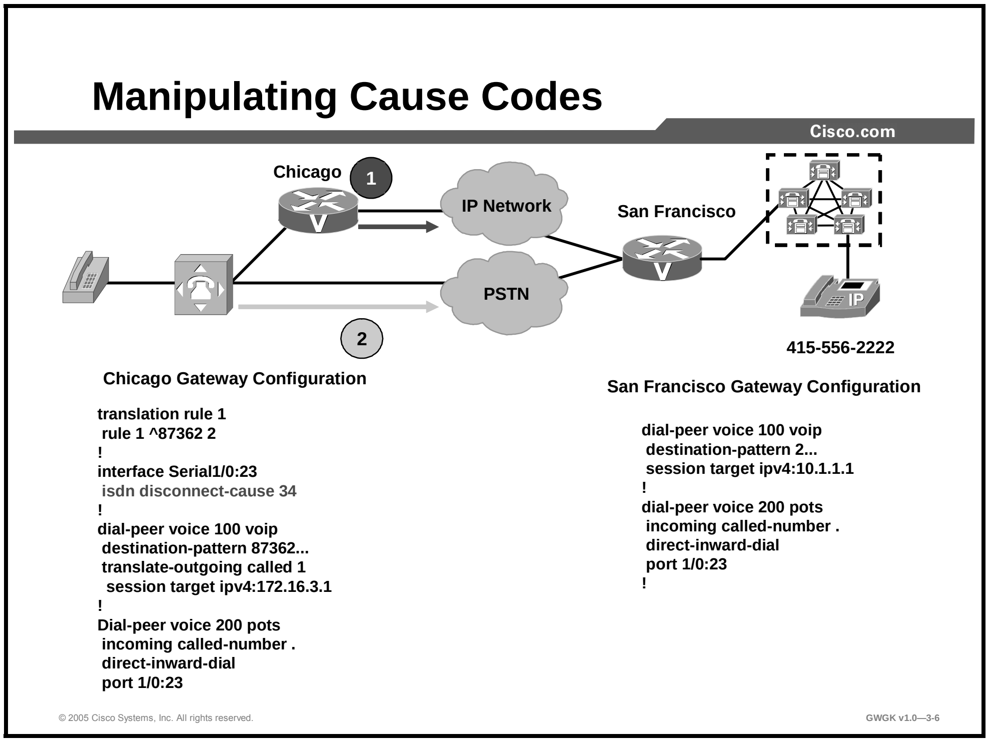
When a call is placed from Chicago to 87362222, dial peer 100 is matched. Because this is a VoIP dial peer, the explicitly matched digits are not stripped. Because the dial peer in the San Francisco gateway will match the extension, a simple translation rule is configured to strip off the access code and the site code from the called number.

If the IP WAN is not available, dial peer 200 is matched. This plain old telephone service (POTS) dial peer will strip the explicitly matched digits from the destination pattern. The digits required to route the call correctly over the PSTN are prefixed, and the call is setup across the PSTN.

In this configuration, the PSTN is sending a four-digit dialed number identification service (DNIS) to the San Francisco gateway. If this were not the case, dial peer 200 would also require digit manipulation to allow the incoming call to be routed correctly.

Manipulating Cause Codes

This topic describes methods to manipulate cause codes that are sent to the originating device.



Manipulating Cause Codes

Chicago Gateway Configuration

```
translation rule 1
 rule 1 ^87362 2
!
interface Serial1/0:23
 isdn disconnect-cause 34
!
dial-peer voice 100 voip
 destination-pattern 87362...
 translate-outgoing called 1
  session target ipv4:172.16.3.1
!
Dial-peer voice 200 pots
 incoming called-number .
 direct-inward-dial
 port 1/0:23
```

San Francisco Gateway Configuration

```
dial-peer voice 100 voip
 destination-pattern 2...
 session target ipv4:10.1.1.1
!
dial-peer voice 200 pots
 incoming called-number .
 direct-inward-dial
 port 1/0:23
!
```

GWGK v1.0—3-6

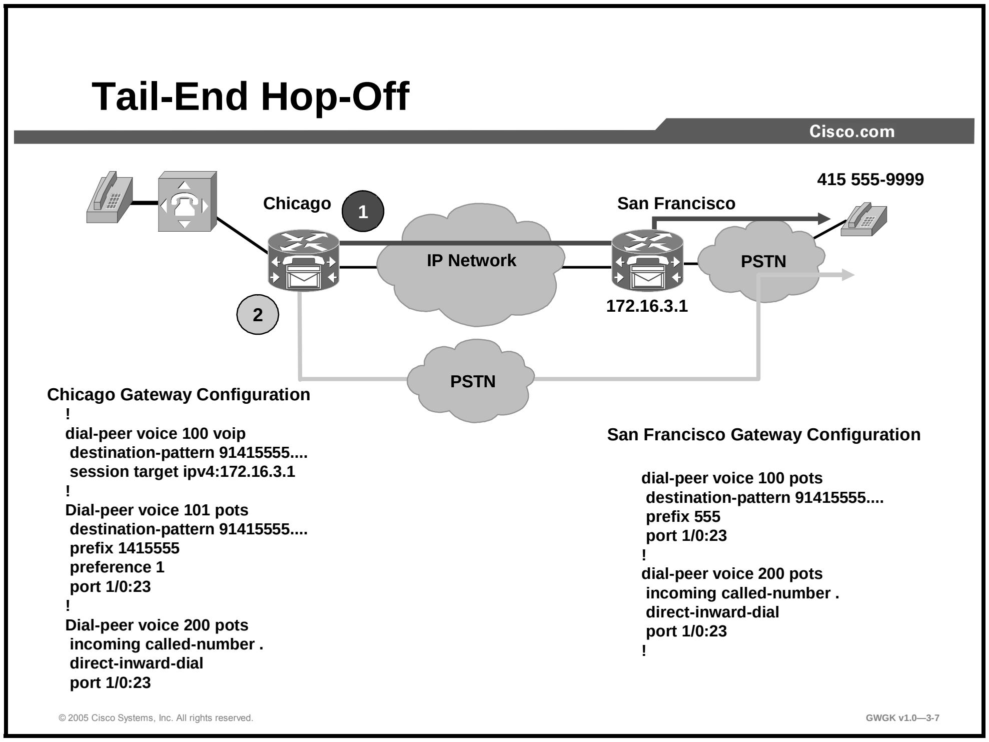
This figure shows a typical PBX toll-bypass integration. In this example, the second route is controlled by the PBX instead of by the gateway. The PBX will determine whether to reroute the call based on the disconnect cause code returned by the gateway. For example, a PBX may not attempt a reroute if the cause code indicates that the end station is busy. The gateway can be configured to send a cause code in the range of 1 to 127.

In this partial configuration sample, the cause code is set to 34, which indicates that no circuit or channel is available. A complete list of disconnect codes is available at http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_command_reference_chapter09186a008007ff75.html.

It is typically not necessary to manipulate cause codes.

Tail-End Hop-Off

This topic describes tail-end hop-off (TEHO) and how it is configured on a H.323 Gateway.



Tail-End Hop-Off

Chicago Gateway Configuration

```
!
dial-peer voice 100 voip
 destination-pattern 91415555....
 session target ipv4:172.16.3.1
!
Dial-peer voice 101 pots
 destination-pattern 91415555....
 prefix 1415555
 preference 1
 port 1/0:23
!
Dial-peer voice 200 pots
 incoming called-number .
 direct-inward-dial
 port 1/0:23
```

San Francisco Gateway Configuration

```
dial-peer voice 100 pots
 destination-pattern 91415555....
 prefix 555
 port 1/0:23
!
dial-peer voice 200 pots
 incoming called-number .
 direct-inward-dial
 port 1/0:23
!
```

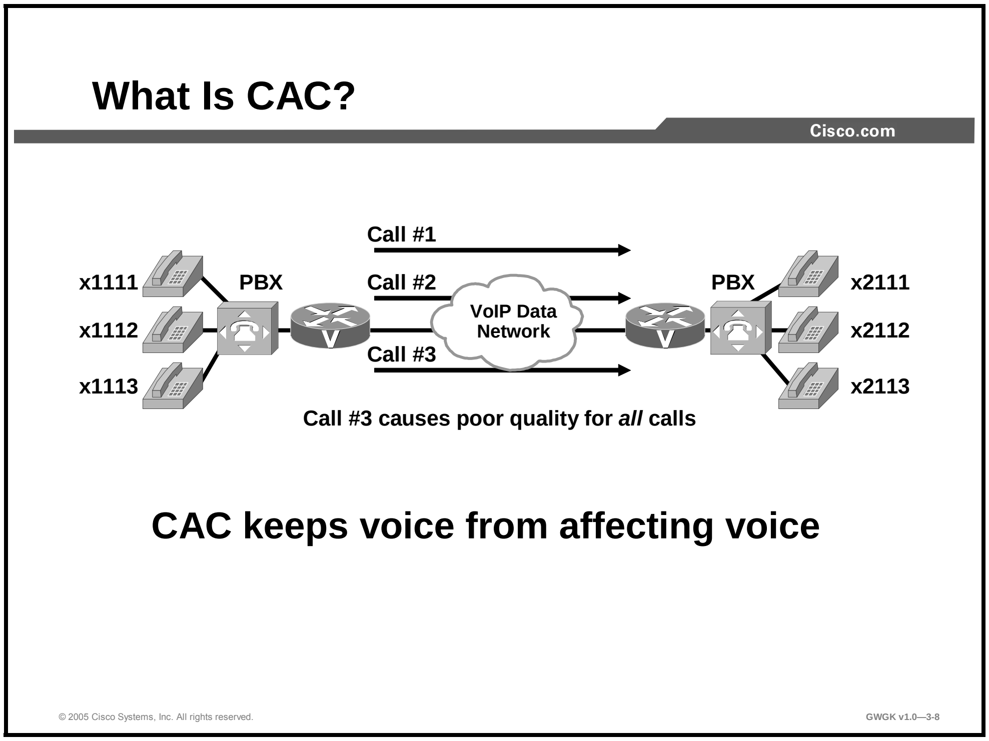
GWGK v1.0—3-7

TEHO allows an enterprise to route long-distance calls over the IP WAN to off-net locations. The example in the figure expands on the previous example and show that TEHO allows calls from Chicago to San Francisco to route over the IP WAN as the first choice and over the PSTN as the alternate choice. The benefit of TEHO is reduced long-distance charges, but implementing TEHO can greatly complicate your dial plan. TEHO requires specific dial-plan entries for each remote destination. You may also need multiple entries for each site. For example, in the United States, some large cities have multiple area codes that are considered local calls, while less densely populated areas may have an area code that includes both local and long distance prefixes. As the number of sites grows, dial-plan maintenance can become very difficult. Most enterprises quickly realize that a gatekeeper is necessary to effectively manage a dial plan supporting TEHO.

Before implementing TEHO, consider the local regulations governing telecommunications. Many countries allow intracompany calls to be routed over a private network but require external calls to be handled exclusively by the PSTN. This is especially important for enterprises with locations in multiple countries. You may be able to take advantage of TEHO for some of your locations and not for others. To minimize the impact on users, it is best to implement your dial plan so that the caller does not have to dial specific access codes to route the call over the IP WAN. The call route should be transparent to the caller.

Call Admission Control

This topic describes common types of Call Admission Control (CAC) and how to configure it on a H.323 gateway.



What Is CAC?

Cisco.com

Call #3 causes poor quality for *all* calls

CAC keeps voice from affecting voice

GWGK v1.0—3-8

A variety of quality of service (QoS) mechanisms other than CAC exist in Cisco IOS software for the purpose of designing and configuring packet networks to provide the necessary low latency and guaranteed delivery of voice traffic. These QoS mechanisms include tools such as queueing, policing, traffic shaping, packet marking, and fragmentation and interleaving. These mechanisms differ from CAC in the following important ways:

- They are designed to protect voice traffic from data traffic contending for the same network resources.
- They are designed to deal with traffic already present on the network.

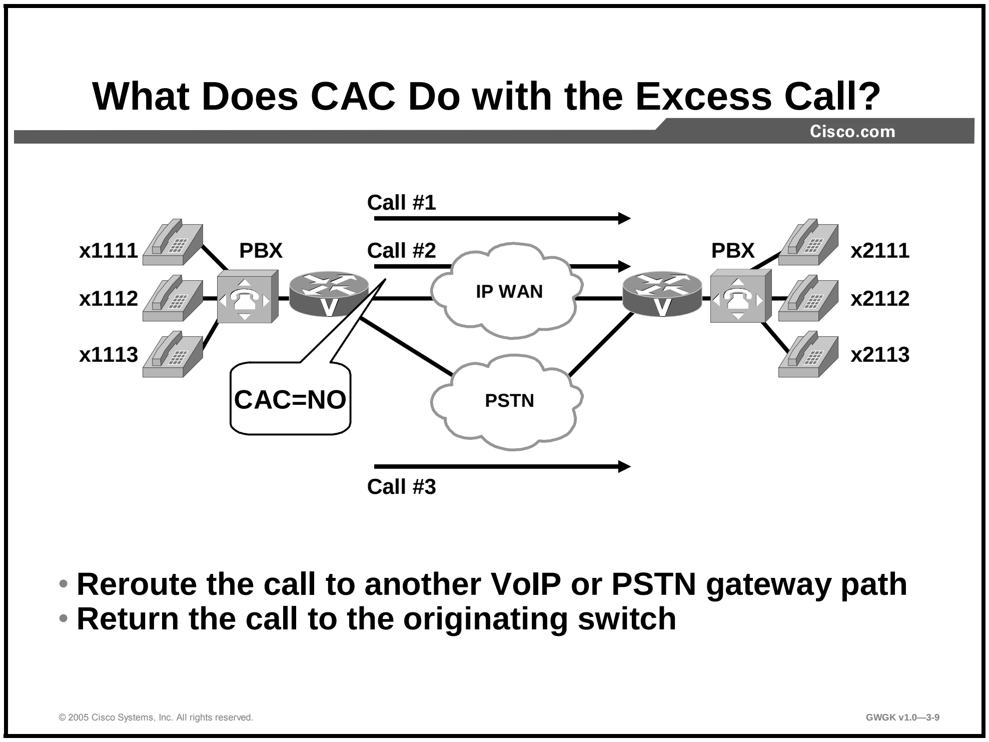
CAC mechanisms extend the capabilities of the QoS tool suite to protect voice traffic from being negatively affected by other voice traffic and to keep excess voice traffic off the network. CAC is needed to maintain the voice quality of VoIP calls. As the figure shows, if the WAN access link between the two PBXs has the bandwidth to carry only two VoIP calls, admitting the third call will impair the voice quality of all three calls.

The reason for this impairment is that the queueing mechanisms provide policing, not CAC, which means that if packets exceeding the configured or allowable rate are received, these packets are simply tail-dropped from the queue. There is no capability in the queueing mechanisms to distinguish which IP packet belongs to which voice call, so any packet exceeding the given arrival rate within a certain period of time will be dropped. Thus, all three calls will experience packet loss, which is perceived as clips by the end users.

CAC is a concept that applies to voice traffic only, not data traffic. If an influx of data traffic oversubscribes a particular link in the network, queueing, buffering, and packet-drop decisions resolve the congestion. The extra traffic is simply delayed until the interface becomes available to send the traffic, or, if traffic is dropped, until the protocol or the end user initiates a timeout and requests a retransmission of the information.

Network congestion cannot be resolved in this manner when real-time traffic, sensitive to both latency and packet loss, is present, without jeopardizing the QoS expected by the users of that traffic. For real-time delay-sensitive traffic such as voice, it is better to deny network access under congestion conditions than to allow traffic onto the network to be dropped and delayed, causing intermittent impaired QoS and resulting in customer dissatisfaction.

Therefore, making the decision to use CAC is a deterministic and informed decision that is made before a voice call is established and is based on whether the required network resources are available to provide suitable QoS for the new call.



What Does CAC Do with the Excess Call?

Cisco.com

- Reroute the call to another VoIP or PSTN gateway path
- Return the call to the originating switch

GWGK v1.0—3-9

After the call is rejected, the originating gateway must find another means of handling the call. There are several possibilities, most of which are dependent on the configuration of the gateway. In the absence of any specific configuration, the outgoing gateway will provide a reorder tone to the calling party. This tone is often intercepted by PSTN switches or PBXs with an announcement such as “All circuits are busy; please try your call again later.”

The outgoing gateway can be configured for the following rerouting scenarios:

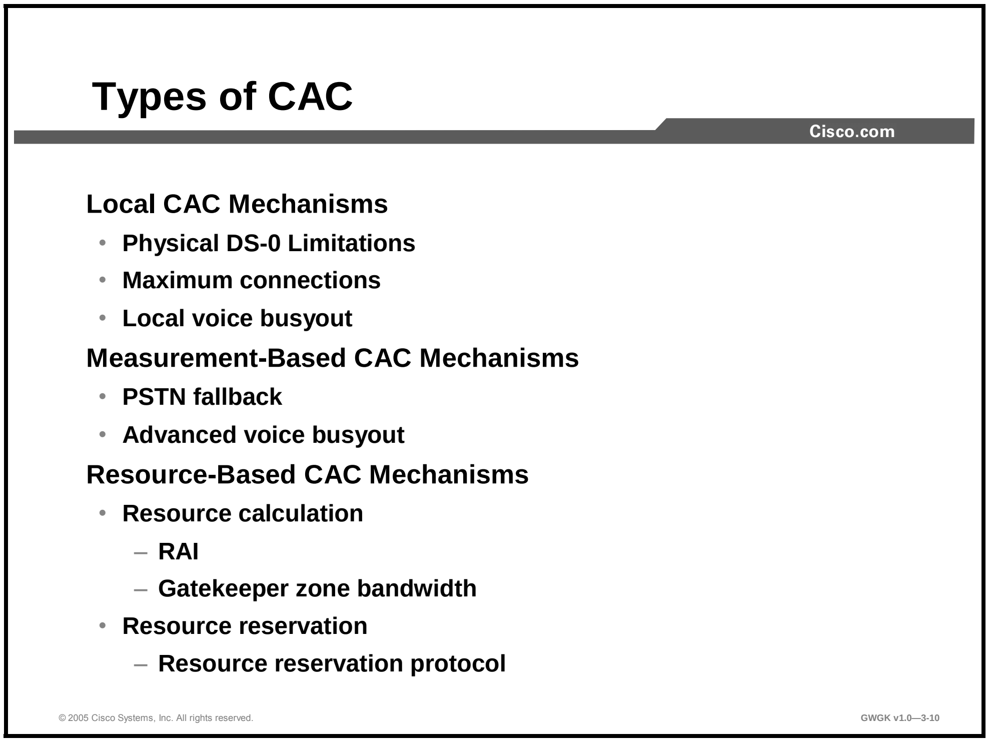
- The call can be rerouted via an alternate packet network path if such a path exists, which requires the configuration of a second VoIP dial peer of a lower preference than the original one chosen.
- The call can be rerouted via an alternate time-division multiplexing (TDM) network path if such a path exists, which requires the configuration of a POTS dial peer and a physical TDM interface to the PSTN or another PBX.

The call can be returned to the originating TDM switch to leverage one of the following rerouting capabilities:

- If the connection between the originating switch and the outgoing gateway is a common channel signaling (CCS) trunk (for example, Q Signaling [QSIG], PRI, or BRI), the call can be rejected with a cause code and the originating switch will tear down the trunk and resume handling of the call.
- If the connection between the originating switch and the outgoing gateway is an analog or CAS trunk, the call must be hairpinned (using a second trunk on the same interface) back to the switch.

Types of CAC

This topic discusses the types of CAC available on Cisco voice gateways.



Types of CAC

Cisco.com

Local CAC Mechanisms

- **Physical DS-0 Limitations**
- **Maximum connections**
- **Local voice busyout**

Measurement-Based CAC Mechanisms

- **PSTN fallback**
- **Advanced voice busyout**

Resource-Based CAC Mechanisms

- **Resource calculation**
  - **RAI**
  - **Gatekeeper zone bandwidth**
- **Resource reservation**
  - **Resource reservation protocol**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—3-10

The remainder of this lesson discusses different CAC mechanisms that are available in current versions of Cisco IOS software. They are grouped into three categories:

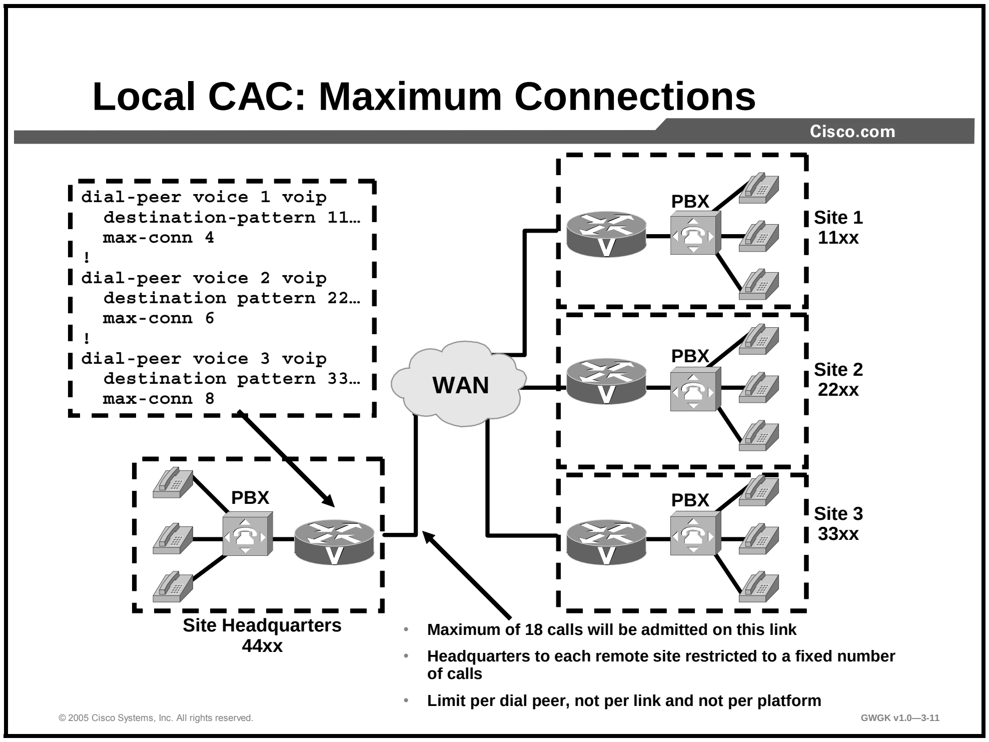
- **Local CAC Mechanisms:** Local CAC mechanisms function on the outgoing gateway. The CAC decision is based on nodal information such as the state of the outgoing LAN or WAN link. If the local packet network link is down, you should not execute complex decision logic based on the state of the rest of the network because that network is unreachable. Local mechanisms include configuration items to disallow more than a fixed number of calls. For example, if the network designer already knows that no more than five calls can fit across the outgoing WAN link because of bandwidth limitations, then it should be possible to configure the local node to allow no more than five calls.

- **Measurement-Based CAC Mechanisms:** Measurement-based CAC techniques look ahead into the packet network to gauge the state of the network to determine whether to allow a new call. Gauging the state of the network implies sending probes to the destination IP address (usually the terminating gateway or terminating gatekeeper) that will return to the outgoing gateway with some measured information on the conditions the probe found while traversing the network to the destination. Typically, loss and delay characteristics are the interesting information elements for voice.

- **Resource-Based CAC Mechanisms:** There are two types of resource-based mechanisms: Those that calculate resources that are needed or available and those reserving resources for the call. Resources of interest include link bandwidth, digital signal processors (DSPs), and digital signal level 0 (DS-0) timeslots on the connecting TDM trunks, CPU power, and memory.

Local CAC Mechanisms

This topic discusses local CAC mechanisms.



Local CAC: Maximum Connections

```
dial-peer voice 1 voip
  destination-pattern 11…
  max-conn 4
!
dial-peer voice 2 voip
  destination pattern 22…
  max-conn 6
!
dial-peer voice 3 voip
  destination pattern 33…
  max-conn 8
```

- Maximum of 18 calls will be admitted on this link
- Headquarters to each remote site restricted to a fixed number of calls
- Limit per dial peer, not per link and not per platform

GWGK v1.0—3-11

The local mechanisms are the simplest CAC mechanisms to understand and implement. They work on the outgoing gateway and consider the local conditions of the node. They also tend to have low overhead, so if any of these mechanisms provide the desired functionality, there is little reason to implement any of the more complex features. However, it is likely that in a medium- to large-sized network, satisfactory CAC functionality will require more than the use of a local mechanism.

Local CAC mechanisms include the following tools:

- Physical DS-0 limitation
- Maximum connections
- Local voice busyout

Physical DS-0 Limitation

By limiting the physical voice paths to the call processing system, you can control how many simultaneous calls can be delivered over the IP WAN. This method of CAC can be useful when connecting to a PBX or key system. Once the available call paths have been used, the PBX or key system is responsible for handling over-flow by either using an alternate call path or by sending reorder tone.

Maximum Connections

The maximum connections CAC mechanism involves using the **max-conn** dial-peer configuration command on the outgoing gateway to restrict the number of concurrent connections (calls) that can be active on that dial peer at any one time.

This tool is easy to use but can only solve a limited number of network design problems. Because it is applied per dial peer, it is not possible to limit the total number of calls the outgoing gateway can have active simultaneously unless you have a limited number of dial peers and you use the **max-conn** command on each one.

With this limitation in mind, the **max-conn** command provides a viable CAC method in at least two scenarios:

- For a relatively small number of dial peers pointing calls to an egress WAN link, the sum of the individual **max-conn** dial-peer statements will provide the maximum number of calls that can be simultaneously active across the WAN link.
- If the design objective is to limit the maximum number of calls between sites (rather than protecting the bandwidth of the egress WAN link), this is a very suitable feature to use, but only if the dial peers are structured so that each remote site has one dial peer pointing calls to it.

The figure shows an example of this type of network: There are three remote sites, each with recognizable first digits in the dialing plan. Therefore, the outgoing VoIP dial peers at the headquarters site match the remote sites one for one. The numbers of calls to remote sites 1, 2, and 3 will be limited to 4, 6, and 8 respectively. The egress WAN link can therefore have no more than 18 calls active at any one time. In this configuration, provisioning the bandwidth of the link for that number of calls would be prudent.

The maximum connections feature can also be used on the POTS dial peer to limit the number of calls that can be active on a T1 or E1 to a PBX or PSTN. Use this feature if the desire is to provision all timeslots on that connection but to limit the number of calls to a lesser number than the physical number of timeslots.

Although this feature is useful in many scenarios, it has the following drawbacks:

- It provides little or no protection for links in the network backbone.
- It does not work for IP telephony applications that do not use dial peers.
- It is limited to simple topologies.
- It does not react to link failures or changing network conditions.

Local Voice Busyout

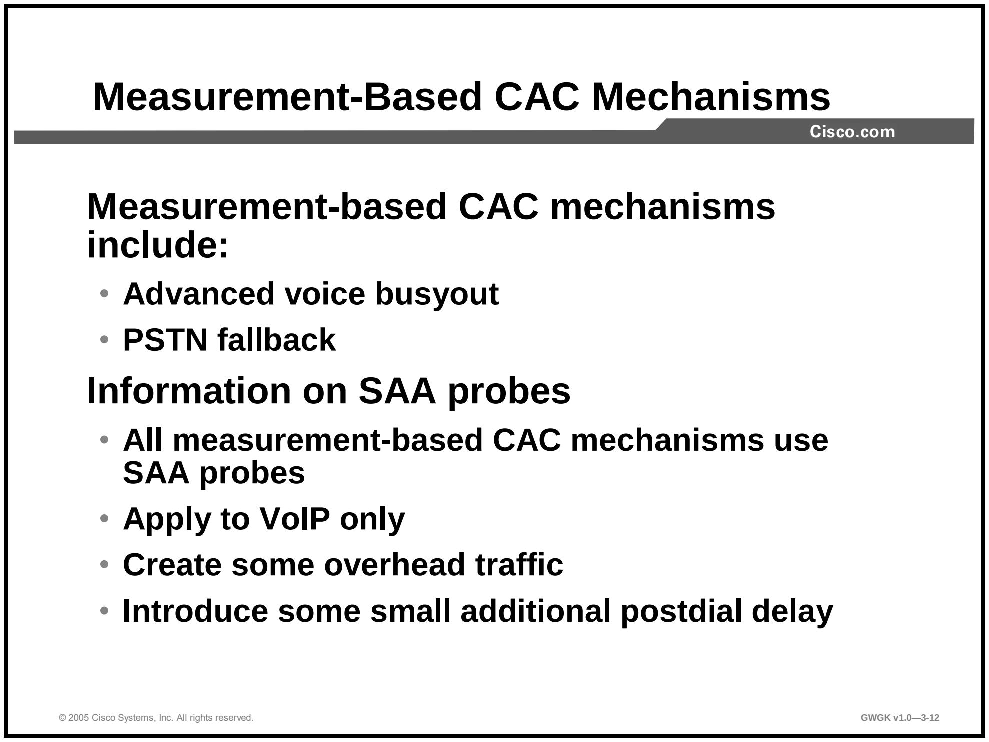
Local voice busyout monitors the physical router port that is used for IP network connectivity and busies out voice ports if the physical router interface is down. This prevents the PBX or key system from sending calls to the gateway if there is not an IP path available to support the VoIP call leg. Local voice busyout is used in PBX or key system integrations.

Here is an example from a voice gateway configured for local voice busyout:

```
router(config)# voice-port 1/2/2
router(config-voiceport)# busyout monitor interface serial 0
```

Measurement-Based CAC Mechanisms

This topic discusses measurement-based CAC mechanisms.



Measurement-Based CAC Mechanisms

Cisco.com

Measurement-based CAC mechanisms include:

- **Advanced voice busyout**
- **PSTN fallback**

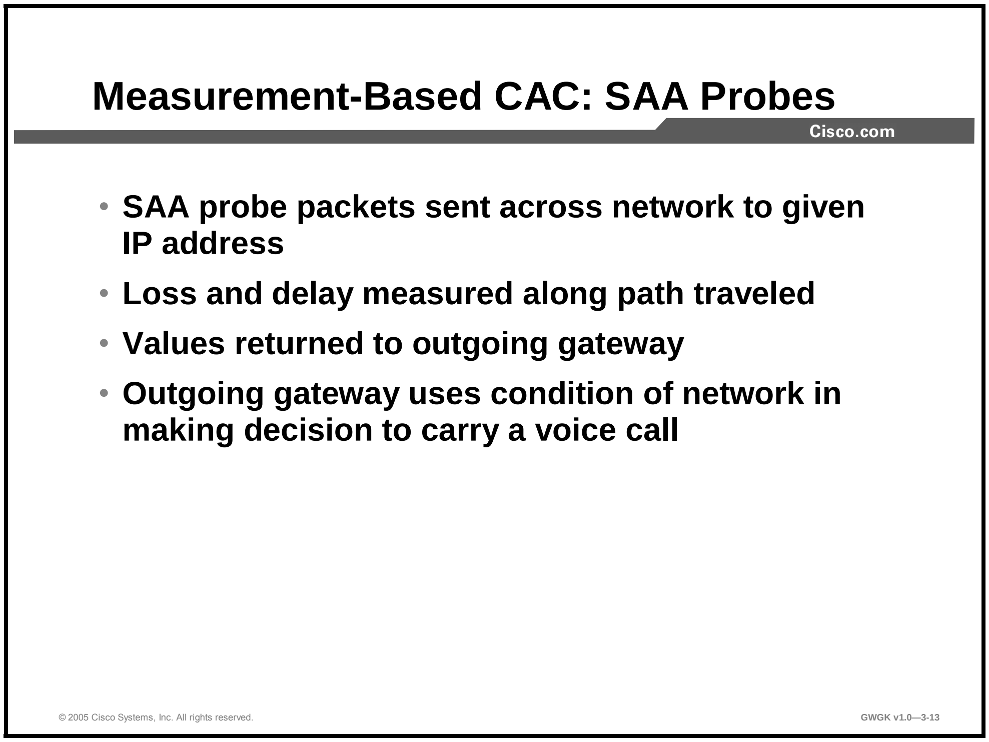
Information on SAA probes

- **All measurement-based CAC mechanisms use SAA probes**
- **Apply to VoIP only**
- **Create some overhead traffic**
- **Introduce some small additional postdial delay**

GWGK v1.0—3-12

Measurement-based CAC mechanisms include the following techniques:

- PSTN fallback
- Advanced voice busyout



Measurement-Based CAC: SAA Probes

Cisco.com

- SAA probe packets sent across network to given IP address
- Loss and delay measured along path traveled
- Values returned to outgoing gateway
- Outgoing gateway uses condition of network in making decision to carry a voice call

GWGK v1.0—3-13

Information on SAA probes

Before the actual features of measurement-based CAC mechanisms are discussed, some background information on Service Assurance Agent (SAA) probes is necessary because this is the underlying technique employed by the measurement-based CAC methods. SAA probes traverse the network to a given IP destination and measure the loss and delay characteristics of the network along the path traveled. These values are returned to the outgoing gateway for use in making a decision on the condition of the network and its ability to carry a voice call.

The following are attributes of measurement-based CAC mechanisms that are derived from their use of SAA probes:

- Because an SAA probe is an IP packet traveling to an IP destination, all measurement-based CAC techniques apply to VoIP only (including Voice over Frame Relay [VoFR] and Voice over ATM [VoATM]networks).
- As probes are sent into the network, a certain amount of overhead traffic is produced in gathering the information needed for CAC.
- If the CAC decision for a call must await a probe to be dispatched and returned, there is some small additional post-dial delay for the call. This should be insignificant in a properly designed network.

The Cisco SAA

SAA is a network management feature that is integrated in Cisco IOS software and provides a mechanism for network congestion analysis. It also underlies a multitude of other Cisco IOS features. It was not implemented for accomplishing CAC nor is it a part of the CAC suite. However, its capabilities to measure network delay and packet loss are useful as building blocks on which to base CAC features. The SAA feature is an extension to the Response Time Reporter (RTR) feature found in earlier releases of Cisco IOS software.

SAA probes do not provide any bandwidth information, either configured or available. However, if bandwidth across a link anywhere in the path that the voice call will follow is oversubscribed, it is reasonable to assume that the packet delay and loss values that the probe returns will indeed reflect this condition, even if indirectly.

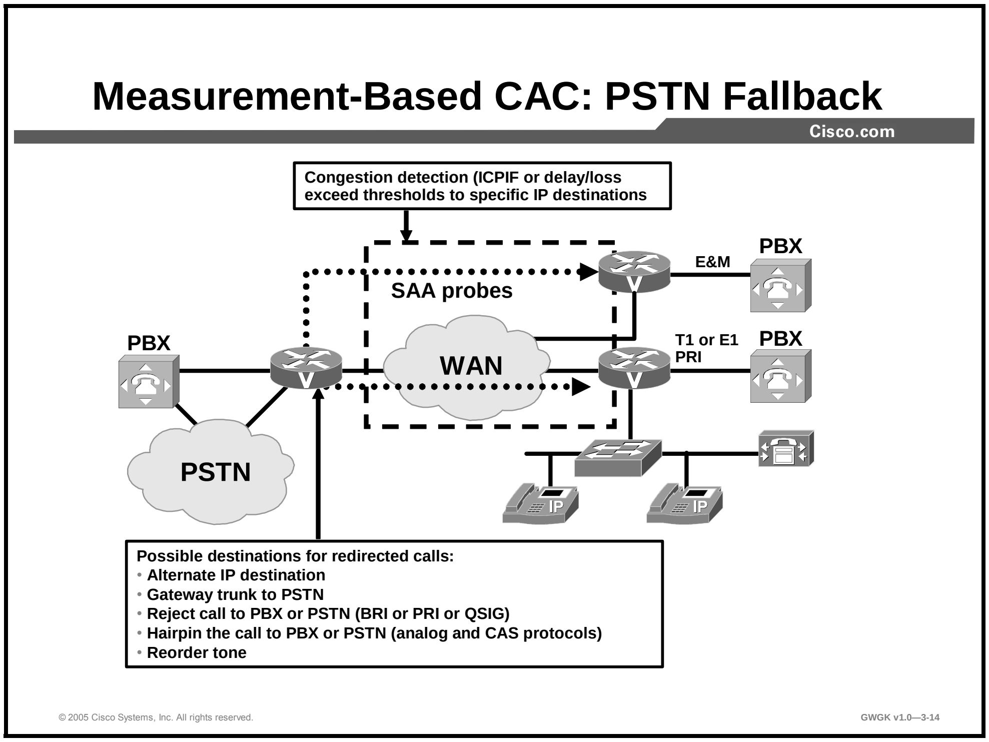
SAA Probes vs. Pings

SAA probes are similar in concept to the popular *ping* IP connectivity mechanism, but are far more sophisticated. SAA packets can be built and customized to mimic the type of traffic for which they are measuring in the network, in this case, a voice packet. A ping packet is almost by definition a best-effort packet, and even if the IP precedence is set, it does not resemble a voice packet in size or protocol. Nor will the QoS mechanisms deployed in the network classify and treat a ping packet as a voice packet. The delay and loss experienced by a ping are therefore a worst-case measure of the treatment a voice packet might be subject to while traversing the same network. With the penetration of sophisticated QoS mechanisms in network backbones, a ping becomes unusable as a practical indication of the capability of the network to carry voice.

SAA Protocol

The SAA protocol is a client-to-server protocol defined on User Data Protocol (UDP). The client builds and sends the probe, and the target device (with the RTR responder enabled) returns the probe to the sender. The SAA probes that were used for CAC go out randomly on ports selected from within the top end of the audio UDP-defined port range (16384 to 32767). The packet size they use is based on the codec the call will use. IP precedence can be set if desired, and a full RTP/UDP/IP header is used like the header a real voice packet would carry. By default, the SAA probe uses the RTP Control Protocol (RTCP) port (the odd RTP port number), but it can also be configured to use the RTP media port (the even RTP port number) if desired.

SAA was introduced on selected platforms in Cisco IOS Release 12.0(7)T. The higher-end Cisco router platforms tend to support it (for example, the Cisco 7200 and 7500 series routers), and the lower-end platforms tend not to support it (for example, the Cisco 1750 router). Neither the Cisco cable-access routers nor the IP phones support SAA probes or respond to SAA probes.



Measurement-Based CAC: PSTN Fallback

Cisco.com

Congestion detection (ICPIF or delay/loss exceed thresholds to specific IP destinations

Possible destinations for redirected calls:

- Alternate IP destination
- Gateway trunk to PSTN
- Reject call to PBX or PSTN (BRI or PRI or QSIG)
- Hairpin the call to PBX or PSTN (analog and CAS protocols)
- Reorder tone

GWGK v1.0—3-14

PSTN fallback is a per-call CAC mechanism: PSTN fallback does not busy out any trunks or provide any general indication to the attached PBX that the IP cloud cannot take calls. The CAC decision is triggered only when a call setup is attempted.

Because PSTN fallback is based on SAA probes, it has all the benefits and drawbacks of a measurement-based technique. It is unusually flexible in that it can make CAC decisions based on any type of IP network, including the Internet. All IP networks carry the SAA probe packet as they do with any other IP packet. Therefore, it does not matter if the customer backbone network comprises one or more service provider networks, the Internet, or any combination of these network types. The only requirement is that the destination device (the owner of the IP address to which the probe is sent) must support SAA responder functionality.

This destination device should be part of the customer network at the destination site, with an SP backbone in between. Therefore, PSTN fallback cannot be used directly with IP phones and PC-based VoIP application destinations, but it can be used indirectly if these destinations are behind a Cisco IOS router that can support the SAA responder. The destination device itself does not need to support the PSTN fallback feature (it is an outgoing gateway feature only). Only the SAA probe responder needs to be supported.

Calculated Planning Impairment Factor

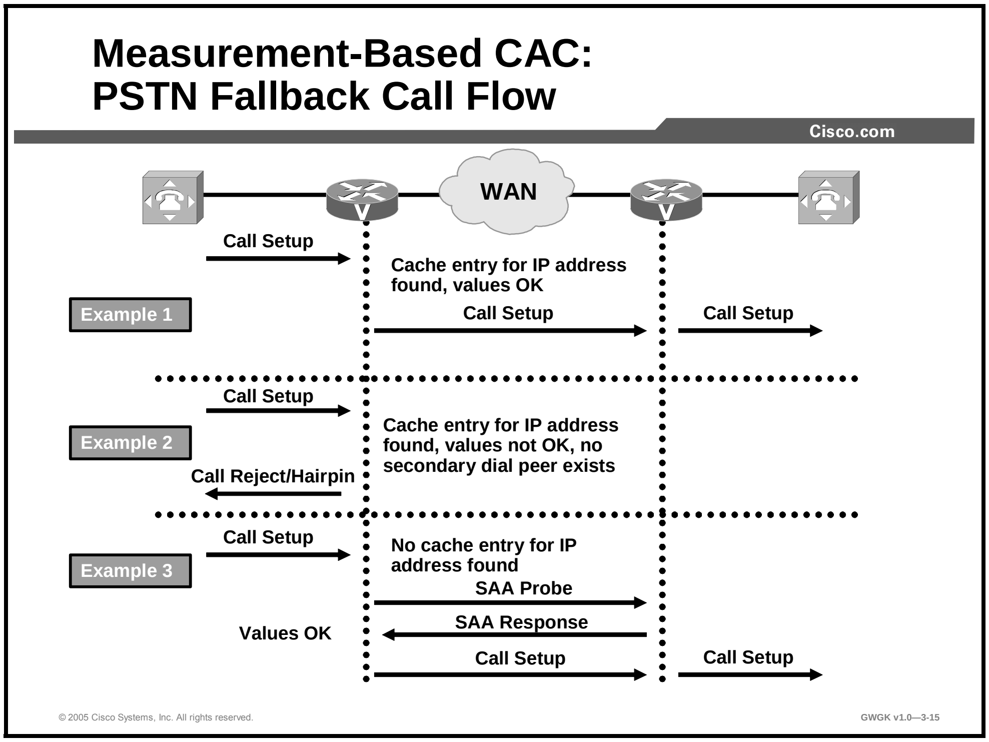
The ITU standardizes network transmission impairments in ITU G.113. This standard defines the term Calculated Planning Impairment Factor (ICPIF), which is a calculation based on network delay and packet loss figures obtained from SAA. ICPIF yields a single value that can be used as a gauge of network impairment. ITU G.113 provides the following interpretations of specific ICPIF values:

- **5:** Very good
- **10:** Good
- **20:** Adequate
- **30:** Limiting case
- **45:** Exceptional limiting case
- **55:** Customers likely to react strongly

SAA probe delay and loss information is used in calculating an ICPIF value that is then used as a threshold for CAC decisions. The CAC decisions are based either on the ITU interpretation described or on the requirements of an individual customer network.

SAA Probes Used for PSTN Fallback

As shown in the figure, when a call is attempted at the outgoing gateway, the network congestion values for the IP destination will be used to allow or reject the call. The network congestion values for delay, loss, or ICPIF are provided when the router sends an SAA probe to the IP destination the call is trying to reach. The threshold values for rejecting a call are configured at the outgoing gateway.



Measurement-Based CAC: PSTN Fallback Call Flow

Cisco.com

WAN

Example 1

Call Setup

Cache entry for IP address found, values OK

Call Setup

Call Setup

Example 2

Call Setup

Cache entry for IP address found, values not OK, no secondary dial peer exists

Call Reject/Hairpin

Example 3

Call Setup

No cache entry for IP address found

SAA Probe

SAA Response

Values OK

Call Setup

Call Setup

GWGK v1.0—3-15

IP Destination Caching

PSTN fallback does not require the static configuration of the IP destinations. The software keeps a cache of configurable size that tracks the most recently used IP destinations to which calls were attempted. If the IP destination of a new call attempt is found in the cache, the CAC decision for the call can be made immediately. (Examples 1 and 2 in the figure illustrate “call allowed” and “call rejected” scenarios, respectively.) If the entry does not appear in the cache, a new probe is started, and the call setup is suspended until the probe response arrives, as shown in example 3 in the figure. Therefore, an extra post-dial delay is imposed *only* for the first call to a new IP destination.

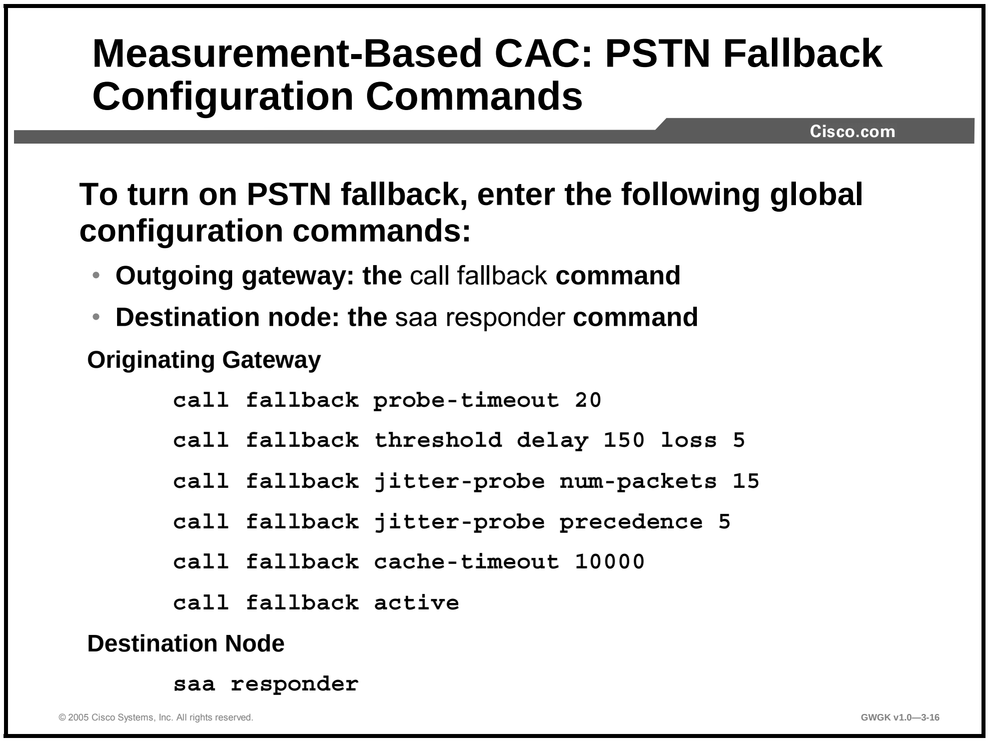
Once an IP destination has been entered into the cache, a periodic probe with a configurable timeout value will be sent to that destination to refresh the information in the cache. If no further calls are made to this IP destination, the entry will age out of the cache and probe traffic to that destination will be discontinued. Thus, PSTN fallback dynamically adjusts the probe traffic to the IP destinations that are actively seeing call activity.

SAA Probe Format

Each probe consists of multiple packets, which is a configurable parameter of the feature. The delay, loss, and ICPIF values entered into the cache for the IP destination will be averaged from all the responses.

If the call uses the G.729 and G.711 codecs, the probe packet sizes will mimic those of a voice packet for that codec. Other codecs will use G.711-like probes. In Cisco IOS software releases later than Release 12.1(3)T, other codec choices may also be supported with their own exact probes.

The IP precedence of the probe packets can also be configured to mimic the priority of a voice packet more closely. This parameter should be set equal to the IP precedence used for other voice media packets in the network.



Measurement-Based CAC: PSTN Fallback Configuration Commands

To turn on PSTN fallback, enter the following global configuration commands:

- **Outgoing gateway: the** call fallback **command**
- **Destination node: the** saa responder **command**

Originating Gateway

```
      call fallback probe-timeout 20
      call fallback threshold delay 150 loss 5
      call fallback jitter-probe num-packets 15
      call fallback jitter-probe precedence 5
      call fallback cache-timeout 10000
      call fallback active
```

Destination Node

```
      saa responder
```

PSTN Fallback Configuration

PSTN fallback configuration applies only to calls initiated by the outgoing gateway; it has no bearing on calls received by the gateway. The destination node (often the terminating gateway, but not necessarily so) should be configured with the SAA responder feature. In most networks, gateways generate calls to each other, meaning that every gateway is both an outgoing gateway and a terminating gateway. However, in some networks (for example, service provider networks), call traffic direction is occasionally one-sided, either outgoing or incoming.

PSTN fallback configuration happens at the global level, and therefore applies to all calls attempted by the gateway. You cannot selectively apply PSTN fallback only to calls initiated by certain PSTN or PBX interfaces.

To turn on PSTN fallback, enter the following global configuration commands:

- Outgoing gateway: The **call fallback** commands
- Destination node: The **saa responder** command

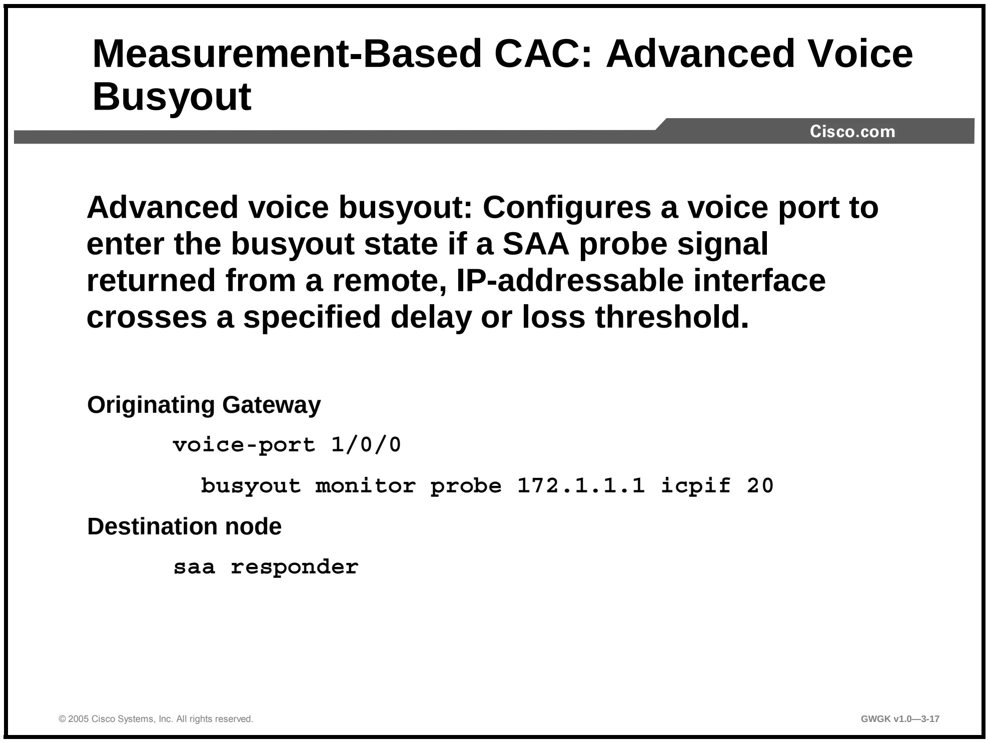
The Key Call Fallback Commands table describes these commands and their options in more detail.

Key Call Fallback Commands

Command	Purpose
`call fallback`	To enable a call request to fall back to a specific dial peer in case of network congestion, use the **call fallback** command in dial-peer configuration mode. To disable PSTN fallback for a specific dial peer, use the no form of this command. Disabling the **call fallback** command for a dial peer causes the call fallback subsystem to not fall back to the specified dial peer. Disabling the command is useful when internetworking fallback-capable H.323 gateways with the Cisco CallManager or third-party equipment that does not run fallback.
`call fallback active`	To enable a call request to fall back to alternate dial peers in case of network congestion, use the **call fallback active** command in global configuration mode. To disable PSTN fallback, use the no form of this command. Enabling the **call fallback active** command determines whether calls should be accepted or rejected based on the probing of network conditions. The **call fallback active** command checks each H.323 call request and rejects the call if the network congestion parameters are greater than the value of the configured threshold parameters of the destination. If this is the case, alternative dial peers are tried from the session application layer. Use the **call fallback threshold delay loss** or **call fallback threshold icpif** command to set the threshold parameters.
call fallback cache-size *number*	To specify the **call fallback cache-size** command for network traffic probe entries, use this command in global configuration mode. To restore the default value, use the no form of this command. The cache size can be changed only when the **call fallback active** command is not enabled. The overflow process deletes up to one-fourth of the cache entries to allow for additional calls beyond the specified cache size. The cache entries chosen for deletion are the oldest entries in the cache. The following example specifies 120 cache entries: **Router(config)# call fallback cache-size 120**

Command	Purpose
`call fallback instantaneous-value-weight` *`weight`*	To configure the call fallback subsystem to take an average from the last two probes registered in the cache for call requests, use the **call fallback instantaneous-value-weight** command in global configuration mode. To return to the default before the average was calculated, use the no form of this command. Probes that return the network congestion information are logged into the cache to determine whether the next call request is granted. When the network is regularly busy, the cache entries reflect the heavy traffic conditions. However, one probe may return with low traffic conditions, which is in contrast to normal conditions. All call requests received between the time of this probe and the next, use this entry to determine call acceptance. These calls are allowed through the network, but before the next probe is sent and received, the normal, heavy traffic conditions may have returned. The calls sent through congest the network and worsen traffic conditions. Use the **call fallback instantaneous-value-weight** command to recover gradually from heavy traffic network conditions. While the system waits for a call, probes update the cache. When a new probe is received, the weight is set and indicates how much the system is to rely upon the new probe and the previous cache entry. If the weight is set to 50 percent, the system enters a cache entry based upon an average from the new probe and the most recent entry in the cache. Call requests use this blended entry to determine acceptance. This allows the call fallback subsystem to keep conservative measures of network congestion. The configured weight applies to the new probe first. If the **call fallback instantaneous-value-weight** command is configured with the default weight of 66 percent, the new probe is given a higher value to calculate the average for the new cache entry.
`call fallback jitter-probe num-packets` *`number-of-packets`*	To specify the number of packets in a jitter probe used to determine network conditions, use the **call fallback jitter-probe num-packets** command in global configuration mode. To restore the default number of packets, use the no form of this command. A jitter probe, consisting of 2 to 50 packets, details the conditions of the network. More than one packet is used by the probe to calculate an average of delay, loss, or ICPIF. After the packets return to the probe, the probe delivers the traffic information to the cache where it is logged for call acceptance or denial. Use the **call fallback threshold delay loss** or **call fallback threshold icpif** commands to set the threshold parameters. To get a more realistic estimate on the network congestion, increase the number of packets. If more probing packets are sent, better estimates of network conditions are obtained, but the bandwidth for other network operations is negatively affected. Use fewer packets when you need to maximize bandwidth.
`call fallback jitter-probe precedence` *`precedence-value`*	To specify the priority of the jitter-probe transmission, use the **call fallback jitter-probe precedence** command in global configuration mode. To restore the default priority, use the no form of this command. Every IP packet has a precedence header. Precedence is used by various queuing mechanisms in routers to determine the priority of traffic passing through the system. Use the **call fallback jitter-probe precedence** command if there are different queuing mechanisms in your network. Enabling the **call fallback jitter-probe precedence** command sets the precedence for jitter probes to pass through your network.

Command	Purpose
`call fallback reject-cause-code` ***number***	To enable a specific call fallback reject cause code in case of network congestion, use the **call fallback reject-cause-code** command in global configuration mode. To reset the code to the default of 49, use the no form of this command. It may be necessary to set the reject cause code to a value that will allow the call processing system to reroute the call.
`call fallback threshold delay` ***delay-value*** `loss` ***loss-value***	To specify the call fallback threshold to use only packet delay and loss values, use the **call fallback threshold delay loss** command in global configuration mode. To restore the default value, use the no form of this command. Use the **call fallback threshold delay loss** command to configure parameters for voice quality. Lower values of delay and loss allow higher quality of voice. Call requests match the network information in the cache with the configured thresholds of delay and loss. The amount of delay set by the **call fallback threshold delay loss** command should not be more than half the amount of the time-to-wait value set by the **call fallback wait-timeout** command; otherwise, the threshold delay will not work correctly. Because the default value of the **call fallback wait-timeout** command is set to 300 milliseconds, the user can configure a delay of up to 150 milliseconds for the **call fallback threshold delay loss** command. If the user wants to configure a higher threshold, the time-to-wait delay has to be increased from its default by using the **call fallback wait-timeout** command.
`call fallback threshold icpif` ***threshold-value***	To specify that call fallback use the ICPIF threshold, use the call **fallback threshold icpif** command in global configuration mode. To restore the default value, use the no form of this command. Use the **call fallback threshold icpif** command to configure parameters for voice quality. A low ICPIF value allows for higher quality of voice. Call requests match the network information in the cache with the configured ICPIF threshold. If you enable the **call fallback active** command, the call fallback subsystem uses the last cache entry compared with the configured ICPIF threshold to determine whether the call is connected or denied. If you enable the **call fallback monitor** command, all calls are connected regardless of the configured threshold or voice quality. In this case, configuring the **call fallback threshold icpif** command allows you to collect network statistics for further tracking. A lower ICPIF value tolerates less delay and loss of voice packets (according to ICPIF calculations). Use lower values for higher quality of voice. Configuring a value of 34 equates to 100 percent packet loss. The ICPIF is calculated and used according to the ITU G.113 specification.



Measurement-Based CAC: Advanced Voice Busyout

Cisco.com

Advanced voice busyout: Configures a voice port to enter the busyout state if a SAA probe signal returned from a remote, IP-addressable interface crosses a specified delay or loss threshold.

Originating Gateway

```
voice-port 1/0/0
  busyout monitor probe 172.1.1.1 icpif 20
```

Destination node

```
saa responder
```

GWGK v1.0—3-17

Advanced voice busyout extends the voice busyout feature previously discussed. This feature allows the gateway to take into account the quality of the IP path in addition to its availability.

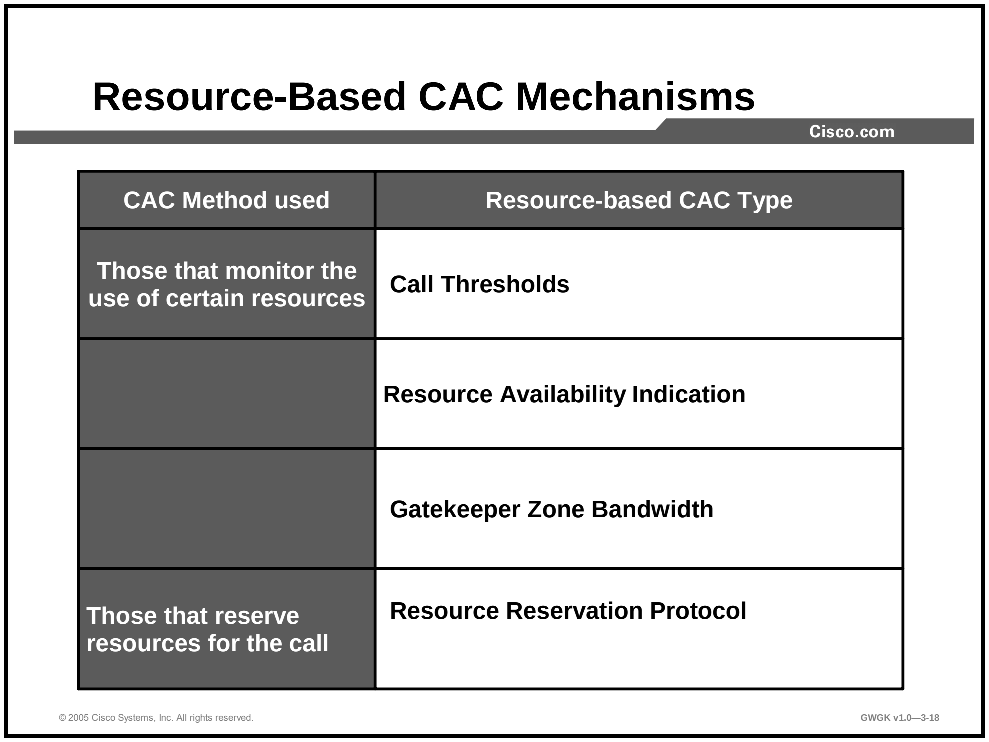
The **busyout monitor** command is applied to the voice port. It is also possible to configure busyout commands in a voice class, which can then be assigned to one or more voice ports. The following is an example of the busyout command:

```
busyout monitor probe ip-address [codec codec-type] [icpif
number | loss loss-value delay ms]
```

The **busyout monitor** command either can operate on the ICPIF value calculated by the SAA probe or can be configured to operate on specific packet-loss and delay values.

Resource-Based CAC Mechanisms

This topic discusses resource-based CAC mechanisms.



Resource-Based CAC Mechanisms

Cisco.com

CAC Method used	Resource-based CAC Type
Those that monitor the use of certain resources	Call Thresholds
	Resource Availability Indication
	Gatekeeper Zone Bandwidth
Those that reserve resources for the call	Resource Reservation Protocol

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—3-18

Resource-based CAC includes the following techniques:

- Call thresholds on H.323 gateways
- Resource availability indication
- Gatekeeper zone bandwidth
- Resource Reservation Protocol (RSVP)

Like the measurement-based CAC techniques, these techniques add visibility into the network itself in addition to the local information on the outgoing gateway that can be used for CAC.

Note Gatekeeper zone bandwidth is discussed in the "Deploying Gatekeepers" module.

Resource Calculation vs. Resource Reservation

There are two types of resource-based CAC mechanisms:

- Those that monitor the use of certain resources and calculate a value that affects the CAC decision
- Those that reserve resources for the call

The resource reservation mechanisms are the only ones that can guarantee QoS for the duration of the call. All other CAC mechanisms (local, measurement-based, and resource calculation-based) simply make a one-time decision prior to call setup that is based on knowledge of network conditions at that time.

The following resources are of interest to voice calls:

- The DS-0 timeslot on the originating and terminating TDM trunks
- DSP resources on the originating and terminating gateways
- CPU use of the nodes (typically the gateways)
- Memory use of the nodes (typically the gateways)
- Bandwidth availability on one or more links in the path the call will take

In Cisco IOS software (Release 12.2), the resource calculation CAC methods previously discussed consider the DS-0and DSP availability of the terminating gateway (Resource Availability Indication [RAI]), along with bandwidth at a high level (gatekeeper zone bandwidth management). The resource reservation mechanism (RSVP) considers only bandwidth availability.

Resource Availability Indication

RAI is an H.323v2 feature that describes a RAS message that is sent from the terminating gateway to the gatekeeper to deliver information about the current ability of the gateway to take more calls. The gatekeeper does not have knowledge of the individual resources or the type of resources that the gateway considers. It is a simple yes or no toggle indication sent by the terminating gateway to control whether subsequent voice calls are routed to the gateway.

As a CAC mechanism, RAI is unique in its ability to provide information on the terminating POTS connection. Other discussed in this topic enable CAC decisions based on local information at the outgoing gateway and on the condition of the IP cloud between the outgoing gateway and terminating gateways. No other CAC mechanism is able to look at the availability of resources to terminate the POTS call at the terminating gateway, which is what makes RAI valuable.

Because it is an indication between a gateway and gatekeeper, RAI applies only to H.323 voice networks that use a gatekeeper design. RAI is also unique in that the CAC decision is controlled by the terminating gateway. In all of the other methods, the CAC decision is controlled by the outgoing gateway or by the gatekeeper.

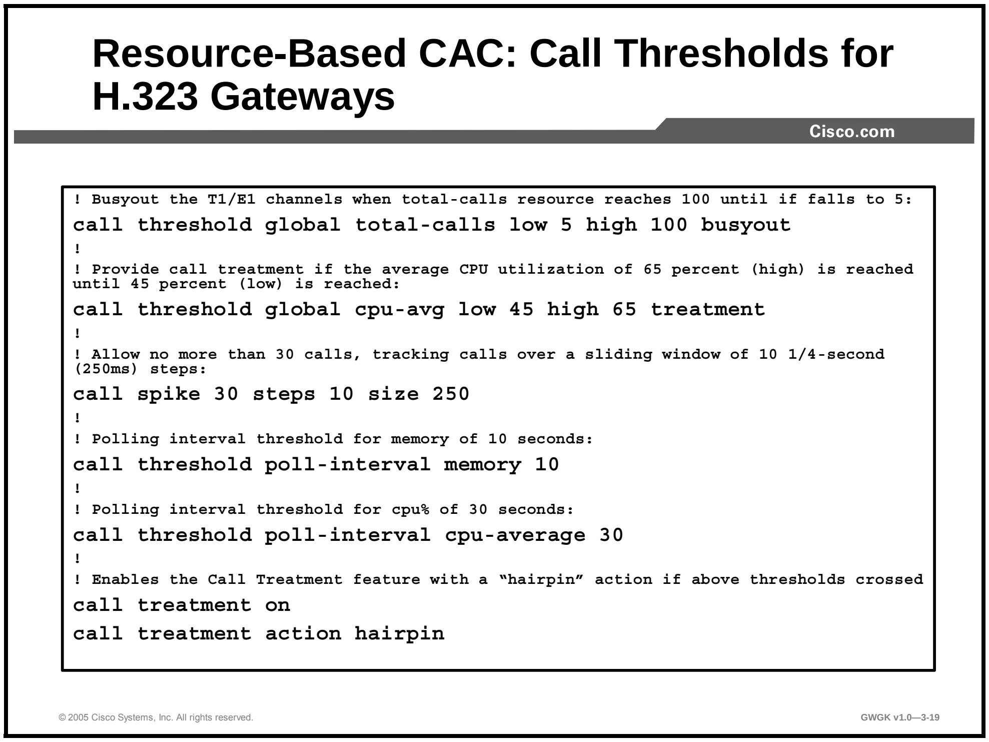
Gateway Calculation of Resources

The calculation to reach the yes or no decision is performed on the gateway. Different gateway platforms may use different algorithms. The H.323 standard does not prescribe the calculation or the resources that are to be included in the calculation. It merely specifies the RAI message format and also specifies that the gatekeeper must stop routing calls to a gateway that cannot receive further calls until the gateway informs the gatekeeper that it can take calls again.

To gauge resource availability for a call for the Cisco 2600 and 3600 series routers, the calculation algorithm considers each call as a unit according to the following formula:

- Each free DS-0 is a unit
- Each high-complexity DSP is two units
- Each medium-complexity DSP is four units

RAI is calculated per platform, not per T1/E1 interface or per card (which could mean per network module, or specifically per NMM-HDV in the case of the Cisco 2600 and 3600 series routers). Only DS-0s that are reachable through a VoIP dial peer are included in the calculation.



Resource-Based CAC: Call Thresholds for H.323 Gateways

Cisco.com

```
! Busyout the T1/E1 channels when total-calls resource reaches 100 until if falls to 5:
call threshold global total-calls low 5 high 100 busyout
!
! Provide call treatment if the average CPU utilization of 65 percent (high) is reached
until 45 percent (low) is reached:
call threshold global cpu-avg low 45 high 65 treatment
!
! Allow no more than 30 calls, tracking calls over a sliding window of 10 1/4-second
(250ms) steps:
call spike 30 steps 10 size 250
!
! Polling interval threshold for memory of 10 seconds:
call threshold poll-interval memory 10
!
! Polling interval threshold for cpu% of 30 seconds:
call threshold poll-interval cpu-average 30
!
! Enables the Call Treatment feature with a "hairpin" action if above thresholds crossed
call treatment on
call treatment action hairpin
```

GWGK v1.0—3-19

Prior to the CAC for H.323 VoIP gateways feature, gateways did not have a mechanism to gracefully prevent calls from entering them when certain resources were not available to process the call. This inability caused the new call to fail with unreported behavior and potentially caused the calls that were in progress to have quality-related issues.

This feature provides the ability to support resource-based call admission control processes. These resources include system resources such as CPU, memory, call volume, and other interface.

If system resources are not available to admit the call, two kinds of actions are provided:

- System denial, which busies out all of T1 or E1
- Per call denial, which disconnects, hairpins, or plays a message or tone

If the interface-based resource is not available to admit the call, the call is dropped from the session protocol (such as H.323).

User-Selected Call Admission Controls

The CAC for H.323 VoIP gateways feature allows a user to configure thresholds for local resources, including memory and CPU resources. With the **call threshold** command, a user is allowed to configure two thresholds, one high and one low, for each resource. Call treatment is triggered when the current value of a resource goes beyond the configured high. The call treatment remains in effect until the current resource value falls below the configured low. Having high and low thresholds prevents call admission flapping.

With the **call spike** command, a user is allowed to configure the limit for incoming calls during a specified time. A call spike is the term for when a large number of incoming calls arrive from the PSTN in a very short period of time (for example, 100 incoming calls in 10 ms).

With the **call treatment** command, users are allowed to select how the call should be treated when local resources are not available to handle the call. For example, when the current resource value for any one of the configured triggers for call threshold has exceeded the configured threshold, the call treatment choices are as follows:

- **TDM hairpinning:** Hairpins the calls through the POTS dial peer
- **Reject:** Disconnects the call
- **Play message or tone:** Plays a configured message or tone to the user

Configuration Tasks

The following are configuration tasks for the CAC and PSTN fallback features. Each task in the list is identified as either required or optional.

- Configuring call spike (required)
- Configuring call threshold (required)
- Configuring call threshold poll interval (optional)
- Configuring call treatment (optional)
- Configuring PSTN fallback (required)

Configuring Call Spike

To configure the limit for the number of incoming calls at a time, enter the following command in global configuration mode:

```
Router(config)# call spike call-number [steps number-of-steps
size milliseconds]
```

The **call spike call-number** command configures the limit for the number of incoming calls in a short period of time.

Configuring Call Threshold

To configure the call threshold, use the following command in global configuration mode:

```
Router(config)# call threshold {global trigger-name |
interface interface-name interface-number int-calls} low value
high value [busyout | treatment]
```

The **call threshold** command enables a resource and defines associated parameters. Action is enabled when the resource cost goes beyond the *high value* option and is not disabled until the resource cost drops below the *low value*.

Configuring Call Threshold Poll Interval

To configure the interval at which the call threshold is polled, use the following command in global configuration mode:

```
Router(config)# call threshold poll-interval {cpu-average |
memory} seconds
```

The **call threshold poll-interval** command enables a polling interval threshold for CPU or memory.

Configuring Call Treatment

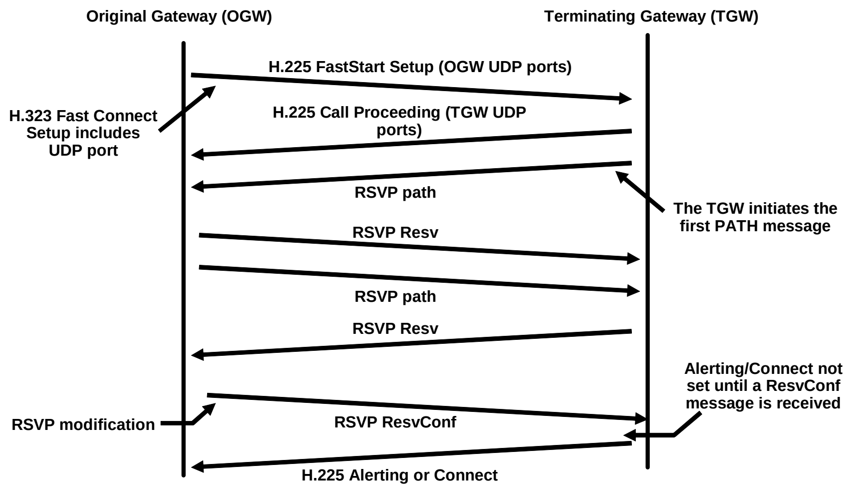
To configure the call treatment, use the following command in global configuration mode:

```
Router(config)# call treatment {on | action action [ value] |
cause-code cause-code | isdn-reject value}
```

The **call treatment** command configures how calls should be processed when local resources are unavailable and indicates whether the call should be disconnected (with a cause code), hairpinned, or play a message or busy tone to the user.

Resource-Based CAC: RSVP

Cisco.com



Original Gateway (OGW)

Terminating Gateway (TGW)

H.225 FastStart Setup (OGW UDP ports)

H.323 Fast Connect Setup includes UDP port

H.225 Call Proceeding (TGW UDP ports)

RSVP path

The TGW initiates the first PATH message

RSVP Resv

RSVP path

RSVP Resv

Alerting/Connect not set until a ResvConf message is received

RSVP modification

RSVP ResvConf

H.225 Alerting or Connect

GWGK v1.0—3-20

Resource Reservation Protocol

RSVP is the only CAC mechanism that makes a bandwidth reservation and does not make a call admission decision based on a “best guess look-ahead” before the call is set up. This gives RSVP the unique advantage of not only providing CAC for voice but also guaranteeing the QoS against changing network conditions for the duration of the call.

RSVP Reservation for a Voice Call

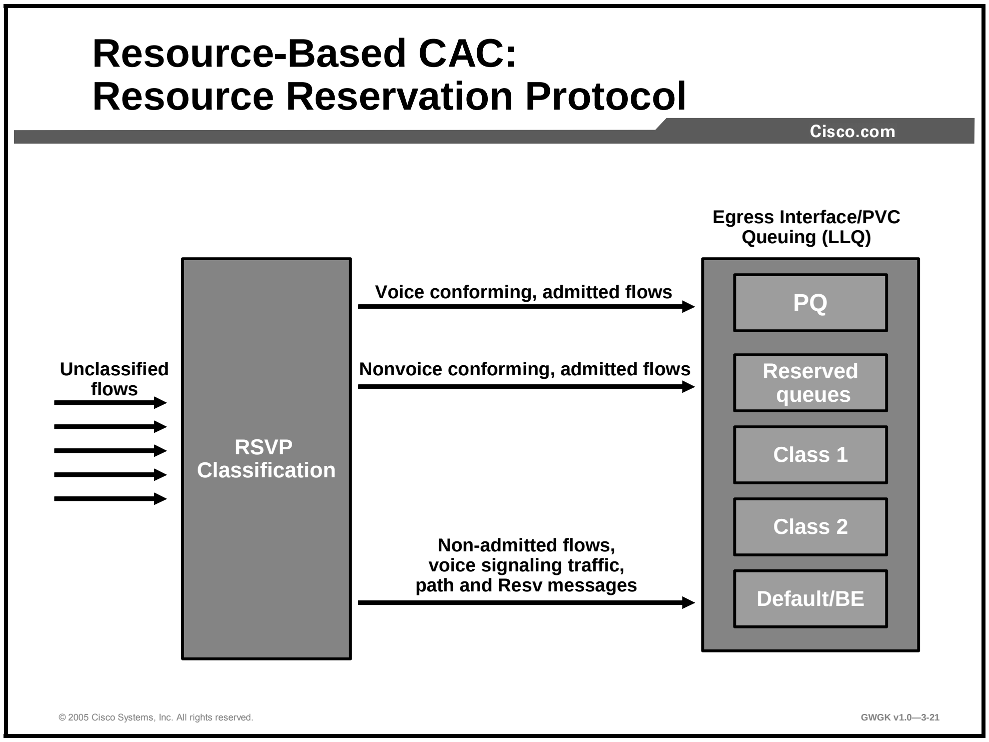
The figure shows a call flow of the H.323 call setup messages and the RSVP reservation messages.

The H.323 setup is suspended before the destination phone starts ringing, an action that is triggered by the H.225 alerting message,. The RSVP reservation is made in both directions because a voice call requires a two-way speech path and, therefore, bandwidth in both directions. The terminating gateway ultimately makes the CAC decision based on whether both reservations succeed. Then, the H.323 state machine continues either with an H.225 alerting/connect message (the call is allowed and proceeds) or with an H.225 reject/release message (the call is denied). The RSVP reservation is in place by the time the destination phone starts ringing and the caller hears ringback.

RSVP has the following important differences from other CAC methods discussed in this lesson:

- The ability to maintain QoS for the duration of the call.
- Awareness of topology. In concept, the RSVP reservation is installed on every interface the call will traverse through the network (exceptions to this are discussed in later sections). Therefore, RSVP will ensure bandwidth over every segment without needing to know the actual bandwidth provisioning on an interface nor the path on which the routing protocols will direct the packets. (RSVP adjusts automatically to network configuration changes, and no manual calculations are necessary to keep different aspects of the configuration synchronized.)

RSVP is an end-to-end reservation that works per call and only has visibility for that call. It is unaware of how many other calls are active from a site or across an interface, or of the source or destination of any other call. Therefore, there is no way to configure aggregate levels of CAC with RSVP, such as the site-to-site CAC that is possible with gatekeeper zone bandwidth control.



Resource-Based CAC: Resource Reservation Protocol

Cisco.com

Egress Interface/PVC Queuing (LLQ)

Unclassified flows

RSVP Classification

Voice conforming, admitted flows

Nonvoice conforming, admitted flows

Non-admitted flows, voice signaling traffic, path and Resv messages

PQ

Reserved queues

Class 1

Class 2

Default/BE

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—3-21

Classification for Voice Packets into LLQ

Low latency queuing (LLQ) is one of the important Cisco QoS mechanisms that is used to ensure quality for voice because it prioritizes voice packets over data packets at the router egress interface. For this process to work, voice packets must be classified such that they are placed in the priority queue (PQ) portion of LLQ. Traditionally, this is accomplished with access control list (ACL) classification, where the Transmission Control Protocol (TCP) (signaling) and UDP (media) ports are matched to funnel voice packets into the appropriate queues.

As a general Cisco IOS feature, RSVP has its own set of reserved queues within weighted fair queuing (WFQ) for traffic with RSVP reservations. Though these queues have a low weight, they are separate from the PQ. Packets in reserved queues do not get priority over packets from other queues except because of their low weight. It is known that this treatment (a low weight queue inside WFQ) is insufficient for voice quality over a congested interface with several different flows of traffic. Therefore, when RSVP is configured for a voice call, the voice packets need to be classified into the PQ. RSVP data flow packets should not be classified into the PQ in this case.

RSVP uses a profile to determine whether a flow of packets is a voice flow. The profile considers packet sizes, arrival rates, and other parameters, and a packet flow conforming to the parameters is considered a voice flow. If it does not conform to those parameters, it is considered a nonvoice flow, which including both data and video. The internal profile is tuned so that all voice traffic originating from a Cisco IOS gateway will fall within the parameters and will therefore be considered a voice flow without needing extra configuration. For third-party applications such as NetMeeting, the profile may need to be tuned to pick up that kind of traffic. The slide figure shows how this is accomplished.

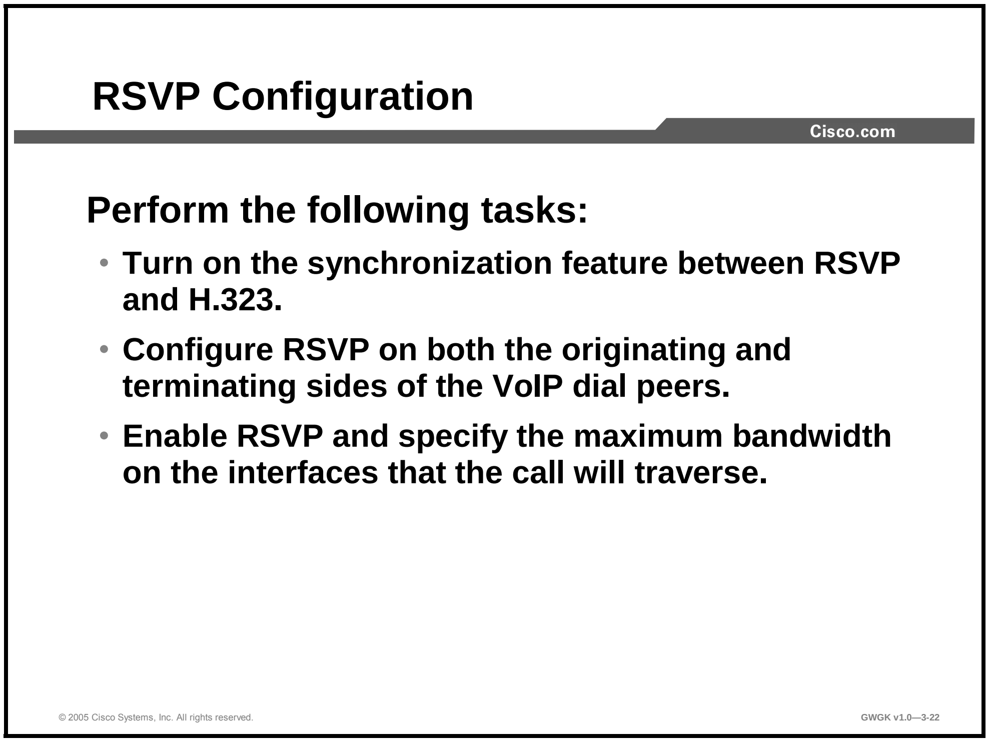
RSVP is the first egress interface classifier to examine an arriving packet.

If RSVP considers the packet to be a voice flow, the packets will be put into the PQ portion of LLQ.

If the flow does not conform to the voice profile but is nevertheless an RSVP-reserved flow, it will be placed into the normal RSVP reserved queues.

If the flow is neither a voice flow nor a data RSVP flow, the other egress interface classifiers (such as ACLs and “match” statements within a class map) will attempt to classify the packet for queuing.

It is important to note that RSVP will classify only voice bearer traffic, not signaling traffic. One of the other classification mechanisms such as ACLs or differentiated services code points (DSCPs) must still be used to classify the voice signaling traffic if any treatment better than best-effort is desired for that traffic. If the decision is left up to RSVP alone, signaling traffic will be considered best-effort traffic, as shown in the figure.



RSVP Configuration

Cisco.com

Perform the following tasks:

- **Turn on the synchronization feature between RSVP and H.323.**
- **Configure RSVP on both the originating and terminating sides of the VoIP dial peers.**
- **Enable RSVP and specify the maximum bandwidth on the interfaces that the call will traverse.**

GWGK v1.0—3-22

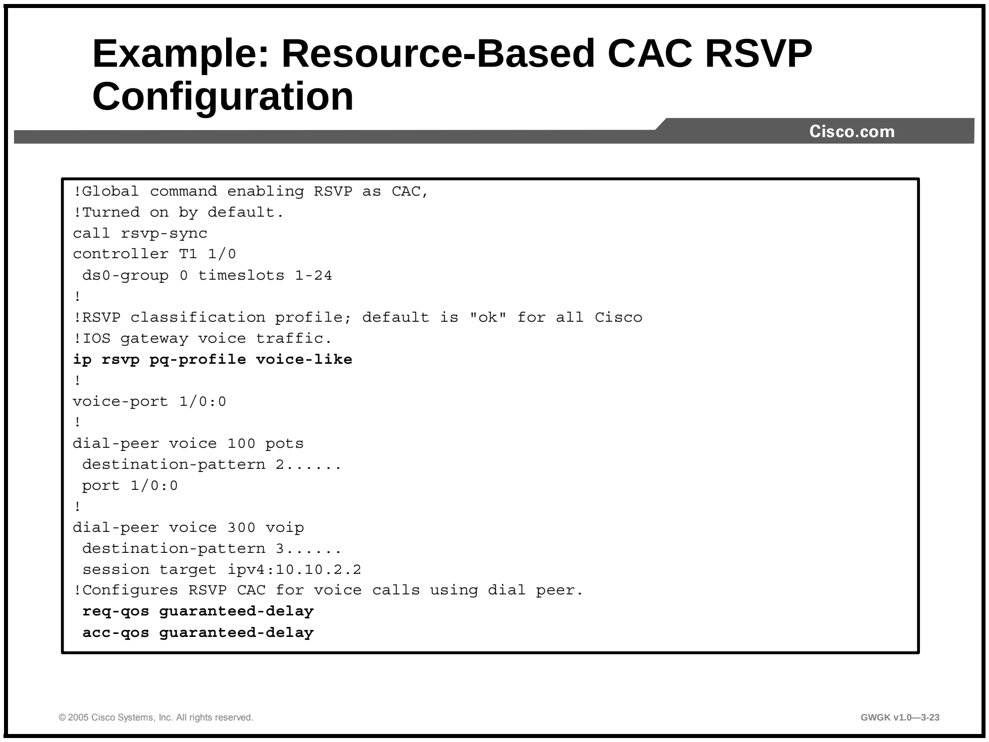
RSVP Configuration

Perform the following three tasks on a gateway to originate or terminate voice traffic using RSVP:

Step 1 Turn on the synchronization feature between RSVP and H.323. This is a global command and is turned on by default when Cisco IOS Release 12.1(5)T or later is loaded.

Step 2 Configure RSVP on both the originating and terminating sides of the VoIP dial peers. Configure both the requested QoS (req-qos) and the acceptable QoS (acc-qos) guaranteed-delay commands for RSVP to act as a CAC mechanism. (Other combinations of parameters may lead to a reservation, but CAC will not.)

Step 3 Enable RSVP and specify the maximum bandwidth on the interfaces that the call will traverse.



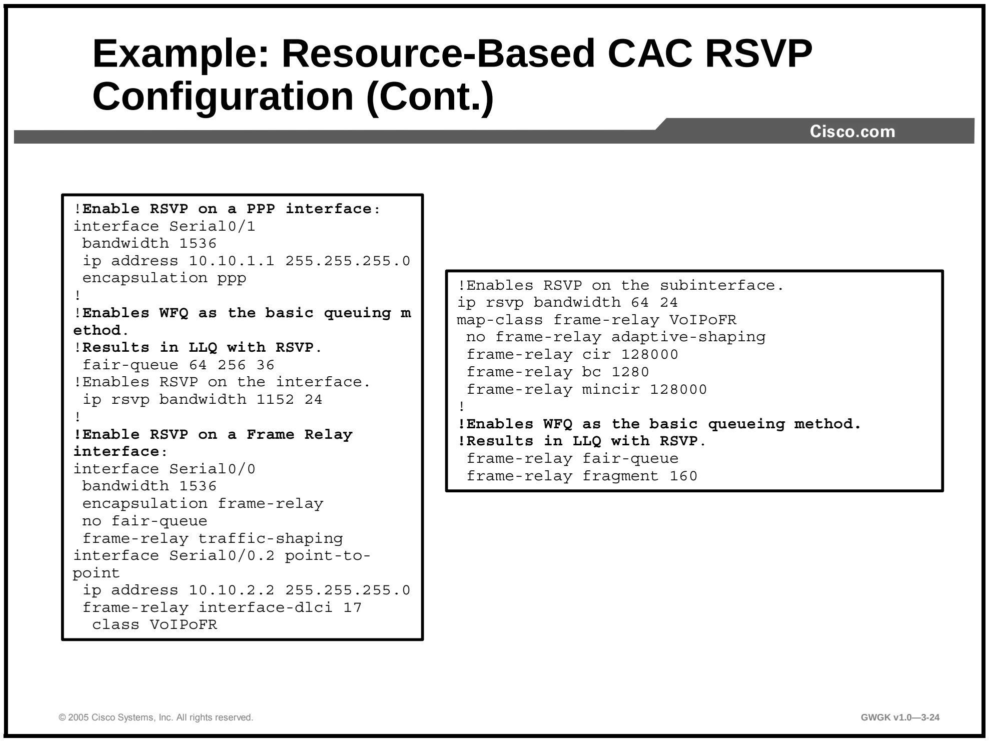
Example: Resource-Based CAC RSVP Configuration

Cisco.com

```
!Global command enabling RSVP as CAC,
!Turned on by default.
call rsvp-sync
controller T1 1/0
 ds0-group 0 timeslots 1-24
!
!RSVP classification profile; default is "ok" for all Cisco
!IOS gateway voice traffic.
ip rsvp pq-profile voice-like
!
voice-port 1/0:0
!
dial-peer voice 100 pots
 destination-pattern 2......
 port 1/0:0
!
dial-peer voice 300 voip
 destination-pattern 3......
 session target ipv4:10.10.2.2
!Configures RSVP CAC for voice calls using dial peer.
 req-qos guaranteed-delay
 acc-qos guaranteed-delay
```

GWGK v1.0—3-23

The screen capture shows an example of a resource-based CAC RSVP configuration. The commands to enable RSVP CAC are highlighted in the figure.



Example: Resource-Based CAC RSVP Configuration (Cont.)

Cisco.com

```
!Enable RSVP on a PPP interface:
interface Serial0/1
 bandwidth 1536
 ip address 10.10.1.1 255.255.255.0
 encapsulation ppp
!
!Enables WFQ as the basic queuing m
ethod.
!Results in LLQ with RSVP.
 fair-queue 64 256 36
!Enables RSVP on the interface.
 ip rsvp bandwidth 1152 24
!
!Enable RSVP on a Frame Relay
interface:
interface Serial0/0
 bandwidth 1536
 encapsulation frame-relay
 no fair-queue
 frame-relay traffic-shaping
interface Serial0/0.2 point-to-
point
 ip address 10.10.2.2 255.255.255.0
 frame-relay interface-dlci 17
  class VoIPoFR
```

```
!Enables RSVP on the subinterface.
ip rsvp bandwidth 64 24
map-class frame-relay VoIPoFR
 no frame-relay adaptive-shaping
 frame-relay cir 128000
 frame-relay bc 1280
 frame-relay mincir 128000
!
!Enables WFQ as the basic queueing method.
!Results in LLQ with RSVP.
 frame-relay fair-queue
 frame-relay fragment 160
```

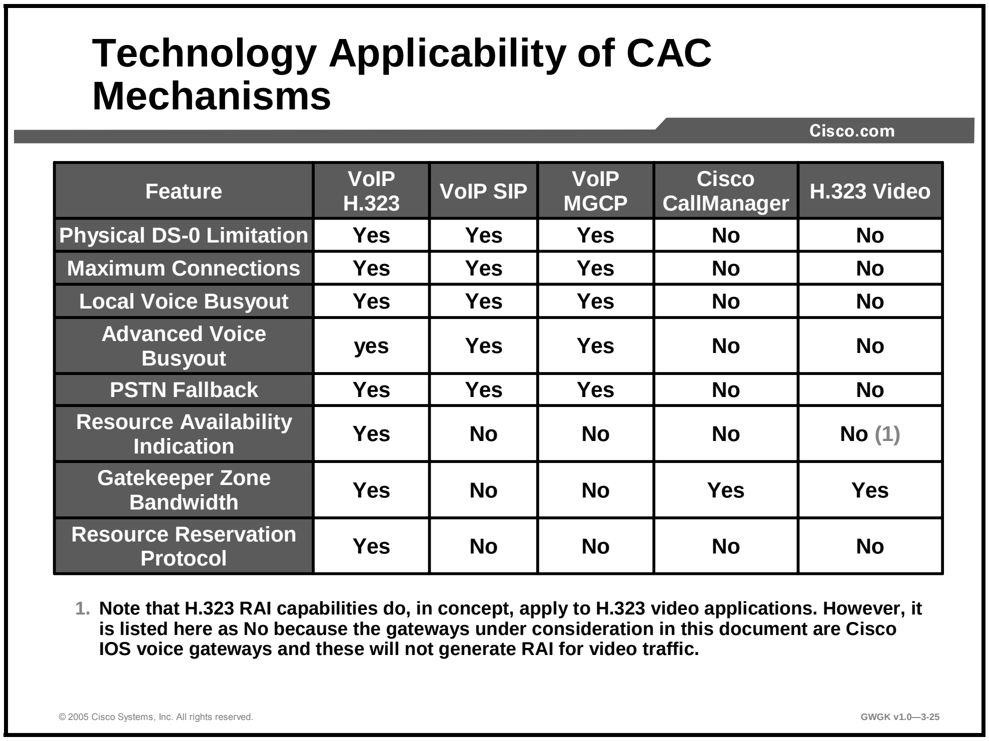
GWGK v1.0—3-24

The screen capture shows another example of a resource-based CAC RSVP configuration. This example shows two ways to configure CAC features so that the result is LLQ with RSVP:

- Enable RSVP on a PPP interface with WFQ enabled as the basic queuing method
- Enable RSVP on a Frame Relay interface with WFQ enabled as the basic queuing method

Evaluating CAC Mechanisms

This topic describes the CAC mechanisms that are available with each gateway protocol and the considerations for choosing which CAC mechanism to implement.



Technology Applicability of CAC Mechanisms

Cisco.com

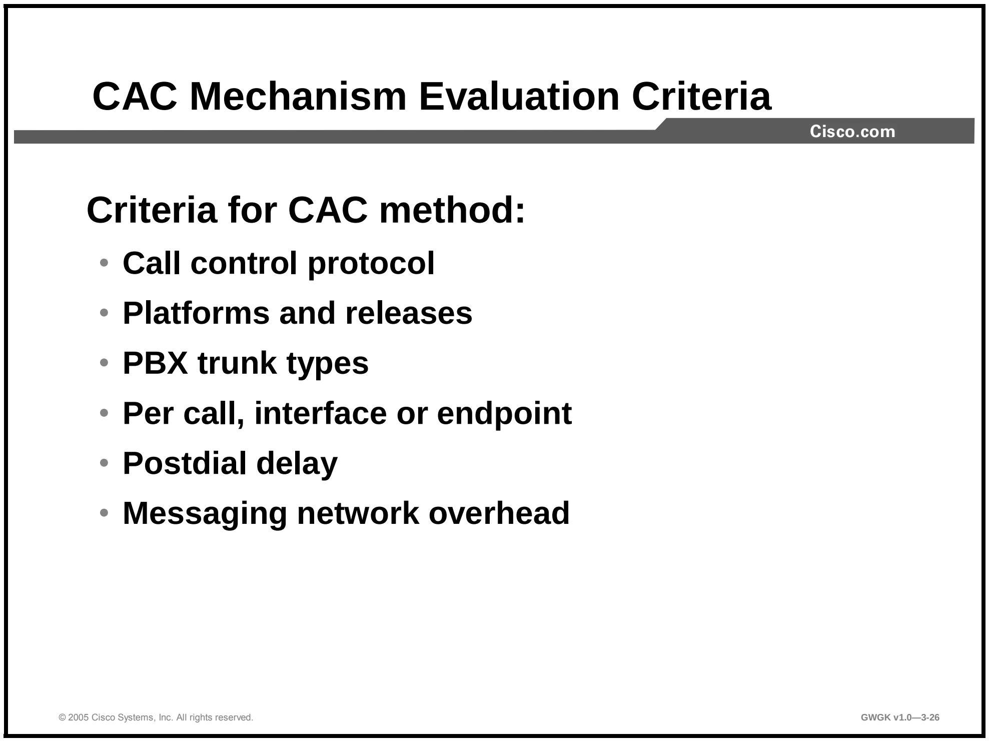
Feature	VoIP H.323	VoIP SIP	VoIP MGCP	Cisco CallManager	H.323 Video
Physical DS-0 Limitation	Yes	Yes	Yes	No	No
Maximum Connections	Yes	Yes	Yes	No	No
Local Voice Busyout	Yes	Yes	Yes	No	No
Advanced Voice Busyout	yes	Yes	Yes	No	No
PSTN Fallback	Yes	Yes	Yes	No	No
Resource Availability Indication	Yes	No	No	No	No (1)
Gatekeeper Zone Bandwidth	Yes	No	No	Yes	Yes
Resource Reservation Protocol	Yes	No	No	No	No

1. Note that H.323 RAI capabilities do, in concept, apply to H.323 video applications. However, it is listed here as No because the gateways under consideration in this document are Cisco IOS voice gateways and these will not generate RAI for video traffic.

GWGK v1.0—3-25

Technology Applicability of CAC Mechanisms

When you are considering the various features that are available to solve a particular design requirement such as CAC, it is helpful to eliminate immediately the mechanisms that do not apply to the network technology under consideration. The table in the figure summarizes the voice technologies to which the various CAC features apply.



CAC Mechanism Evaluation Criteria

Cisco.com

Criteria for CAC method:

- **Call control protocol**
- **Platforms and releases**
- **PBX trunk types**
- **Per call, interface or endpoint**
- **Postdial delay**
- **Messaging network overhead**

GWGK v1.0—3-26

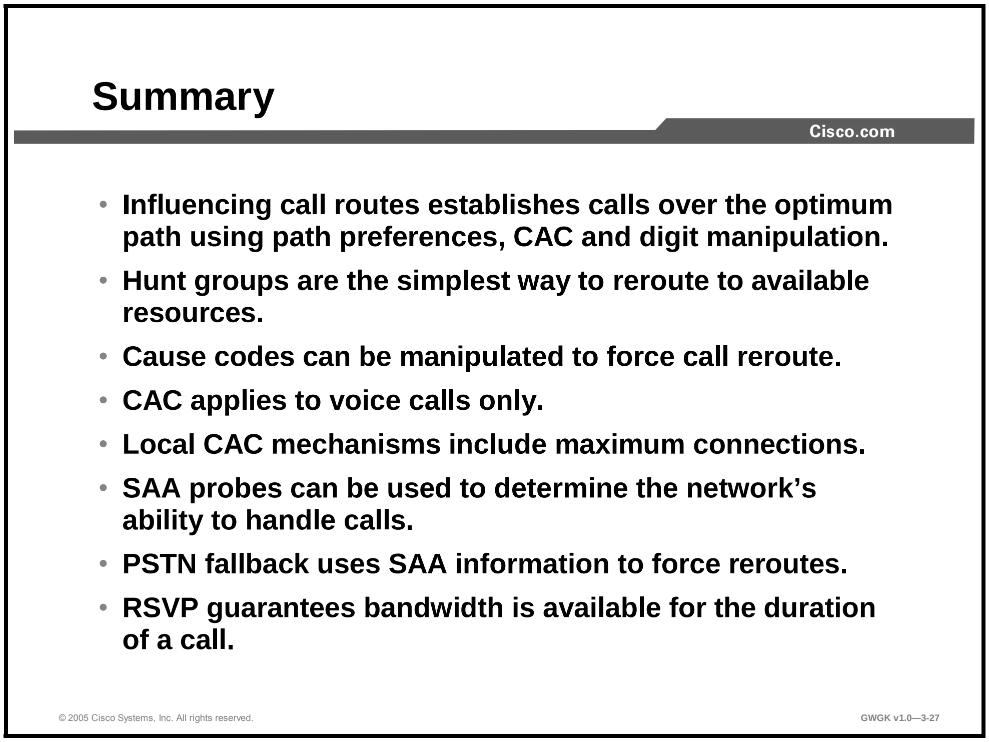
CAC Mechanism Evaluation Criteria

When you are determining the appropriate CAC method to select, the criteria should be based on finding the least complex method that will meet your minimum requirements. For most enterprise networks, local CAC mechanisms such as maximum connections or, for larger networks, gatekeeper zone bandwidth, provide this functionality.

For most gateways, CPU usage or the number of simultaneous call setups is not a factor on call quality. The biggest impact for enterprise customers is available bandwidth, which is most effectively managed with a gatekeeper. The other methods are typically used in service provider networks or in very large enterprise networks. They can also be useful if available resources are constrained.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

Cisco.com

- Influencing call routes establishes calls over the optimum path using path preferences, CAC and digit manipulation.
- Hunt groups are the simplest way to reroute to available resources.
- Cause codes can be manipulated to force call reroute.
- CAC applies to voice calls only.
- Local CAC mechanisms include maximum connections.
- SAA probes can be used to determine the network's ability to handle calls.
- PSTN fallback uses SAA information to force reroutes.
- RSVP guarantees bandwidth is available for the duration of a call.

GWGK v1.0—3-27

References

For additional information, refer to these resources:

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/vcltrunk.htm#wp1052598

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) What is the primary purpose of TEHO? (Source:)

A) to make use of H.323 gateways
B) to make use of gatekeepers
C) to reduce toll charges
D) to make use of Cisco CallManager

Q2) Which CAC mechanism guarantees that bandwidth is available for the duration of a call? (Source:)

A) gatekeeper zone bandwidth
B) RSVP
C) maximum connections
D) RAI

Q3) Hunt groups are driven by which element? (Source:)

A) rotary groups
B) dial peers
C) voice ports
D) preference

Q4) Cisco CallManager uses _________ for TEHO functionally. (Source:)

A) route-lists
B) route-group and route-patterns
C) route-list, route-group, and route patterns
D) SRST fallback

Q5) Which CAC mechanisms make use of SAA probes? (Choose two.) (Source:)

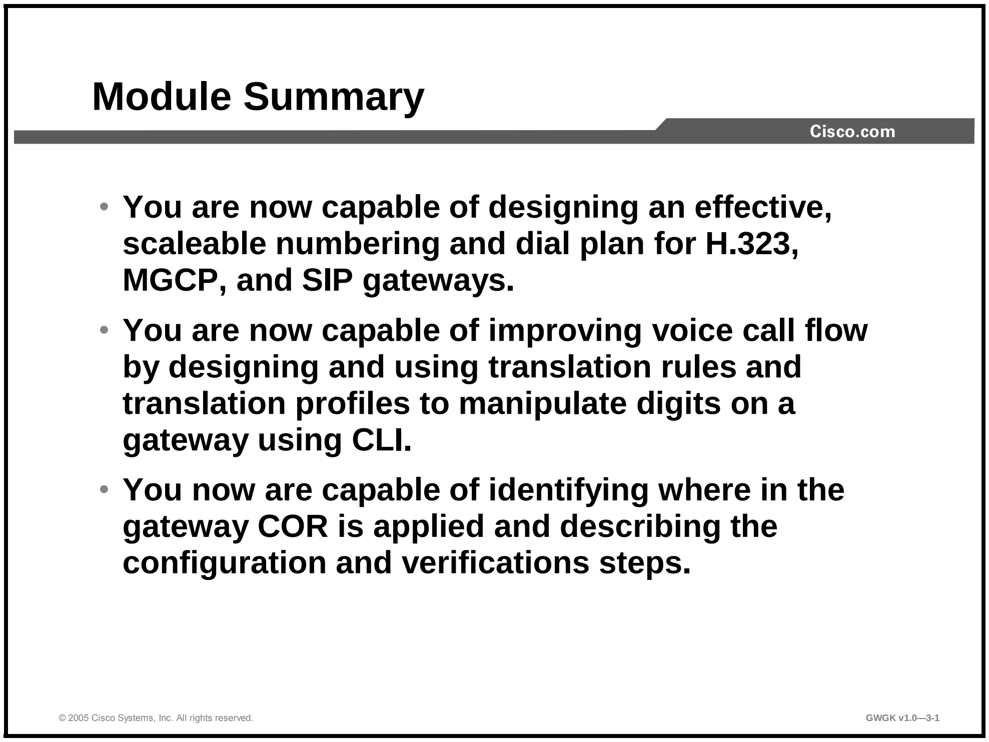
A) RSVP
B) PSTN fallback
C) RAI
D) advanced voice busyout

Lesson Self-Check Answer Key

Q1)	C
Q2)	B
Q3)	D
Q4)	C
Q5)	B, D

Module Summary

This topic summarizes the key points discussed in this module.



Module Summary

Cisco.com

- You are now capable of designing an effective, scaleable numbering and dial plan for H.323, MGCP, and SIP gateways.
- You are now capable of improving voice call flow by designing and using translation rules and translation profiles to manipulate digits on a gateway using CLI.
- You now are capable of identifying where in the gateway COR is applied and describing the configuration and verifications steps.

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—3-1

This module discussed what a dial plan is and described the critical elements that are required for implementing a scalable voice network. Having this knowledge is key in knowing how to manipulate voice traffic.

References

For additional information, refer to these resources:

- The “Dial Plan” chapter of *Cisco IP Telephony Solution Reference Network Design (SRND) for Cisco CallManager 4.0*. http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_chapter09186a00802c37f9.html.
- The “Dial Plan Overview” section of *Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*. http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a0080080aec.html#wp1241391.
- The “Assigning Translation Profiles to Inbound Dial Peers” section of *VoIP Gateway Trunk and Carrier Based Routing Enhancements*. http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00800b5dbf.html#wp1032356.
- The “Configuring Dial Plans, Dial Peers, and Digit Manipulation” chapter of *Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*. http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a0080080aec.html.

- Technical Support for Call Routing and Dial Plans. http://www.cisco.com/en/US/tech/tk652/tk90/tsd_technology_support_protocol_home.htm.

- *Voice Translation Rules*. http://www.cisco.com/en/US/tech/tk652/tk90/technologies_tech_note09186a0080325e8e.shtml.

- *Cisco IOS SRST Version 3.2 System Administrator Guide*. http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_administration_guide_book09186a00802d3ca5.html.

- *Trunk-Management Features*. http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/vcltrunk.htm#wp1052598,

Module 4

Implementing Advanced Gateway Features

Overview

This module discusses configuring Cisco Survivable Remote Site Telephony (SRST), deploying digital signal processor (DSP) farms to employ conferencing, transcoding, and media termination point (MTP), and using Tool Command Language (TCL) to offer interactive voice response (IVR) on a gateway. This module will give you a better understanding of and hands-on experience with deploying these technologies.

Module Objectives

Upon completing this module, you will be able to configure advanced voice gateway features. This ability includes being able to meet these objectives:

- Configure Cisco SRST on a remote site gateway in a centralized call-processing model
- Configure DSP farming resources to support hardware conferencing, transcoding, and MTP services on a gateway
- Configure TCL scripts on a gateway

Lesson 1

Deploying SRST

Overview

One critical element to centralized call processing modules is the need to have support for backup telephony services in the event of an IP WAN outage. Survivable Remote Site Telephony (SRST) is a solution that provides call-processing backup in case Cisco CallManager becomes unavailable or the IP WAN goes down.

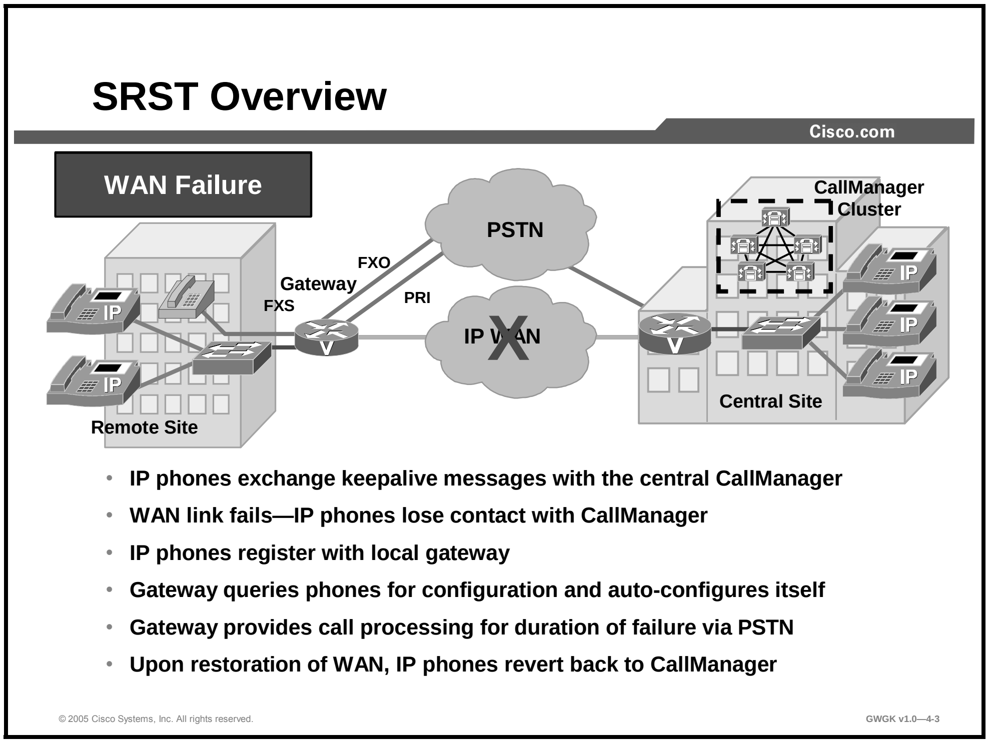
Objectives

Upon completing this lesson, you will be able to configure SRST on a remote site gateway in a centralized call-processing model. This ability includes being able to meet these objectives:

- Describe the function and operation of SRST
- Describe dial-plan considerations in SRST
- Configure SRST to provide redundancy
- Configure advanced SRST features
- Troubleshoot SRST

SRST Overview

This topic describes gives an overview of how SRST operates.



SRST Overview

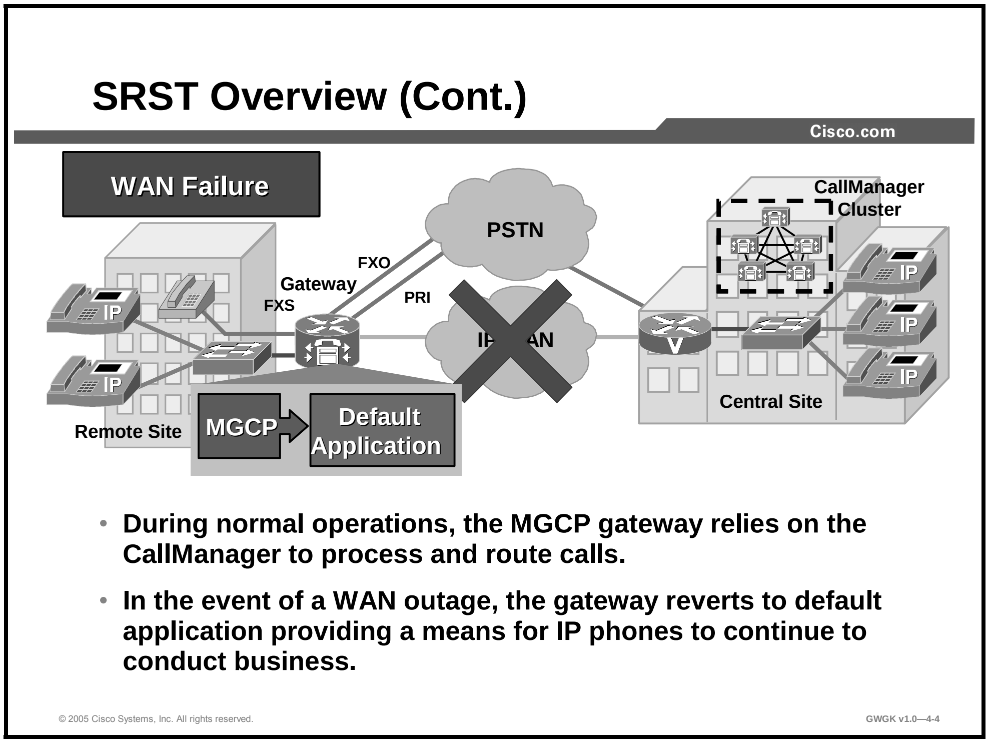
- IP phones exchange keepalive messages with the central CallManager
- WAN link fails—IP phones lose contact with CallManager
- IP phones register with local gateway
- Gateway queries phones for configuration and auto-configures itself
- Gateway provides call processing for duration of failure via PSTN
- Upon restoration of WAN, IP phones revert back to CallManager

GWGK v1.0—4-3

The Cisco SRST software operates by taking advantage of the keepalive packets coming from both the centralized Cisco CallManager cluster and the local IP phones. During normal operations, the Cisco CallManager receives keepalive packets from the IP phones. Cisco CallManager performs call setup, call processing, call maintenance, and call termination. The remote site router is configured for SRST, but it has no awareness of the IP phones when it is in normal mode.

When the WAN link fails, the Cisco IP Phones detect that they are no longer receiving keepalive packets from the Cisco CallManager. The IP phones then register with the router, which queries the phone about its configuration and then autoconfigures itself. In this instance, the SRST is automatically activated and builds a local database of all IP phones attached to it (up to its stated maximum). The IP phones are configured to query the router as a backup call-processing source when the central Cisco CallManager does not acknowledge keepalive packets. The SRST router now performs call setup, call processing, call maintenance, and call termination. The IP phones indicate on their display that they are in “CM Fallback Operating” mode for the duration of the failure.

When the WAN link is restored, the IP phones detect keepalive packets from the central Cisco CallManager and revert to it for primary call setup and processing. As IP phones re-home to the Cisco CallManager, the SRST router purges its call-processing database and reverts to standby mode. Calls in progress are not interrupted because they are managed by the gateway function. Phones in use during WAN link recovery re-home to the Cisco CallManager after they return to idle state.



SRST Overview (Cont.)

- During normal operations, the MGCP gateway relies on the CallManager to process and route calls.
- In the event of a WAN outage, the gateway reverts to default application providing a means for IP phones to continue to conduct business.

Media Gateway Control Protocol (MGCP) gateways require additional consideration when you are implementing SRST. In addition to being configured for SRST, the gateway also must be configured for MGCP fallback. The command **ccm-manager fallback-mgcp** causes the gateway to fall back and provide call-processing services if connectivity is lost between the gateway and all Cisco CallManager servers. An additional command, **call application alternate default**, is also required. The **call application alternate default** command triggers the gateway into using its default call processing in the event that the currently used application fails. For example, a gateway configured to use MGCP as its primary call processing fails, the gateway will reconfigure itself to use dial peers to process telephony calls and handle public switched telephone network (PSTN) traffic. The default portion of the gateway is simply falling back its default dial-peer call process application.

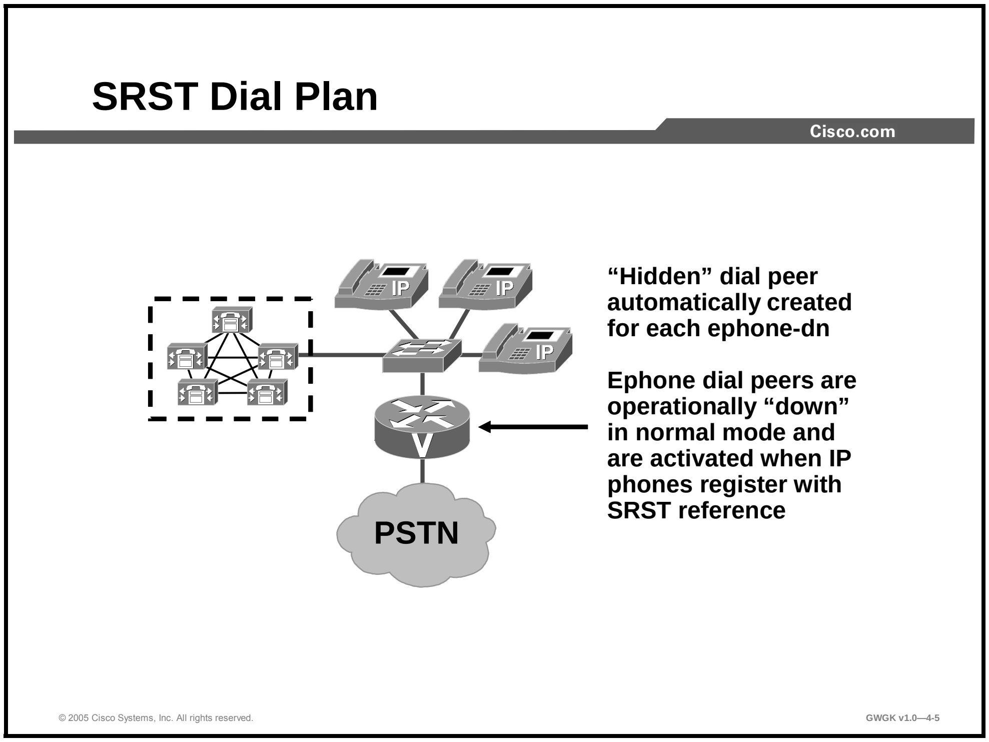
If **call application alternate default** command is not configured, calls are rejected when the dial peer that matches the call does not specify a valid voice application. In releases earlier than Cisco IOS Release 12.2(11)T, the default application was automatically triggered if no application was configured in the dial peer or if the configured application failed. The default application is no longer automatically executed unless the **call application alternate** command is configured.

On MGCP gateways, active calls on MGCP channel associated signaling (CAS) or Foreign Exchange Office (FXO) ports will be preserved during a WAN outage. The calls will remain active until either end hangs up the call. IP phones with active calls will not failover to SRST, but rather will stay in a "limbo" state with no access to supplementary features like hold, call transfer, and so on, until the call is disconnected. Once the call is disconnected, the IP phone fails over to SRST mode, and the voice port fails over to H.323 mode. Active calls on MCCP PRI circuits are dropped during fallback.

On H.323 gateways, when the WAN link fails, active calls from Cisco IP phones to the PSTN are maintained until they are completed or terminated by one of the parties or until the H.225 keepalive expires. Calls in transition and calls that have not yet connected are dropped and must be reinitiated once the Cisco IP phones reestablish connection to their local Cisco SRST router. Telephone service remains unavailable from the time the connection to the remote Cisco CallManager is lost until the Cisco IP phone establishes connection to the Cisco SRST router. Cisco CallManager resets active calls when the WAN link is restored. SRST version 3.2 added support for the **no h225 timeout keepalive** command. This allows all calls to be preserved when SRST is invoked.

SRST Dial Plan

This topic describes the SRST dial plan.



SRST Dial Plan

Cisco.com

“Hidden” dial peer automatically created for each ephone-dn

Ephone dial peers are operationally “down” in normal mode and are activated when IP phones register with SRST reference

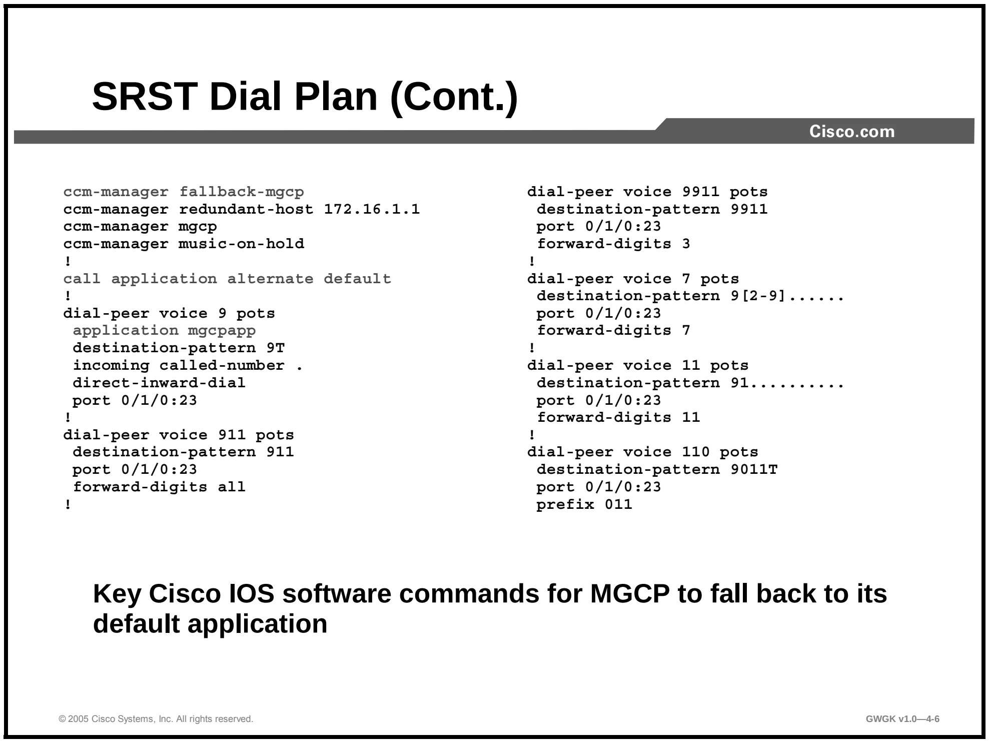
© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—4-5

When SRST is configured, a plain old telephone service (POTS) dial peer is created for each Ethernet phone (ephone). These dial peers are not displayed when you are viewing the configuration, but you can see them by issuing a **show dial-peer voice summary** command. When an IP phone loses contact with the Cisco CallManager cluster and initiates registration with the SRST gateway, these dial peers become active.

The SRST dial peers typically start at 20001. To view the details of these dial peers, use the **show dial-peer voice** detailed or show **dial-peer voice 20001** commands.

For H.323 gateways, the existing POTS dial peers are typically sufficient to handle PSTN calls when operating in SRST mode. The main consideration for H.323 gateways is how digits are sent from Cisco CallManager. If the Cisco CallManager is configured to strip the access code from the dialed string, either you will need to configure two dial peers for each pattern or you will need to train your users *not* to dial the access code when the phone is in SRST mode. It is much easier to retain the access code in Cisco CallManager.



SRST Dial Plan (Cont.)

```
ccm-manager fallback-mgcp
ccm-manager redundant-host 172.16.1.1
ccm-manager mgcp
ccm-manager music-on-hold
!
call application alternate default
!
dial-peer voice 9 pots
 application mgcpapp
 destination-pattern 9T
 incoming called-number .
 direct-inward-dial
 port 0/1/0:23
!
dial-peer voice 911 pots
 destination-pattern 911
 port 0/1/0:23
 forward-digits all
!
```

```
dial-peer voice 9911 pots
 destination-pattern 9911
 port 0/1/0:23
 forward-digits 3
!
dial-peer voice 7 pots
 destination-pattern 9[2-9]......
 port 0/1/0:23
 forward-digits 7
!
dial-peer voice 11 pots
 destination-pattern 91..........
 port 0/1/0:23
 forward-digits 11
!
dial-peer voice 110 pots
 destination-pattern 9011T
 port 0/1/0:23
 prefix 011
```

Key Cisco IOS software commands for MGCP to fall back to its default application

For MGCP gateways, a dial plan must be configured for SRST mode. The following example shows an SRST dial plan for an MGCP gateway. Dial peer 999 is controlled by MGCP. When the router is operating in fallback mode, dial peer 999 is handled by the default application and is used to match inbound calls into the gateway. The other dial peers listed are typical of a U.S. dial plan that resolves emergency calls, 7-digit local calls, 11-digit long distance calls and international calls.

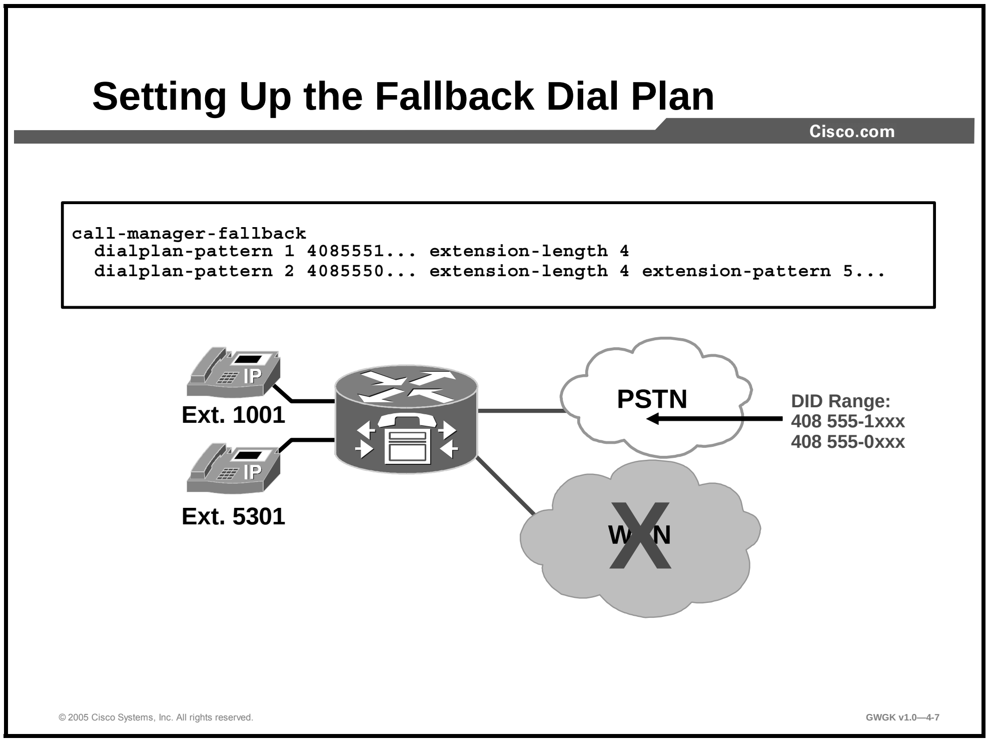
```
!
dial-peer voice 9 pots
 application mgcpapp
 incoming called-number .
 direct-inward-dial
 port 0/1/0:23
!
dial-peer voice 911 pots
 destination-pattern 911
 port 0/1/0:23
 forward-digits all
!
dial-peer voice 9911 pots
 destination-pattern 9911
 port 0/1/0:23
 forward-digits 3
!
dial-peer voice 7 pots
```

```
 destination-pattern 9[2-9]......
 port 0/1/0:23
 forward-digits 7
!
dial-peer voice 11 pots
 destination-pattern 91..........
 port 0/1/0:23
 forward-digits 11
!
dial-peer voice 110 pots
 destination-pattern 9011T
 port 0/1/0:23
 prefix 011
!
call-manager-fallback
 ip source-address 172.16.3.6 port 2000
 max-ephones 2
 max-dn 12
 default-destination 5002
```

Another option, shown in the following example, is to configure direct trunk access using the **access-code** command. This command configures trunk access codes for each type of line—BRI, recEive and transMit (E&M), FXO, and PRI—so that the Cisco IP phones can access the trunk lines during Cisco CallManager fallback when Cisco SRST is enabled. This provides system-wide access.

```
Router(config-cm-fallback)#access-code pri 8 direct-inward-
dial
```

The **access-code** command creates temporary POTS voice dial peers for all of the selected types of voice ports during Cisco CallManager fallback. Use this command only if your normal network dial-plan configuration prevents you from configuring permanent POTS voice dial peers to provide trunk access for use in the fallback mode. When the **access-code** command is used, it is important to ensure that all ports covered by the command have valid trunk connections. Selection between ports for outgoing calls is random. One significant drawback of this approach is you will not be able to use Class of Restrictions (COR) to restrict access to certain numbers.



Setting Up the Fallback Dial Plan

Cisco.com

```
call-manager-fallback
  dialplan-pattern 1 4085551... extension-length 4
  dialplan-pattern 2 4085550... extension-length 4 extension-pattern 5...
```

GWGK v1.0—4-7

The **dialplan-pattern** command is used to create a global prefix that can be used to expand the extension numbers of inbound and outbound calls into fully qualified E.164 numbers.

The **dialplan-pattern** command builds additional dial peers, as in shown in the following example, taken from the configuration in the previous figure:

```
Router(config)# dial-peer voice 20001 pots
Router(config-dial-peer)# destination-pattern 1001
Router(config-dial-peer)# voice-port 50/0/2
```

If a dial-plan pattern is created, such as 4085551..., then an additional dial peer will be created that allows calls to both the 1001 and 4085551001 numbers, shown in this example:

```
Router(config)# dial-peer voice 20002 pots
Router(config-dial-peer)# destination-pattern 4085551001
Router(config-dial-peer)# voice-port 50/0/2
```

When the **extension-pattern** keyword and argument are used, the leading digits of an extension pattern are stripped and replaced with the corresponding leading digits of the dial plan. The **dialplan-pattern 2** command in the figure maps all extension numbers 5xxx to the PSTN number 4083330xxx, so that extension 5301 corresponds to 4083335301. This command is useful when the Direct Inward Dialing (DID) range provided begins with a number that has special meaning, such as 0, or conflicts with the access code used in the dial plan (typically 8 or 9).

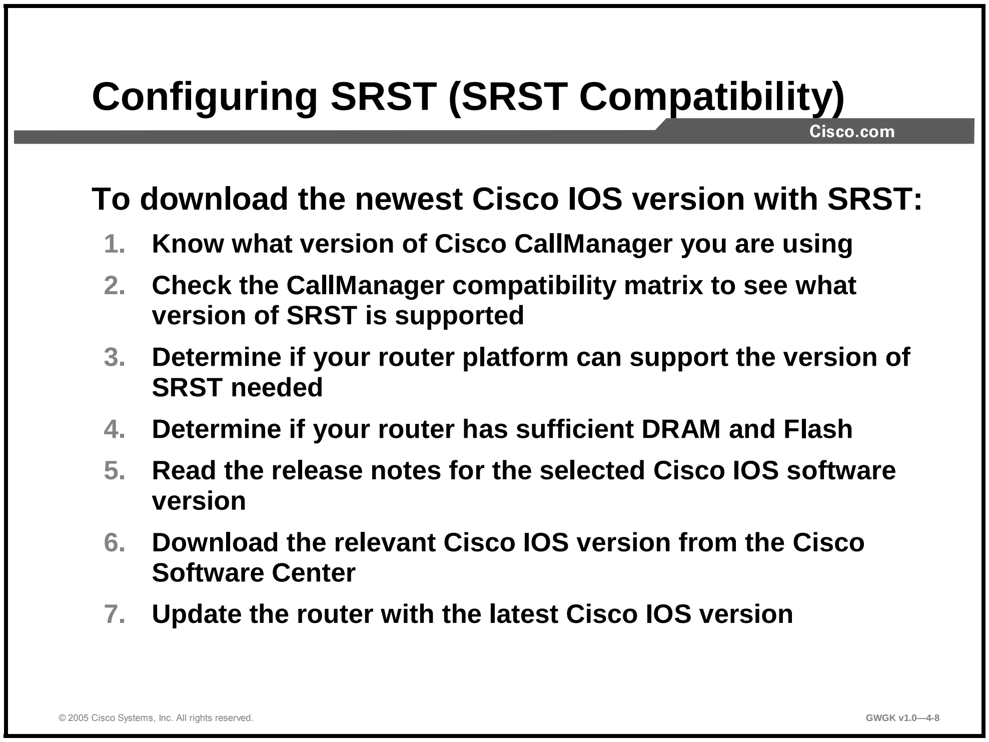
The **dialplan-pattern** command also creates a global prefix that can be used by inbound calls (calls to an IP phone in a Cisco SRST system) and outbound calls (calls made from an IP phone in a Cisco SRST system) to expand their extension numbers to fully qualified E.164 numbers.

For inbound calls (calls to an IP phone in a Cisco SRST system) where the calling party number matches the dial-plan pattern, the call is considered a local call and has a distinctive ring that identifies the call as internal. Any calling party number that does not match the dial-plan pattern is considered to be an external call and has a distinctive ring that is different from the internal ringing. For outbound calls, the **dialplan-pattern** command converts the calling party extension number to an E.164 calling party number.

If there are multiple patterns, called-party numbers are checked in numeric order, starting with pattern 1, until a match is found or until the last pattern has been checked. The valid dial-plan pattern with the lowest tag is used as a prefix to all local Cisco IP phones.

Configuring SRST

This topic describes how to configure SRST.



Configuring SRST (SRST Compatibility)

Cisco.com

To download the newest Cisco IOS version with SRST:

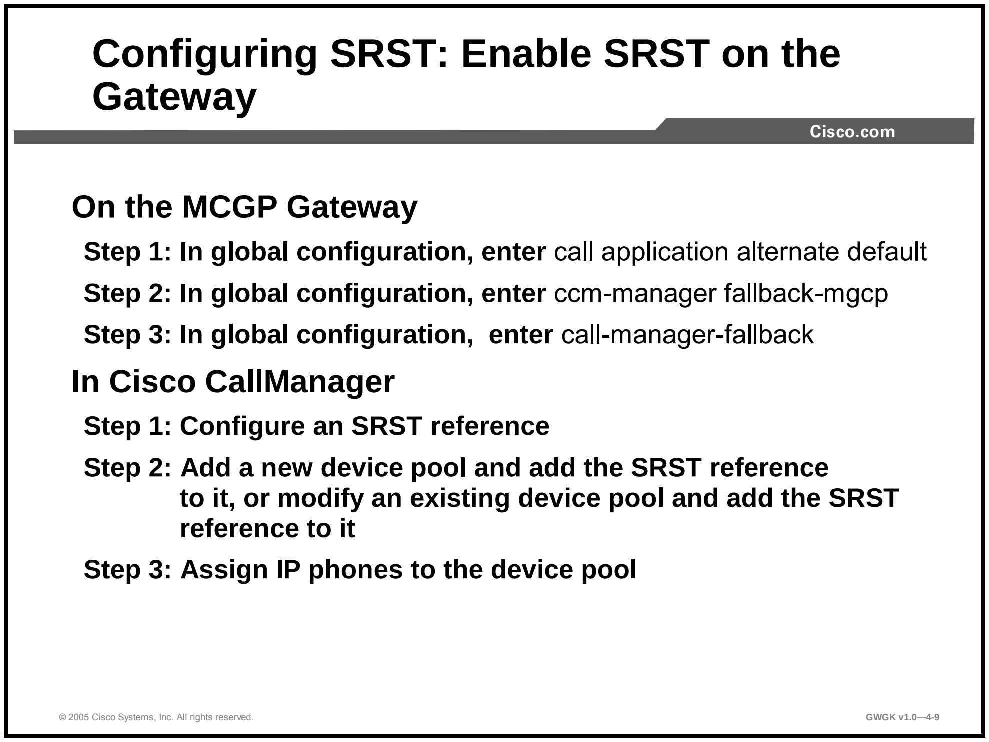
1. **Know what version of Cisco CallManager you are using**
2. **Check the CallManager compatibility matrix to see what version of SRST is supported**
3. **Determine if your router platform can support the version of SRST needed**
4. **Determine if your router has sufficient DRAM and Flash**
5. **Read the release notes for the selected Cisco IOS software version**
6. **Download the relevant Cisco IOS version from the Cisco Software Center**
7. **Update the router with the latest Cisco IOS version**

GWGK v1.0—4-8

The first step in configuring SRST is to verify that the Cisco IOS software on your gateway supports SRST. There are various versions of SRST; the latest is v3.3.

To find the Cisco IOS software version, use these references:

- The *Cisco CallManager Compatibility Matrix* link at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm
- *Cisco SRST Versions* at http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_feature_guide09186a008018912f.html



Configuring SRST: Enable SRST on the Gateway

On the MCGP Gateway

Step 1: In global configuration, enter call application alternate default

Step 2: In global configuration, enter ccm-manager fallback-mgcp

Step 3: In global configuration, enter call-manager-fallback

In Cisco CallManager

Step 1: Configure an SRST reference

Step 2: Add a new device pool and add the SRST reference to it, or modify an existing device pool and add the SRST reference to it

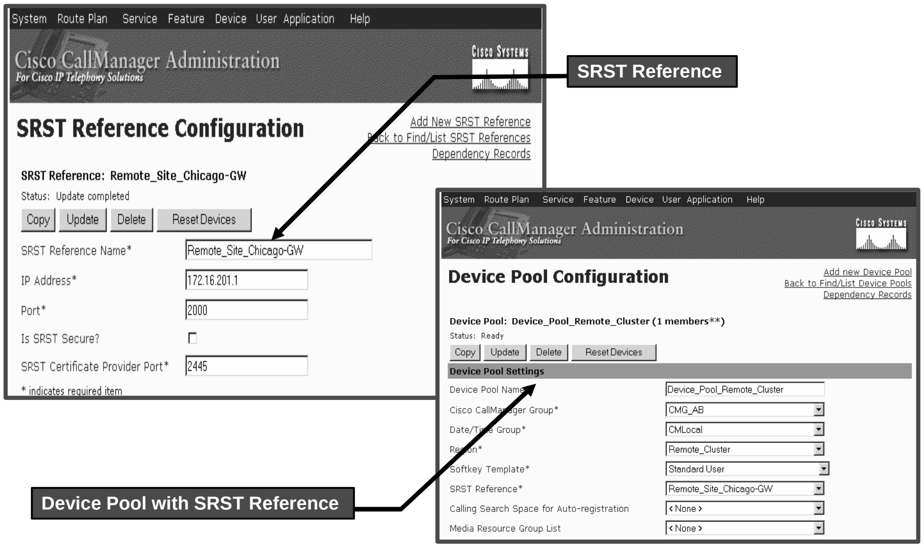
Step 3: Assign IP phones to the device pool

GWGK v1.0—4-9

This figure presents the high-level steps that you need to enable your gateways on Cisco SRST. These configuration steps assume that the gateway has already been configured for MGCP operations. If IP phones reside in a device pool with no SRST reference, the IP phones will not participate in SRST.

Configuring SRST: Enable SRST on CallManager (Cont.)

Cisco.com


System Route Plan Service Feature Device User Application Help
Cisco CallManager Administration
For Cisco IP Telephony Solutions
Cisco Systems
Add New SRST Reference
Back to Find/List SRST References
Dependency Records
Copy
Update
Delete
Reset Devices
System Route Plan Service Feature Device User Application Help
Cisco CallManager Administration
For Cisco IP Telephony Solutions
Cisco Systems
Add new Device Pool
Back to Find/List Device Pools
Dependency Records
Copy
Update
Delete
Reset Devices

SRST Reference

SRST Reference Configuration

SRST Reference: Remote_Site_Chicago-GW

Status: Update completed

SRST Reference Name*	Remote_Site_Chicago-GW
IP Address*	172.16.201.1
Port*	2000
Is SRST Secure?	□
SRST Certificate Provider Port*	2445

* indicates required item

Device Pool Configuration

Device Pool: Device_Pool_Remote_Cluster (1 members)**

Status: Ready

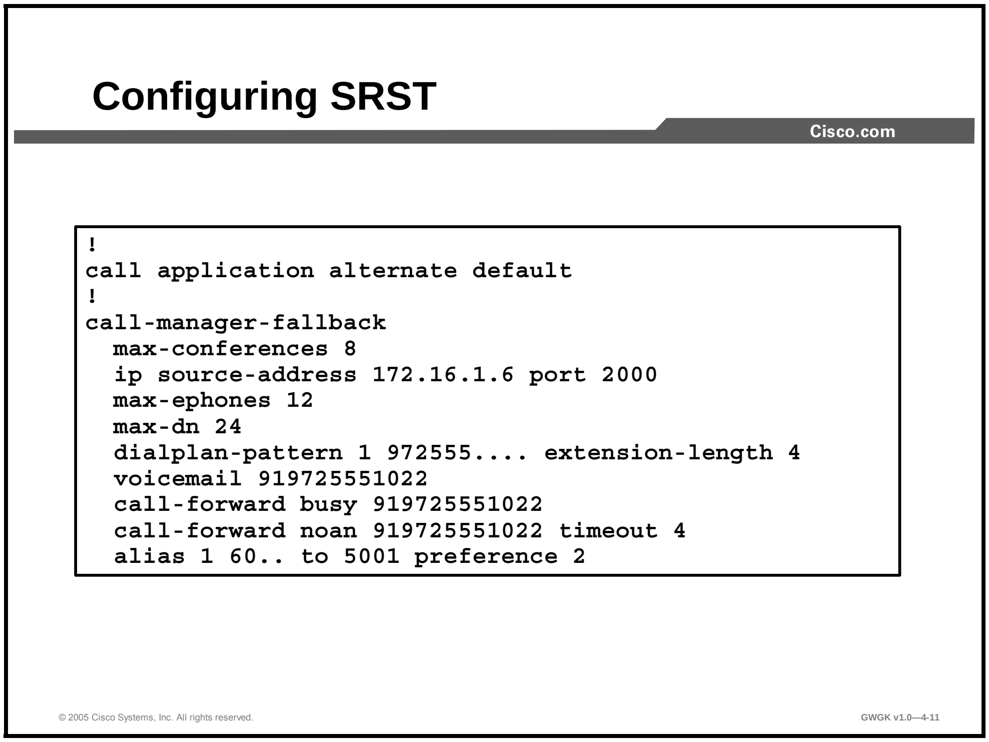
Device Pool Settings

Device Pool Name*	Device_Pool_Remote_Cluster
Cisco CallManager Group*	CMG_AB
Date/Time Group*	CMLocal
Region*	Remote_Cluster
Softkey Template*	Standard User
SRST Reference*	Remote_Site_Chicago-GW
Calling Search Space for Auto-registration	< None >
Media Resource Group List	< None >

Device Pool with SRST Reference

GWGK v1.0—4-10

In Cisco CallManager, you will need to configure the SRST reference configuration for each site. Each site will have an SRST reference name that reflects that site and an IP address that the IP phones will use to register to in the event that SRST is needed. The SRST reference is not assigned to IP phones directly. It is configured in the device pool, which is then assigned to the IP phones.



Configuring SRST

Cisco.com

```
!
call application alternate default
!
call-manager-fallback
  max-conferences 8
  ip source-address 172.16.1.6 port 2000
  max-ephones 12
  max-dn 24
  dialplan-pattern 1 972555.... extension-length 4
  voicemail 919725551022
  call-forward busy 919725551022
  call-forward noan 919725551022 timeout 4
  alias 1 60.. to 5001 preference 2
```

GWGK v1.0—4-11

To get started in configuring SRST Cisco Software IOS version 3.3, you will need to understand the following commands. Note that this list is just a sample of some of the configuration fields on SRST.

- To enable SRST, use the commands described here:
  - **Router(config)#call-manager-fallback**
  - That command enters you into **Router(config-cm-fallback)#**.
- To set up the IP phone signaling path to the SRST, use the commands described here:
  - The **ip source-address** command is a mandatory command, and the fallback subsystem does not start if the IP address is not provided. If the port number is not provided, the default value (2000) is used. The IP address is usually the IP address of the Ethernet, Fast Ethernet, or Gigabit Ethernet port to which the phones are connected.
  - **Router(config-cm-fallback)# ip source-address 10.6.21.4 port 2000**
- To set up a default destination pattern, use the commands described here:
  - If you have some extensions that are not available in SRST mode, you can direct calls to these extensions to a specific IP phone using the **alias** command. The **alias** command supports all port types and makes the **default-destination** command obsolete.
  - **Router(config-cm-fallback)# alias 1 60.. to 5001 preference 2**

- To deploy call forward busy (CFB) and call forward no answer (CFNA), use the commands described here:
  - The following example forwards calls to extension number 5005 when any incoming call reaches a busy or unattended IP phone extension number. Incoming calls will ring for 15 seconds before being forwarded to extension 5005.

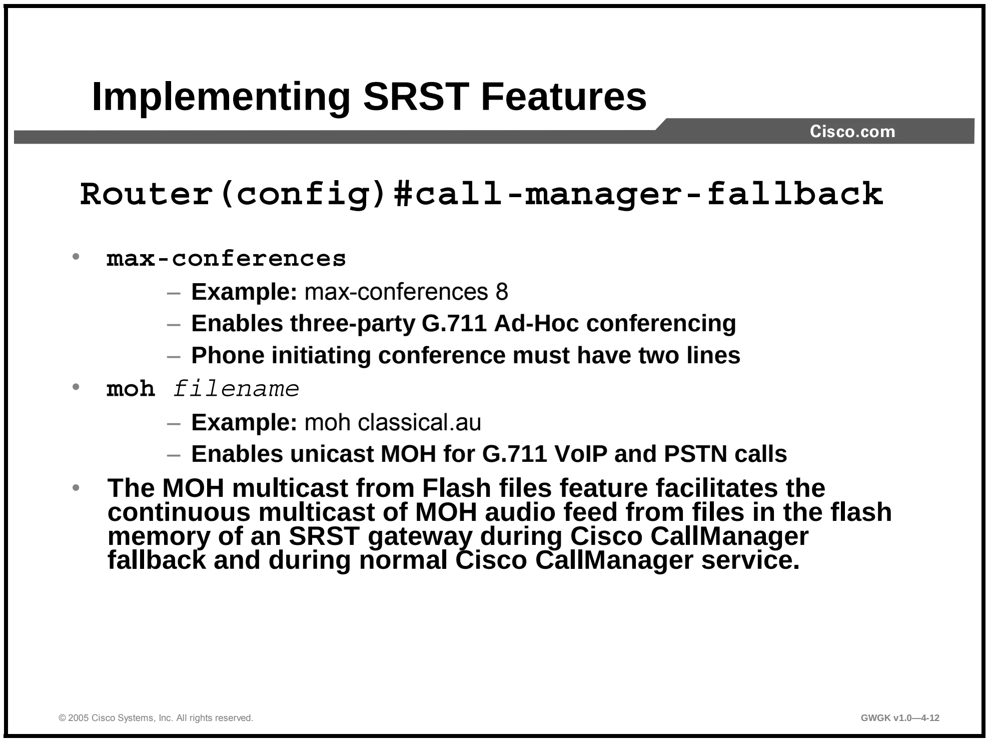
    ```
    call-manager-fallback
     call-forward busy 5005
     call-forward noan 5005 timeout seconds 15
    ```

  - The following example forwards calls to any available extension number in the 50xx bank of extensions when any incoming calls reach a busy or unattended IP phone extension number. Incoming calls will ring for 15 seconds before being forwarded to the bank of extensions.

    ```
    call-manager-fallback
     call-forward busy 50..
     call-forward noan 50.. timeout seconds 15
    ```

Implementing SRST Features

This topic describes how to implement SRST features.



Implementing SRST Features

`Router(config)#call-manager-fallback`

- **`max-conferences`**
  - **Example:** max-conferences 8
  - **Enables three-party G.711 Ad-Hoc conferencing**
  - **Phone initiating conference must have two lines**
- **`moh`** *`filename`*
  - **Example:** moh classical.au
  - **Enables unicast MOH for G.711 VoIP and PSTN calls**
- **The MOH multicast from Flash files feature facilitates the continuous multicast of MOH audio feed from files in the flash memory of an SRST gateway during Cisco CallManager fallback and during normal Cisco CallManager service.**

To implement SRST features, you need to know about Ad-Hoc conferencing, unicast, and multicast music-on-hold (MOH).

Ad-Hoc Conferencing

Three-party Ad-Hoc G.711 conferencing is enabled using the **max-conference** command. For conferencing to be available, an IP phone must have a minimum of two lines connected to one or more buttons. Note that the SRST licensing specifies the number of ephones supported by the SRST gateway, not the number of lines. Increasing the **max-dn** parameter will not affect licensing.

The following example shows the support of up to eight three-way conferences, at one time, on a gateway. The **max-dn** command uses the optional **dual-line** keyword to specify that each IP phone have a virtual voice port with two channels. The **huntstop channel** command is being used to keep incoming calls from hunting to the second channel if the first channel is busy or does not answer. This keeps the second channel free for call transfer, call waiting, or three-way conferencing.

```
call-back-manager
 max-conferences 8
 max-ephones 12
 max-dn 48 dual-line
 huntstop channel
```

Unicast MOH

Unicast MOH for G.711 Ad-Hoc VoIP to PSTN calls uses an audio file stored in the Flash memory of the router. This applies only to IP-phone-to-PSTN calls. This example enables the playing of an audio file called classical.au.

```
call-manager-fallback
 moh classical.au
```

Multicast MOH

The multicast MOH from Flash files feature facilitates the continuous multicast of MOH audio feed from files in the Flash memory of SRST gateways during Cisco CallManager fallback and normal Cisco CallManager service. Multicasting MOH from individual branch routers saves WAN bandwidth by eliminating the need to stream MOH audio from central offices to remote branches.

Details on this MOH multicast feature can be found at http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00802d1c31.html#wp1046574

No multicast MOH routing configuration is required for Cisco SRST gateways because each SRST gateway is configured to act as a host running an application that streams multicast MOH packets from the network. The **multicast moh** command declares the Cisco CallManager multicast MOH address and port number and allows the SRST gateway to route MOH from Flash memory. MoH packets are output only through the router interfaces that match the IP addresses listed using the **route** keyword option. These are the steps to configure these commands:

Step 1 **ccm-manager music-on-hold**

Step 2 **interface loopback** ***number***

Step 3 **ip address** ***ip-address mask***

Step 4 exit

Step 5 **interface fastethernet** ***slot/port***

Step 6 **ip address** ***ip-address mask***

Step 7 exit

Step 8 **call-manager-fallback**

Step 9 **ip source-address** ***ip-address*** **[port** ***port*****]**

Step 10 **max-ephones** ***max-phones***

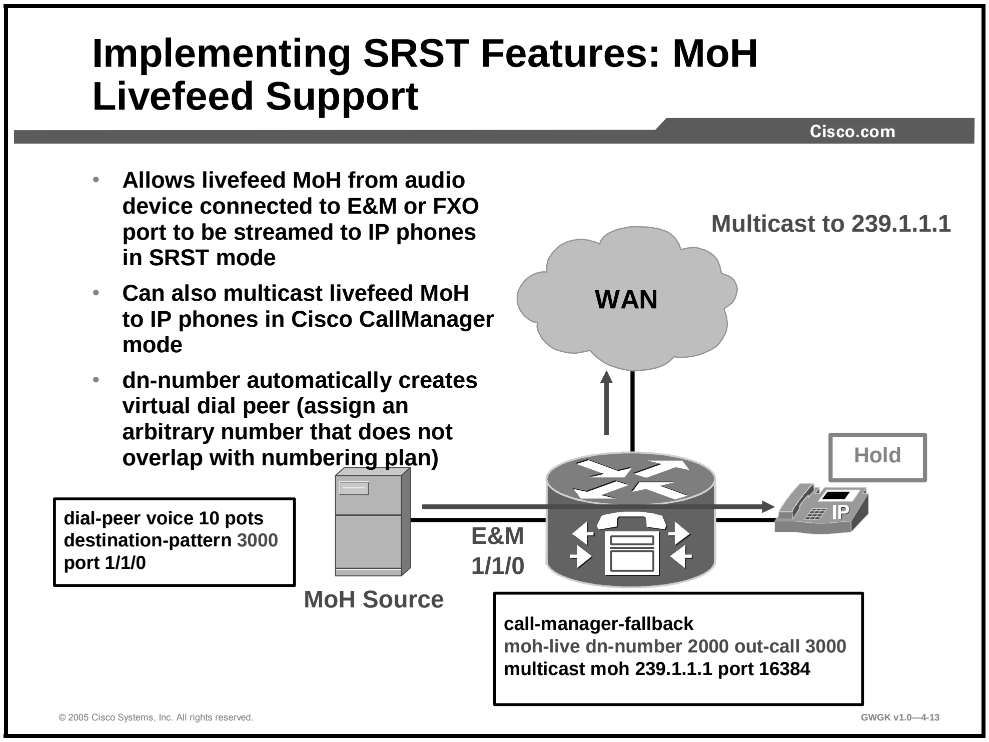
Step 11 **max-dn** ***max-directory-number***

Step 12 **moh** ***filename***

Step 13 **multicast moh** ***multicast-address*** **port** ***port*** **[route** ***ip-address-list*****]**

Step 14 exit

Step 15 To verify the MOH stream, you will need to call a user and ask to be placed on hold. Otherwise, you can access this link and follow the steps in verifying MOH operations: http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00802d1c31.html#wp1046770.



Implementing SRST Features: MoH Livefeed Support

Cisco.com

- Allows livefeed MoH from audio device connected to E&M or FXO port to be streamed to IP phones in SRST mode
- Can also multicast livefeed MoH to IP phones in Cisco CallManager mode
- dn-number automatically creates virtual dial peer (assign an arbitrary number that does not overlap with numbering plan)

```
dial-peer voice 10 pots
destination-pattern 3000
port 1/1/0
```

```
call-manager-fallback
moh-live dn-number 2000 out-call 3000
multicast moh 239.1.1.1 port 16384
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—4-13

Cisco SRST has been enhanced with the **moh-live** command. The **moh-live** command provides live-feed MOH streams from an audio device connected to an E&M or FXO port to Cisco IP phones in SRST mode. Music from a live feed is from a fixed source and is continuously fed into the MOH playout buffer and not read from a Flash file. Live-feed MOH can also be multicast to Cisco IP phones.

To configure MOH from a live feed, first establish a voice port and dial peer for the call, and then create a "dummy" phone or directory number. The dummy number allows for making and receiving calls, but the number is not assigned to a physical phone. It is that number that the MOH system autodials to establish the MOH feed.

The **moh-live** command allocates one of the virtual voice ports from the pool of virtual voice ports created by the **max-dn** command. The virtual voice port places an outgoing call to the dummy number, that is, the directory number specified in the **moh-live** command. The audio stream obtained from the MOH call provides the audio stream.

The recommended interface for live-feed MOH is an analog E&M port because it requires the minimum number of external components. You connect a line-level audio feed (standard audio jack) directly to pins 3 and 6 of an E&M RJ-45 connector. The E&M WAN interface card (WIC) has a built-in audio transformer that provides appropriate electrical isolation for the external audio source. (An audio connection on an E&M port does not require loop current.) The **signal immediate** and **auto-cut-through** commands disable E&M signaling on this voice port. A G.711 audio packet stream is generated by a digital signal processor (DSP) on the E&M port.

If you are using an FXO voice port for live-feed MOH instead of an E&M port, connect the MOH source to the FXO voice port. This connection requires an external adapter to supply normal telephone company battery voltage with the correct polarity to the tip and ring leads of the FXO port. The adapter must also provide transformer-based isolation between the external audio source and the tip and ring leads of the FXO port.

Because music from a live feed is continuously fed into the MOH playout buffer instead of being read from a Flash file, there is typically a 2-second delay. An outbound call to an MOH live-feed source is attempted (or reattempted) every 30 seconds until the connection is made by the directory number that has been configured for MOH. If the live-feed source is shut down for any reason, the Flash memory source will automatically activate.

The Cisco SRST router uses the audio stream from the call as the source for the MOH stream, displacing any audio stream that is available from a Flash file. An example of an MOH stream received over an incoming call is an external H.323-based server device that calls the directory number to deliver an audio stream to the Cisco SRST router.

The following example configures MOH from a live feed. Note that the dial peer references the E&M port that was set with the **voice-port** command and that the dial-peer number (7777) matches the outcall number configured with the **out-call** keyword of the **moh-live** command:

```
voice-port 1/0/0
 input gain 3
 auto-cut-through
 operation 4-wire
 signal immediate
!
dial-peer voice 7777 pots
 destination-pattern 7777
 port 1/0/0
!
call-manager-fallback
 max-conferences 8
 max-dn 1
 moh-live dn-number 3333 out-call 7777
!
```

The Cisco CallManager multicast MOH configuration must run correctly for Cisco SRST multicast MOH to work. Verification of Cisco CallManager multicast MOH will differ for configurations that use a WAN with multicast enabled and ones that use a WAN with multicast disabled.

It is important to verify that the Cisco CallManager multicast MOH is provided through multicasting and not unicasting. Because unicast MOH is enabled by default, it is easy to mistakenly conclude that multicast MOH is working when it is not.

Verifying Cisco SRST MOH to PSTN

To verify that multicast MOH packets transmit over the PSTN, perform the following steps.

Step 1 Verify that a PSTN caller hears MOH when placed on hold by an IP phone caller

Step 2 **show ccm-manager music-on-hold**

Step 3 **debug h245 asn**

Step 4 **show call active voice**

Here are the task-level steps:

Step 1 Verify that a PSTN caller hears MOH when placed on hold by an IP phone caller.

Use a Cisco SRST gateway IP phone to call a PSTN phone, and put the PSTN caller on hold. The PSTN caller should hear MOH.

Step 2 Run the **show ccm-manager music-on-hold** command**.**

Use this command to verify that the MOH is multicast. Note that the **show ccm-manager music-on-hold** command displays information about PSTN connections on hold only. It does not display information about multicast streams going to IP phones on hold. The following is an example of **show ccm-manager music-on-hold** command output.

```
Router# show ccm-manager music-on-hold
Current active multicast sessions : 1
 Multicast       RTP port   Packets       Call   Codec    Incoming
 Address         number     in/out        id              Interface
===================================================================
239.1.1.1         16384   326/326          42   G.711ulaw  Lo0
```

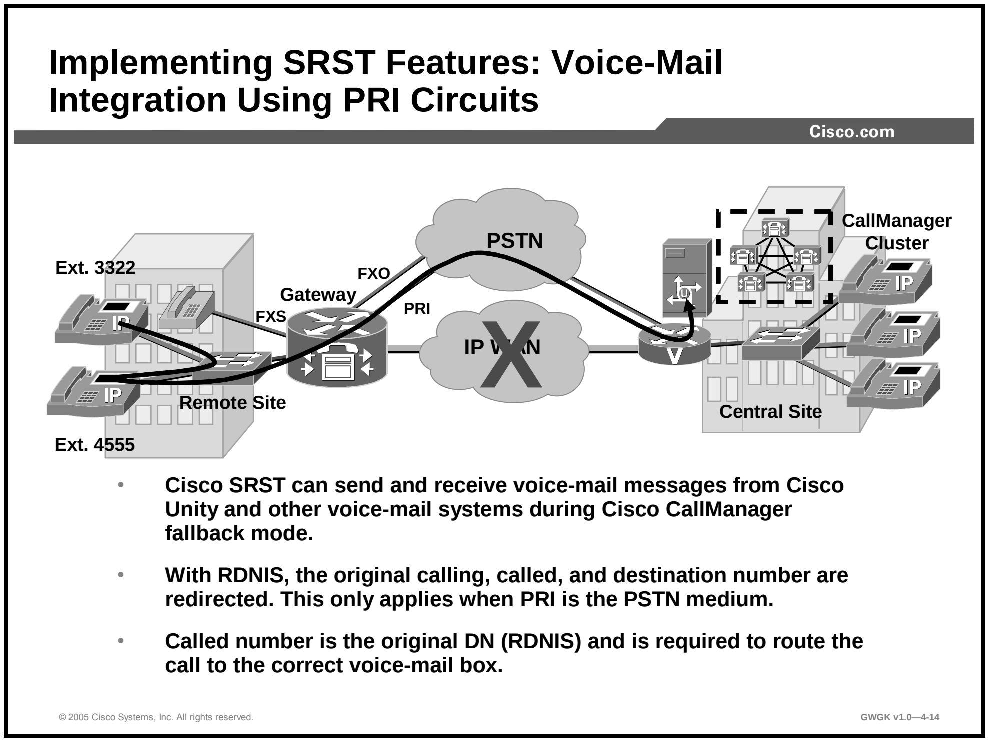
If the PSTN caller hears MOH, but the **show ccm-manager music-on-hold** command displays no active multicast streams, the MOH is unicast. This can be confirmed by checking the MOH performance counters. To check the performance counters, go to the Cisco CallManager server that is hosting MOH:

Step 1 From Microsoft Windows, select Start > Programs > Administrative Tools > Performance.

Step 2 In the Performance window, click the + (plus) icon located at the top of the right pane.

Step 3 In the Add Counters window, select Cisco MOH Device.

Step 4 In the Performance window, you can monitor the MOHMulticastResourceActive and MOHUnicastResourceActive counters to check on multicast activity.



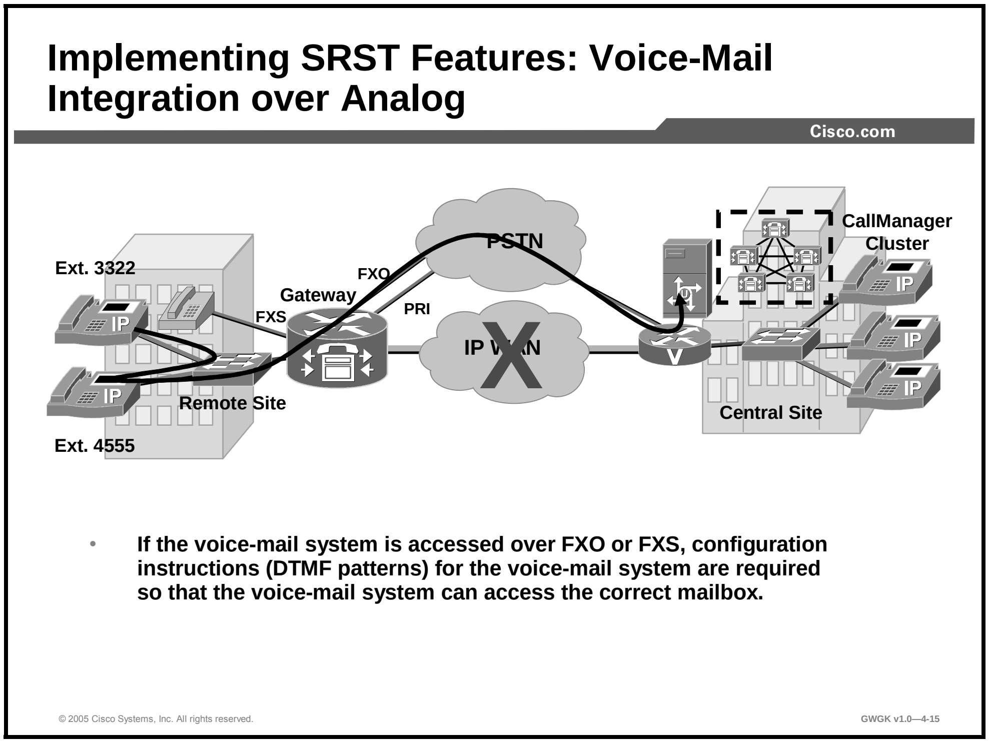
Implementing SRST Features: Voice-Mail Integration Using PRI Circuits

Cisco.com

- Cisco SRST can send and receive voice-mail messages from Cisco Unity and other voice-mail systems during Cisco CallManager fallback mode.
- With RDNIS, the original calling, called, and destination number are redirected. This only applies when PRI is the PSTN medium.
- Called number is the original DN (RDNIS) and is required to route the call to the correct voice-mail box.

GWGK v1.0—4-14

Typically, calls are forwarded to voice mail when the called number is busy or does not answer. To play personal greetings, a voice-mail system requires the number of the phone that does not answer, known as the redirected dialed number identification service (RDNIS). During fallback, an RDNIS must be passed to voice-mail systems through the PSTN. If the trunks are Foreign Exchange Station (FXS) or FXO, the **vm-integration** command can facilitate the in-band passing of RDNIS information to a voice-mail system.



Implementing SRST Features: Voice-Mail Integration over Analog

Cisco.com

- **If the voice-mail system is accessed over FXO or FXS, configuration instructions (DTMF patterns) for the voice-mail system are required so that the voice-mail system can access the correct mailbox.**

GWGK v1.0—4-15

Cisco SRST can send and receive voice-mail messages from Cisco Unity and other voice-mail systems during Cisco CallManager fallback. Systems with FXO or FXS access connect to a PSTN and use in-band dual tone multifrequency (DTMF) for signaling. If the voice-mail system is accessed over FXO or FXS, you must configure instructions (DTMF patterns) for the voice-mail system so that it can access the correct voice-mail system mailbox. If the voice-mail system is accessed over BRI or PRI, no instructions are necessary because the voice-mail system can log in to the mailbox of the calling phone directly.

When you are using analog circuits for voice-mail redirect, use **vm-integration** on the gateway. The following example is a configuration of the same **vm-integration pattern** commands that are entered to describe the DTMF tones expected by the voicemail system:

```
call-manager-fallback
voicemail 918005551000
call-forward busy 918005551000
call-forward noans 918005551000 timeout 20
```

There are five pattern commands, which are listed in this example:

```
vm-integration
 pattern direct * CGN
 pattern ext-to-ext no-answer # FDN #2
 pattern ext-to-ext busy # FDN #2
 pattern trunk-to-ext no-answer # FDN #2
 pattern trunk-to-ext busy # FDN #2
```

The following is a dial-peer configuration example:

```
dial-peer voice 100 pots
 destination-pattern 918005551000 T
 port 1/0/0 (Port connected to voicemail system)
```

Use **dial-peer prefix** command to add pauses before forwarding digits.

The **vm-integration** command does not support PRI or BRI. If the trunks are ISDN, it may be possible to pass the RDNIS as part of Q.931 signaling. Cisco SRST includes RDNIS in the Q.931 setup signaling by default. Note, however, that some carriers drop RDNIS, thus nullifying this solution.

More information on Cisco SRST V3.2: Integrating Voice Mail with Cisco SRST can be found at http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_administration_guide_chapter09186a00802a01f8.html#wp1345432\.

Perform the following steps:

Step 1 pattern direct tag1 {CGN | CDN | FDN} [tag2 {CGN | CDN | FDN}] [tag3 {CGN | CDN | FDN}] [last-tag]

Step 2 pattern ext-to-ext busy tag1 {CGN | CDN | FDN} [tag2 {CGN | CDN | FDN}] [tag3 {CGN | CDN | FDN}] [last-tag]

Step 3 pattern ext-to-ext no-answer tag1 {CGN | CDN | FDN} [tag2 {CGN | CDN | FDN}] [tag3 {CGN | CDN | FDN}] [last-tag]

Step 4 pattern trunk-to-ext busy tag1 {CGN | CDN | FDN} [tag2 {CGN | CDN | FDN}] [tag3 {CGN | CDN | FDN}] [last-tag]

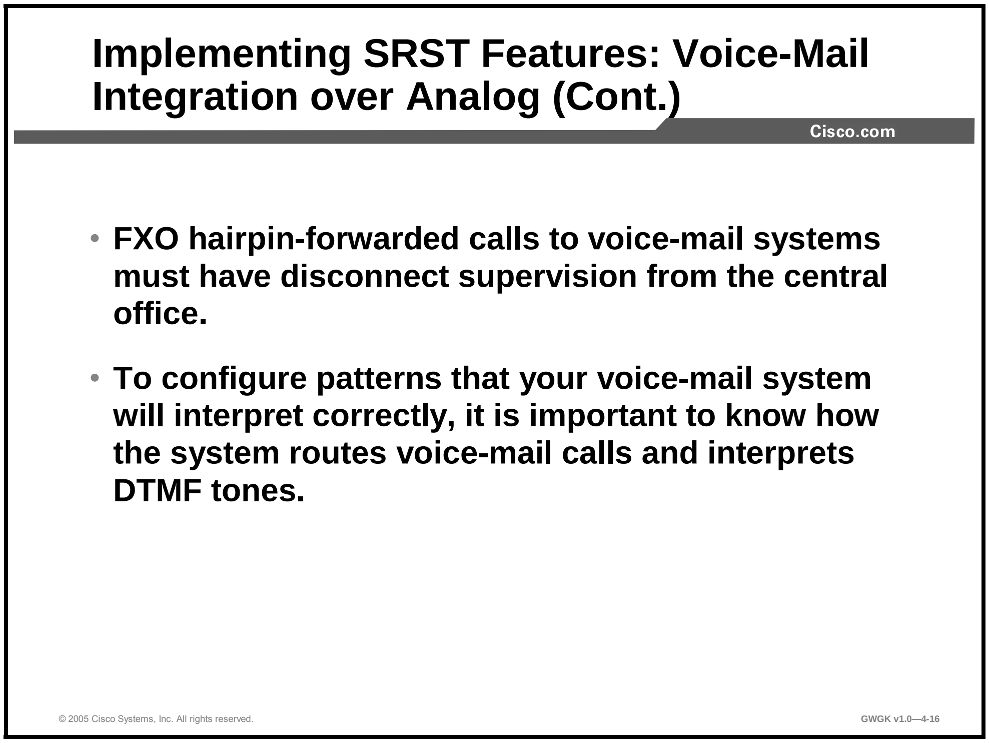
Step 5 pattern trunk-to-ext no-answer tag1 {CGN | CDN | FDN} [tag2 {CGN | CDN | FDN}] [tag3 {CGN | CDN | FDN}] [last-tag]

The “adfk” table shows the detailed steps.

SRST Voice Mail Integration Procedure

Step	Command Action	Purpose
1.	**vm-integration** Example: **Router(config)# vm-integration**	Enters voice-mail integration mode and enables voice-mail integration with DTMF and analog voice-mail systems.
2.	**pattern direct** ***tag1*** **{CGN | CDN | FDN} [*tag2* {CGN | CDN | FDN}] [*tag3* {CGN | CDN | FDN}] [*last-tag*]** Example: **Router(config-vm-int)# pattern direct 2 CGN ***	Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system when the user presses the messages button on the phone. ■ *tag1*—Alphanumeric string fewer than four DTMF digits in length. The alphanumeric string consists of a combination of four letters (A, B, C, and D), two symbols (* and #), and ten digits (0 to 9). The tag numbers match the numbers defined in the voice-mail system's integration file, immediately preceding either the number of the calling party, the number of the called party, or a forwarding number. ■ *tag2* and *tag3*—(Optional) See *tag1*. ■ *last-tag*—See *tag1*. This tag indicates the end of the pattern. ■ **CGN**—Calling number (CGN) information is sent to the voice-mail system. ■ **CDN**—Called number (CDN) information is sent to the voice-mail system. ■ **FDN**—Forwarding number (FDN) information is sent to the voice-mail system.
3.	**pattern ext-to-ext busy** ***tag1*** **{CGN | CDN | FDN} [*tag2* {CGN | CDN | FDN}] [*tag3* {CGN | CDN | FDN}] [*last-tag*]** Example: **Router(config-vm-int)# pattern ext-to-ext busy 7 FDN * CGN ***	Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system once an internal extension attempts to connect to a busy extension and the call is forwarded to voice mail. For argument and keyword information, see Step 2.
4.	**pattern ext-to-ext no-answer** ***tag1*** **{CGN | CDN | FDN} [*tag2* {CGN | CDN | FDN}] [*tag3* {CGN | CDN | FDN}] [*last-tag*]** Example: **Router(config-vm-int)# pattern ext-to-ext no-answer 5 FDN * CGN ***	Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system once an internal extension fails to connect to an extension and the call is forwarded to voice mail. For argument and keyword information, see Step 2.

Step	Command Action	Purpose
5.	**pattern trunk-to-ext busy** ***tag1*** **{CGN | CDN | FDN} [*tag2* {CGN | CDN | FDN}] [*tag3* {CGN | CDN | FDN}] [*last-tag*]** Example: **Router(config-vm-int)# pattern trunk-to-ext busy 6 FDN * CGN ***	Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system once an external trunk call reaches a busy extension and the call is forwarded to voice mail. For argument and keyword information, see Step 2.
6.	**pattern trunk-to-ext no-answer** ***tag1*** **{CGN | CDN | FDN} [*tag2* {CGN | CDN | FDN}] [*tag3* {CGN | CDN | FDN}] [*last-tag*]** Example: **Router(config-vm-int)# pattern trunk-to-ext no-answer 4 FDN * CGN ***	Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system when an external trunk call reaches an unanswered extension and the call is forwarded to voice mail. For argument and keyword information, see Step 2.



Implementing SRST Features: Voice-Mail Integration over Analog (Cont.)

Cisco.com

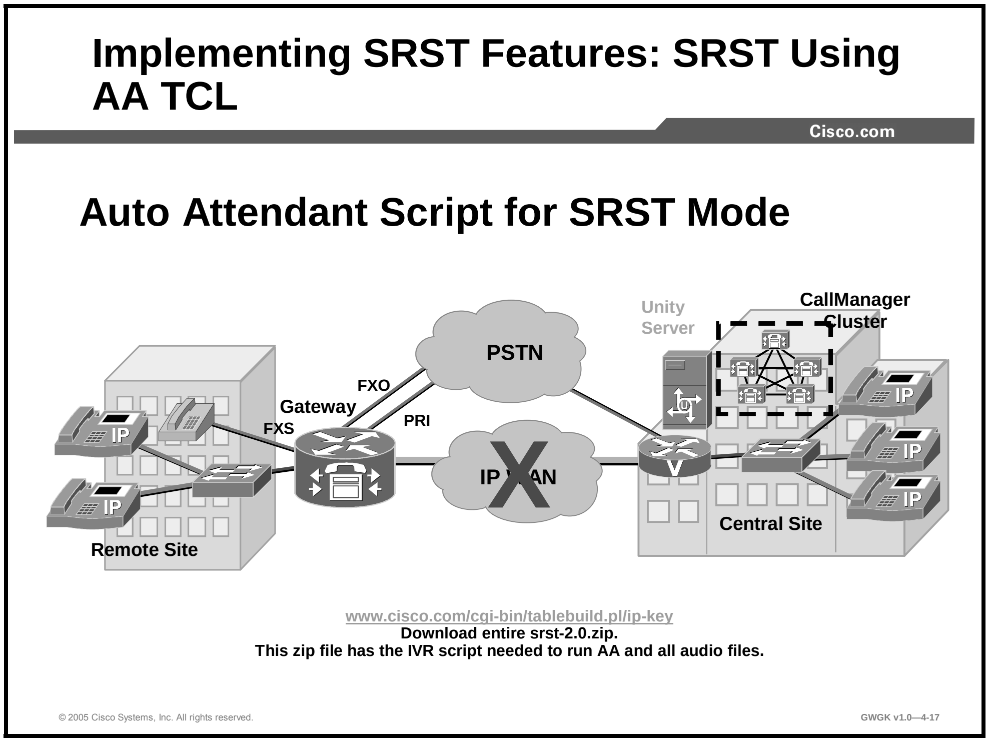
- FXO hairpin-forwarded calls to voice-mail systems must have disconnect supervision from the central office.
- To configure patterns that your voice-mail system will interpret correctly, it is important to know how the system routes voice-mail calls and interprets DTMF tones.

GWGK v1.0—4-16

For information on FXO answer and disconnect supervision, go to http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087b4f.html.

For information on call routing instructions using DTMF digit patterns, go to http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_administration_guide_chapter09186a00802a01f8.html#wp1363986.

For information on how to transfer a caller directly into Cisco Unity, go to http://www.cisco.com/en/US/partner/products/sw/voicesw/ps2237/products_tech_note09186a008015b963.shtml.



Implementing SRST Features: SRST Using AA TCL

Cisco.com

Auto Attendant Script for SRST Mode

www.cisco.com/cgi-bin/tablebuild.pl/ip-key
Download entire srst-2.0.zip.
This zip file has the IVR script needed to run AA and all audio files.

GWGK v1.0—4-17

SRST has the option to be configured to have Auto Attendant functionality when the Cisco CallManager server is down. This feature was first added in SRST version 2.0. The Toolkit Command Language (TCL) interactive voice response (IVR) Auto Attendant mechanism can support the handling of inbound calls on FXO or PRI ports and outbound calls on FXS ports including analog phones configured via POTS and IP phones configured via **ephone-dns**. Based on the TCL script running on the SRST gateway, a caller can hear the prompts, enter digits when prompted, and then be transferred to the person whom the caller wishes to reach.

This section describes the srst_aa TCL script functionality: When the Cisco CallManager is configured and running, all the calls will be directed to the Auto Attendant on the Cisco CallManager when the uses dials the pilot number of the Auto Attendant on the Cisco CallManager. When the WAN connection to the Cisco CallManager is down (SRST mode) or when Cisco CallManager is busy (this might happen when there are not enough IP IVR ports on the Cisco CallManager to handle incoming calls), the TCL IVR on the SRST router will play a welcome prompt to the user and will prompt the user to enter a destination number. The TCL IVR will collect the digits and place the call to the destination based on the dial-plan pattern set in the dial peer.

Operator support is also included with this feature. If the user does not dial any number or enters 0, the user will be transferred to an operator (if an operator number is configured in the command-line interface [CLI]). If the user enters an invalid number, the user will be prompted to reenter the number for up to three times before the call is disconnected.

All of the actual scripts and audio files are found in the zip file on the Instructor's CD for the course, and will be supplied by the Instructor for the labs.

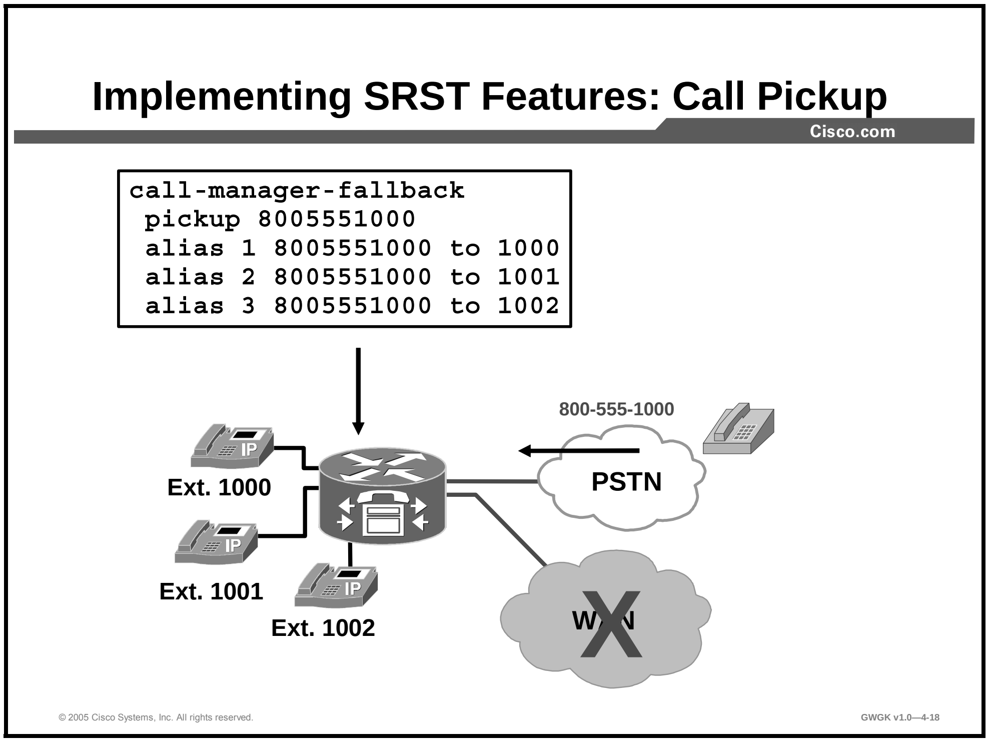
- Languages supported: English
  - — Required minimum IOS image version: 12.2(2)XT, Script: srst_Cisco.2.0.0.0.tcl
- Associated audio files
  - — en_welcome.au, en_dest_busy.au, en_reenter_dest.au, en_dest_busy.au
- Call flow of the script
  - — Check whether **cm-pilot** number (Cisco CallManager IP IVR number), **aa-pilot** number (Auto Attendant pilot number), and operator numbers are configured in the CLI. The **cm-pilot** number is mandatory if Cisco CallManager IP IVR is to be used and **aa-pilot** number configuration is mandatory for handling call transfers successfully.
  - — Check for automatic number identification (ANI) and dialed number identification service (DNIS) on the incoming leg.
  - — When the call is setup, if the Cisco CallManager is connected to the Cisco CallManager IP IVR, Cisco CallManager will handle all the calls.
  - — If the Cisco CallManager is down or unreachable, or number of IP IVR ports on the Cisco CallManager are not sufficient, play the welcome prompt en_welcome.au and ask the user to enter the destination number by playing the en_enter_dest.au prompt.
  - — If the user does not dial any number or dials 0, connect to the operator.
  - — If the user dials an invalid destination number, ask the user to reenter the destination number by playing the en_reenter_dest.au prompt. This will be done up to three times, and after playing the busy prompt en_dest_busy.tcl, disconnect the call.
  - — If the user dials a valid destination number, the call is connected. When the parties hang up, the call legs will be disconnected.
  - — If the user dials a valid destination number and if the destination is busy or unreachable, the user will be prompted to reenter the same destination number or a different destination number.

A complete call-application voice configuration is shown here:

```
call application voice srst-aa flash:// srst_Cisco.2.0.0.0.tcl
call application voice srst-aa language 1 en
call application voice srst-aa cm-pilot 1400
call application voice srst-aa aa-pilot 1010
call application voice srst-aa operator 1001 (an ephone-dn)
call application voice srst-aa set-location en 0 flash://
```

If PSTN callers are to hear the SRST Auto Attendant, you need to set up POTS dial peers with the incoming called number **aa-pilot** number. When callers hit the POTS dial peer, the script will launch. For IP phones on the SRST gateway to access the Auto Attendant script, VoIP dial peers with destination patterns of the **aa-pilot** are required. The example shows

```
dial-peer voice 5 pots
      application srst-aa
 destination-pattern 9T
 incoming called-number 1400
 direct-inward-dial
 port 0/1/0:23
      forward-digits all

       dial-peer voice 4 pots
     application srst-aa
destination-pattern 9T
incoming called-number 1010
direct-inward-dial
preference 1
port 0/1/0:23
forward-digits all
```



Implementing SRST Features: Call Pickup

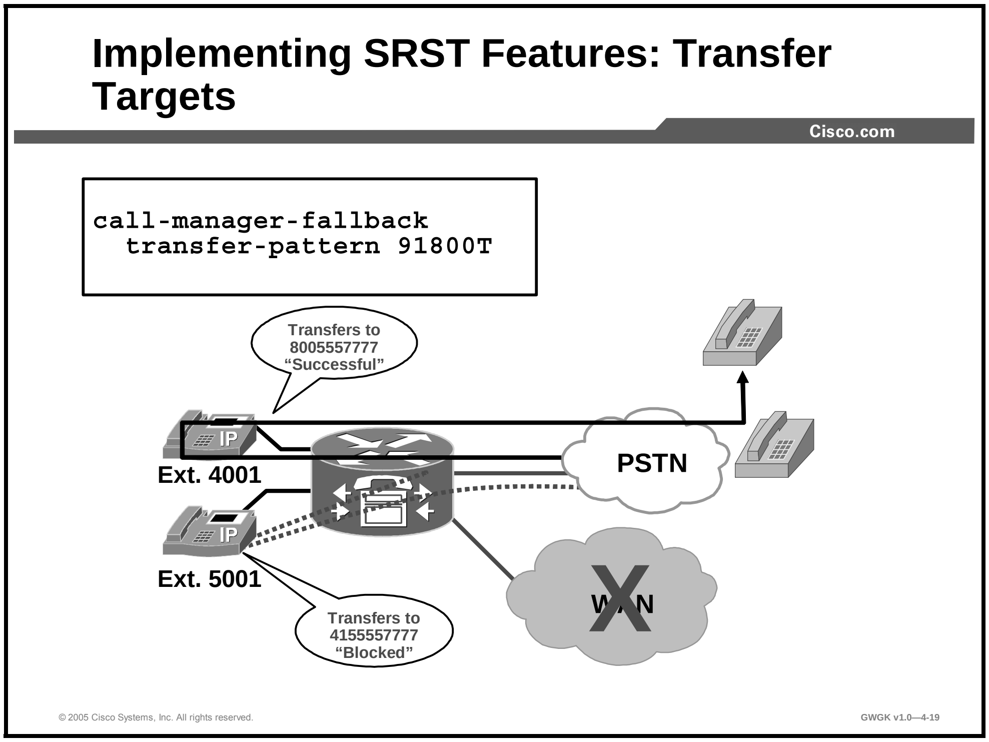
Cisco.com

```
call-manager-fallback
 pickup 8005551000
 alias 1 8005551000 to 1000
 alias 2 8005551000 to 1001
 alias 3 8005551000 to 1002
```

GWGK v1.0—4-18

This figure shows an 800 number terminating at the SRST site. The dial peer on the gateway has an incoming called number that matches the number defined in the **pickup** command. In this figure, an incoming call to 8005551000 will ring numbers 1000 through 1002 randomly. Extensions 1001 through 1002 can pick up the call by pressing the pickup softkey. The pickup feature is best used in combination with the **alias** command.

Setting up pickup in this configuration disables directed call pickup. In other words, you cannot press the pickup softkey followed by the ringing extension if the incoming call does not have a called number that matches the number defined in pickup.



Implementing SRST Features: Transfer Targets

Cisco.com

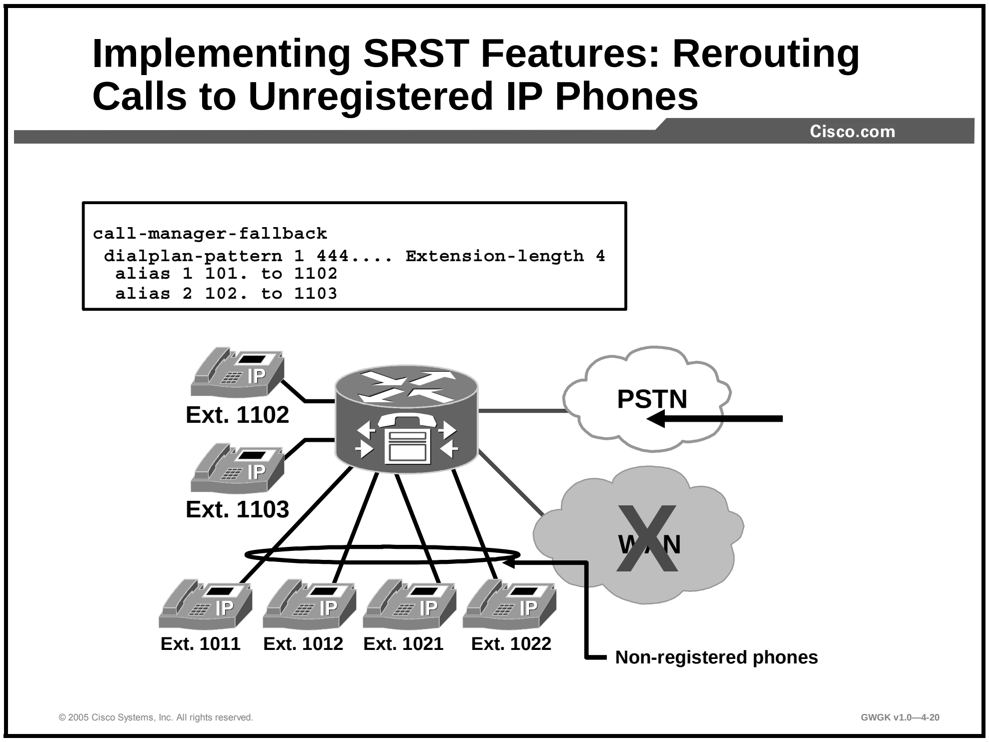
```
call-manager-fallback
  transfer-pattern 91800T
```

Transfers to 8005557777 “Successful”

Transfers to 4155557777 “Blocked”

GWGK v1.0—4-19

Call transfer patterns can be used to limit the transfer of calls during SRST operation. This can be used to allow only certain dial strings to be transfer targets. By default, only SRST phones can be transfer targets. If outside PSTN transfer targets need to be included, they must be specified. This figure shows an outside 800 number transfer target with a leading 9 to match a dial peer. In this scenario, if we added the 91415T transfer pattern, extension 5001 would be able to transfer calls to the 415 area code.



Implementing SRST Features: Rerouting Calls to Unregistered IP Phones

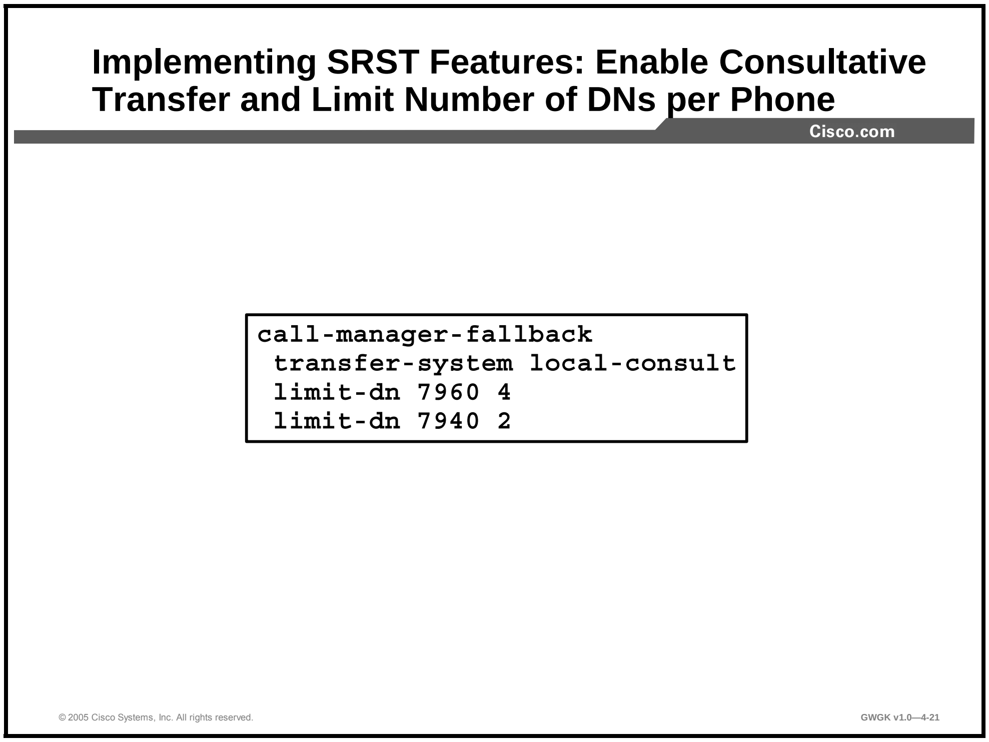
Cisco.com

```
call-manager-fallback
 dialplan-pattern 1 444.... Extension-length 4
  alias 1 101. to 1102
  alias 2 102. to 1103
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—4-20

You can reroute incoming calls that are destined for nonregistered IP phones during SRST mode via the **alias** command. This figure shows four IP phones that did not register with the SRST gateway because of the device pool configuration. In the figure, calls to the unregistered extensions 1011 and 1012 will be forwarded to 1102, and calls to unregistered extensions 1021 and 1022 will be forwarded to extension 1103.



Implementing SRST Features: Enable Consultative Transfer and Limit Number of DNs per Phone

Cisco.com

```
call-manager-fallback
 transfer-system local-consult
 limit-dn 7960 4
 limit-dn 7940 2
```

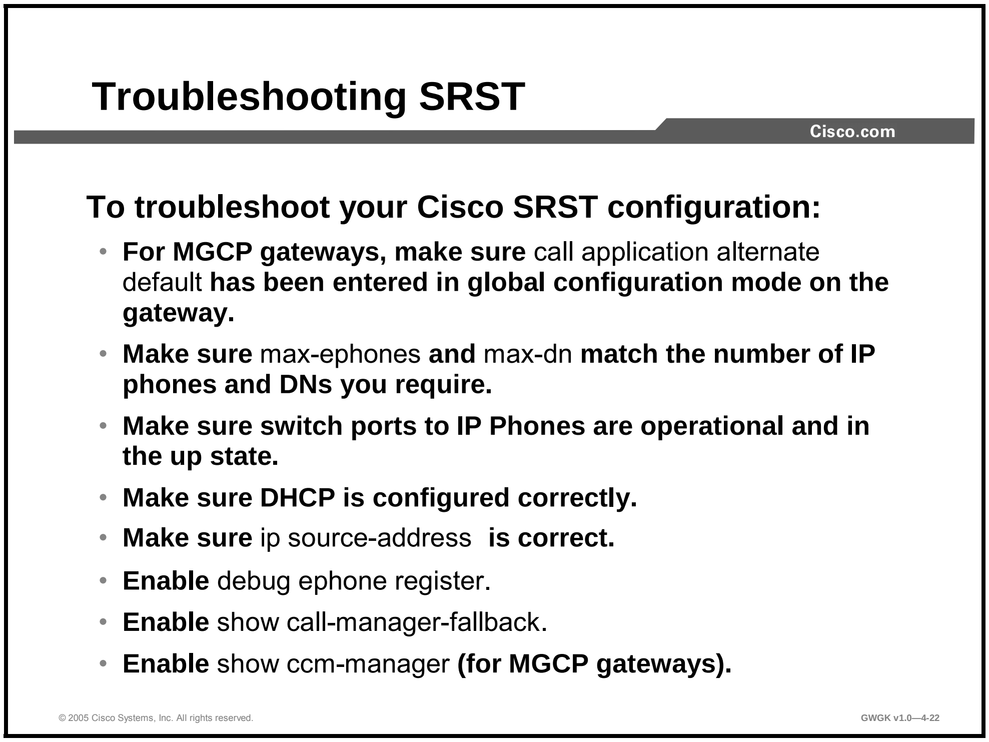
GWGK v1.0—4-21

Many organizations rely on speaking with the target extension before transferring a call; this is known as consultative transfer. Blind transfers are the default. By setting **transfer-system local-consult**, you can change the default transfer rule to consultative.

By setting a maximum line-appearance count with the **limit-dn** command, you can allow a smaller set of line appearances on the phone during SRST operations. If a phone that is registered to Cisco CallManager has six line appearances when it tries to register to the SRST gateway, it will request six lines appearances, which could consume your **max-dn** configuration.

Troubleshooting SRST

This topic describes how to troubleshoot SRST.



Troubleshooting SRST

Cisco.com

To troubleshoot your Cisco SRST configuration:

- **For MGCP gateways, make sure** call application alternate default **has been entered in global configuration mode on the gateway.**
- **Make sure** max-ephones **and** max-dn **match the number of IP phones and DNs you require.**
- **Make sure switch ports to IP Phones are operational and in the up state.**
- **Make sure DHCP is configured correctly.**
- **Make sure** ip source-address **is correct.**
- **Enable** debug ephone register.
- **Enable** show call-manager-fallback.
- **Enable** show ccm-manager **(for MGCP gateways).**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—4-22

Most issues with SRST fall into two categories: Registration issues and dial-plan issues.

Registration issues are typically caused by SRST configuration errors. Here are some common registration issues:

- The parameters **max-ephones**, **max-dn**, or both are not configured. These parameters default to 0.
- The parameters **max-ephones**, **max-dn**, or both are not sufficient to support all phones.
- The SRST reference is not assigned to phones in Cisco CallManager.
- The Dynamic Host Configuration Protocol (DHCP) server is not local, which prevents a phone from obtaining an address.
- The **ip source-address** is not correct.

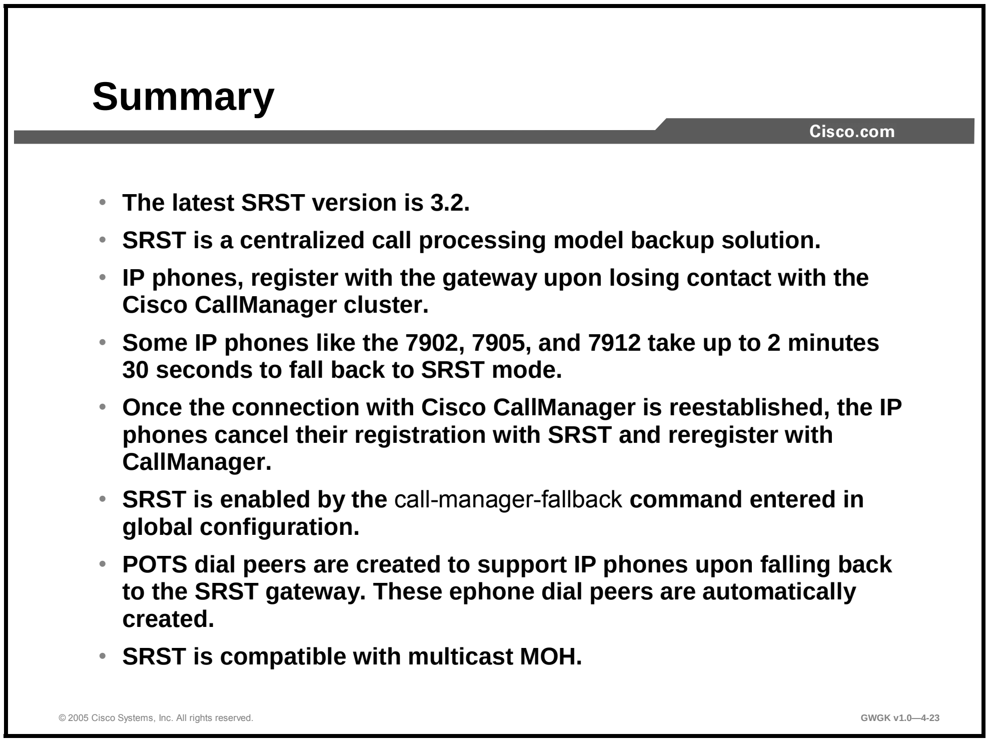
Use the **debug ephone register** command to troubleshoot registration problems.

Troubleshooting dial plan issues uses the same tools and techniques in SRST mode. There are some additional considerations for MGCP gateways, primarily verifying that MGCP fallback is correctly configured.

It is strongly recommended that the SRST configuration be tested before it is needed. The simplest way to do this is to add a null route to the Cisco CallManager addresses. This will prevent the IP phones from receiving their keepalives but still allow other traffic to pass over the WAN.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

Cisco.com

- The latest SRST version is 3.2.
- SRST is a centralized call processing model backup solution.
- IP phones, register with the gateway upon losing contact with the Cisco CallManager cluster.
- Some IP phones like the 7902, 7905, and 7912 take up to 2 minutes 30 seconds to fall back to SRST mode.
- Once the connection with Cisco CallManager is reestablished, the IP phones cancel their registration with SRST and reregister with CallManager.
- SRST is enabled by the call-manager-fallback command entered in global configuration.
- POTS dial peers are created to support IP phones upon falling back to the SRST gateway. These ephone dial peers are automatically created.
- SRST is compatible with multicast MOH.

GWGK v1.0—4-23

References

For additional information, refer to these resources:

- SRST 3.2 System Administrator Guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_feature_guide09186a008018912f.html
- Cisco CallManager Express and SRST TCL Scripts at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp

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) Which command activates SRST? (Source:)

- A) **call application alternate default**
- B) **call-manager-fallback**
- C) **ip source-address**
- D) **application mgcpapp**

Q2) Which command tells the gateway to fallback to the default application? (Source:)

- A) **application mgcpapp**
- B) **call application alternate default**
- C) **H.323 dial-peer statements**
- D) **call-manager-fallback**

Q3) Which device manages the dial-plan during SRST operations? (Source:)

____

Q4) Where would you look to see what version SRST works with your current version of Cisco CallManager? (Source:)

- A) check the MGCP compatibility matrix
- B) check the H.323 compatibility matrix
- C) check the SRST Compatibility matrix
- D) check Cisco CallManager compatibility matrix

Q5) Where do IP phones get their SRST information? (Source:)

- A) DHCP server option 150
- B) local DNS
- C) IP DHCP-pool voice configuration on gateway
- D) device pool assignment in Cisco CallManager

Q6) Before assigning IP phones to a SRST reference, what has to happen first? (Source:)

- A) device pool needs to be created
- B) SRST reference needs to be created
- C) the call application alternative default needs to be configured on the gateway
- D) device pool needs to be assigned in Cisco CallManager

Q7) How would you block remote site users from using SRST mode? (Source:)

- A) unplug the IP phone
- B) put them on a subnet separate from the IP phones that use SRST
- C) do not add an SRST reference to the device pool those phones are in
- D) use calling search space and partitions to block their access

Q8) What happens when **ip source-address** is not configured? (Source:)

- A) The fallback subsystem does not start.
- B) No IP phones can transfer calls.
- C) The IP source address is part of Cisco CallManager Express, not SRST.
- D) DSP farming will not operate.

Lesson Self-Check Answer Key

Q1)	B
Q2)	B
Q3)	SRST gateway
Q4)	D
Q5)	D
Q6)	B
Q7)	C
Q8)	A

Lesson 2

Digital Signal Processors in Gateways

Overview

Digital Signal Processors (DSPs) play a major role in Cisco gateway support of VoIP. DSPs support various features such conference bridging, transcoding, media termination points (MTPs), and basic telephony interfacing to the public switched telephone network (PSTN). In this lesson, you will learn about what the hardware does, how it operates, and how to configure the gateway to accommodate conferencing, transcoding, and MTPs, which rely on DSP technology.

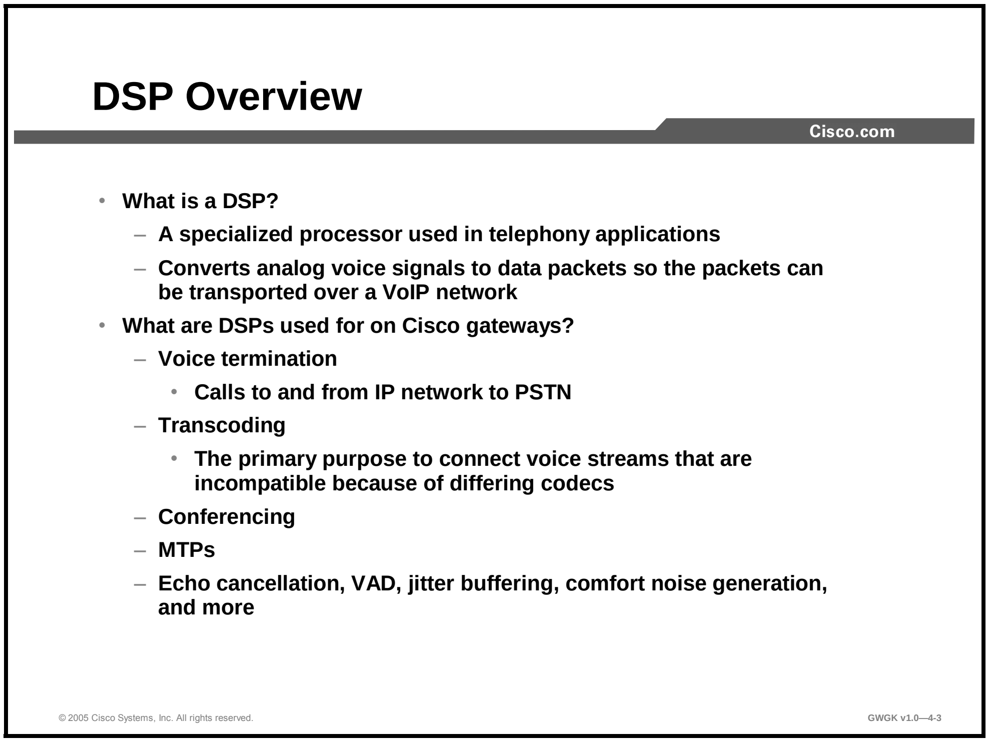
Objectives

Upon completing this lesson, you will be able to configure DSP farming resources to support hardware conferencing, transcoding and MTP services on a gateway. This ability includes being able to meet these objectives:

- Describe DSP functionality and how DSPs support voice
- Configure the appropriate codec on a gateway
- Describe the function of a DSP farm and the hardware and software requirements for DSP support
- Determine the quantity and location of required DSP resources
- Configure a DSP farm to provide support for transcoding and conferencing services

DSP Overview

This topic gives an overview of DSPs.



DSP Overview

Cisco.com

- What is a DSP?
  - A specialized processor used in telephony applications
  - Converts analog voice signals to data packets so the packets can be transported over a VoIP network
- What are DSPs used for on Cisco gateways?
  - Voice termination
    - Calls to and from IP network to PSTN
  - Transcoding
    - The primary purpose to connect voice streams that are incompatible because of differing codecs
  - Conferencing
  - MTPs
  - Echo cancellation, VAD, jitter buffering, comfort noise generation, and more

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—4-3

This figure presents an overview of what DSPs are and where in the Cisco gateway these DSPs are used, providing voice termination, transcoding, conferencing, media termination, and echo cancellation.

Note DSP use in echo cancellation will not be covered in this lesson.

In voice termination, DSPs are used to terminate time-division multiplexing (TDM) calls to the gateway. For example, when an IP phone calls a PSTN user, or a PSTN user calls an IP phone user, a DSP resource is used to accommodate this call.

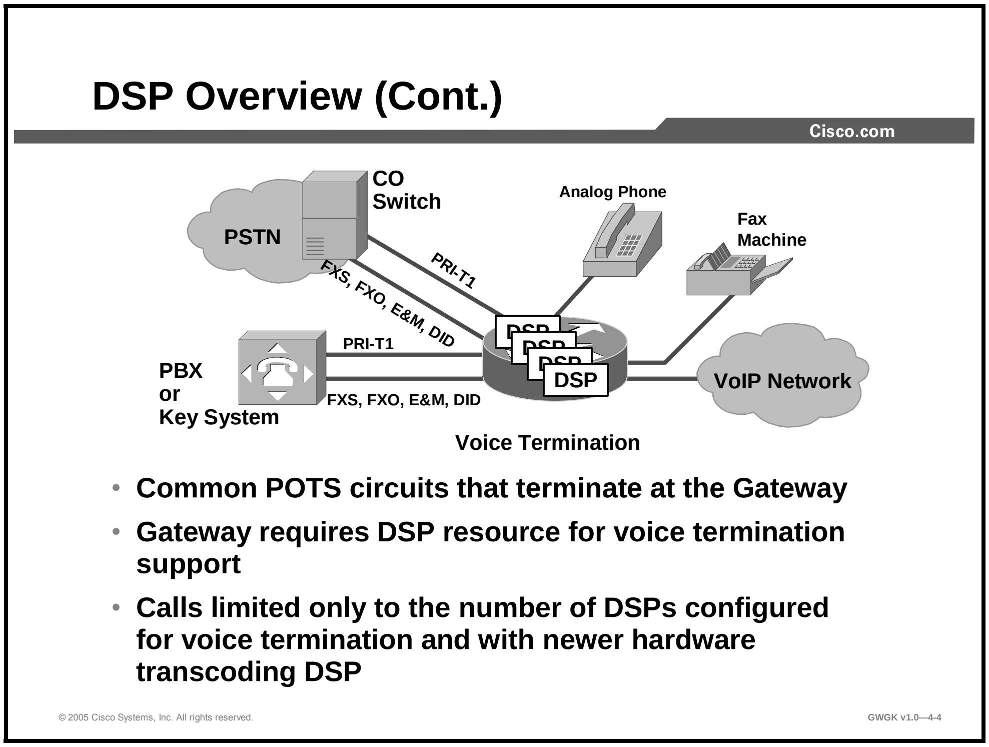
Transcoding takes a voice stream of one codec type and transcodes it or converts it from one codec compression type to another codec compression type. For example, transcoding takes a voice stream from a G.711 codec and transcodes it in real time to a G.729 codec stream. In other words, the DSP takes the G.711 input stream and converts that signal so that this stream can talk with the G.729 stream. The conversion stays within the DSP until the termination of the call.

In audio conferencing, DSPs are used to mix voice streams from multiple participants into a single conference-call stream. In what is called a mixed mode conference, DSPs can accommodate various codec compressions into one voice conference stream.

Through the use of DSPs, media termination points extend supplementary services, such as call hold, call transfer, call park, and conferencing that are otherwise not available when a call is routed to an H.323 endpoint. Some H.323 gateways may require that calls use an MTP to enable supplementary call services. MTPs are used typically where endpoints do not support the starting and stopping of Real-Time Transport Protocol (RTP) steams.

DSPs fully support integrated echo cancellation, voice activity detection, silence suppression, jitter buffering, and comfort noise generation.

- Echo cancellation is implemented in DSP firmware on Cisco voice gateways and is independent of other functions implemented in the DSP protocol and compression algorithm. In voice packet-based networks, echo cancellers are built into the low-bit-rate codecs. An echo canceller removes the echo portion of the signal coming out of the tail circuit and headed into the WAN. It does so by learning the electrical characteristics of the tail circuit and forming its own model of the tail circuit in its memory, and creating an estimated echo signal based on the current and past receive signal. It subtracts the estimated echo from the actual transmit signal coming out of the tail circuit. The quality of the estimation is continuously improved by monitoring the estimation error.
- Jitter buffers intelligently balance delay and packet loss through the gateway for maximum call clarity and quality.
- Voice activity detection (VAD), also known as silence suppression, is used to save bandwidth on the VoIP network by not sending packets during silence periods in the voice conversation. Because callers are accustomed to background noise in the PSTN, the far-end gateway generates comfort noise when VAD is active.



DSP Overview (Cont.)

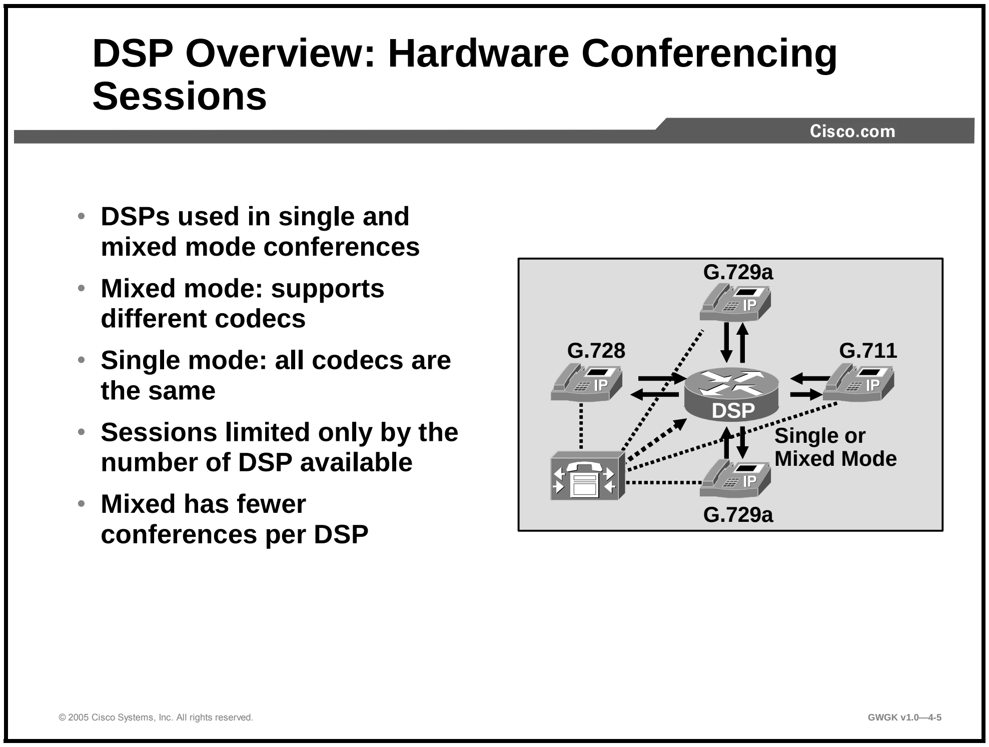
Cisco.com

- **Common POTS circuits that terminate at the Gateway**
- **Gateway requires DSP resource for voice termination support**
- **Calls limited only to the number of DSPs configured for voice termination and with newer hardware transcoding DSP**

GWGK v1.0—4-4

Voice termination applies to a call that has two call legs, one leg on a TDM interface and the second leg on a VoIP connection. The TDM leg must be terminated by hardware that performs coding and decoding as well as packetizing the voice stream. This voice termination function is performed by DSP resources residing in the same hardware module, blade, or platform. All DSP hardware on Cisco gateways is capable of terminating voice streams, and certain hardware is also capable of performing other media resource functions such as conferencing, transcoding, and media termination points, which will be discussed later in this lesson. The number of supported calls depends on the computational complexity of the codec used and also on the complexity mode configured in Cisco IOS software on the gateway. Cisco IOS software enables manual configuration of codec complexity on the gateway hardware module. Some older hardware platforms support only two complexity modes, medium and high complexity, while the new voice network modules and newer gateway (Cisco 2800 and 3800 series routers) hardware platforms support medium, high, and flex modes.

This figure shows the various TDM circuits that can terminate at the gateway and require DSP resources. Voice termination DSP requirements are not to be confused with transcoding, conferencing and MTP DSP requirements and should always be provisioned separately. PSTN connectivity is typically always via codec compression G.711.



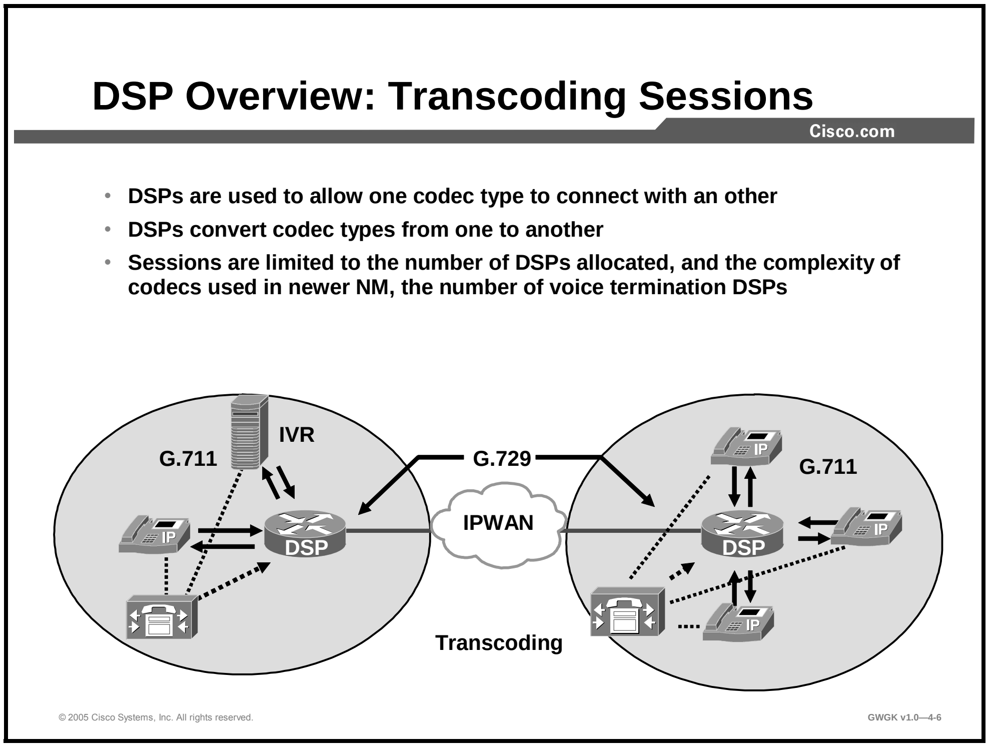
DSP Overview: Hardware Conferencing Sessions

Cisco.com

- DSPs used in single and mixed mode conferences
- Mixed mode: supports different codecs
- Single mode: all codecs are the same
- Sessions limited only by the number of DSP available
- Mixed has fewer conferences per DSP

GWGK v1.0—4-5

Voice conferencing involves adding several parties to a single conversation. The adding of parties can be conducted with all parties using the same codec, which is considered single mode conferencing, or can be of mixed mode variety where the codecs can vary. In mixed mode conferencing, G.711, G.729, G.729a, G.729b, and G.729ab participants are joined in a single conference; no additional transcoding resource is needed to include the disparate codecs. Conferencing requires dedicated DSP resources. When provisioning DSPs for conferencing calculate the required number of DSPs separate from voice termination, transcoding, and MTP services.



DSP Overview: Transcoding Sessions

Cisco.com

- **DSPs are used to allow one codec type to connect with an other**
- **DSPs convert codec types from one to another**
- **Sessions are limited to the number of DSPs allocated, and the complexity of codecs used in newer NM, the number of voice termination DSPs**

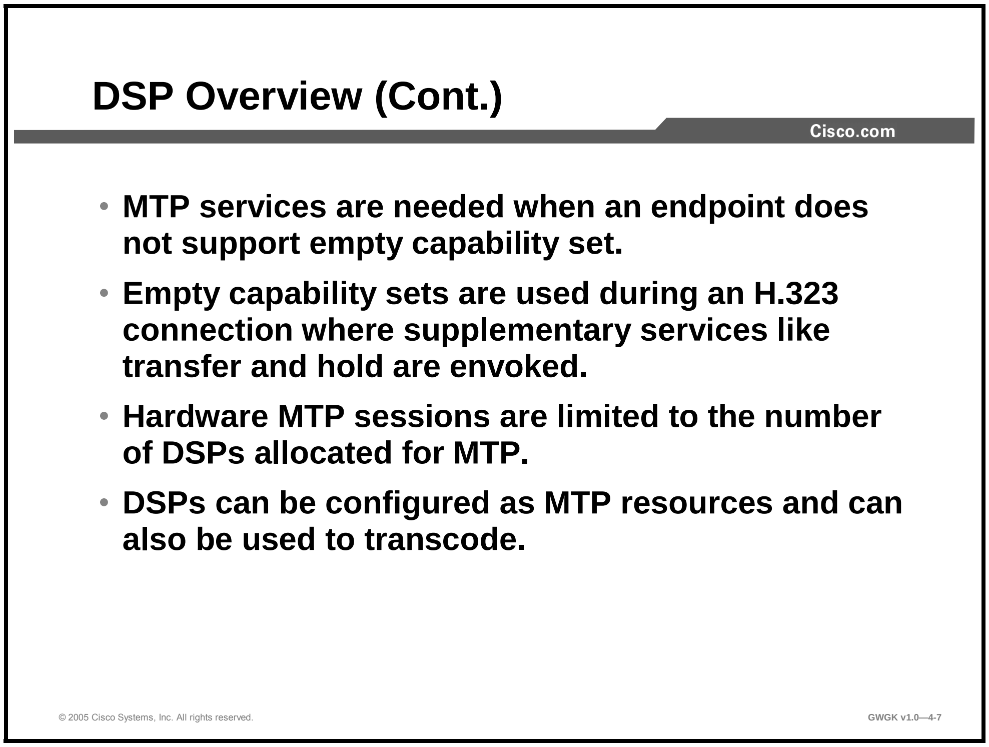
GWGK v1.0—4-6

Transcoding takes a voice stream of one codec type and transcodes it or converts it from one codec compression type to another codec compression type. For example, transcoding takes a voice stream from a G.711 codec and transcodes it in real time to a G.729 codec stream.

In addition, a transcoder can also provide an MTP capability and may be used to enable supplementary services for H.323 endpoints when required.

Transcoding services are needed when a codec from G.729, G729a, G729b, or G729ab global system for mobile communication full rate (GSMFR), or global system for mobile communication enhanced rate codecs (GSMEFR) needs to communicate with codecs G.711ulaw or G.711alaw. Conversely, transcoding is required when G.711ulaw or G.711alaw needs to communicate with codecs G.729, G.729a, G.729b, G.729ab, GSMFR, and GSMEFR.

To provide transcoding services, it is important to know the DSP requirements to support it. With transcoding, allowing diverse codecs to connect will require a certain complexity to the gateway that will increase CPU use, and could require additional DSP support.



DSP Overview (Cont.)

- MTP services are needed when an endpoint does not support empty capability set.
- Empty capability sets are used during an H.323 connection where supplementary services like transfer and hold are envoked.
- Hardware MTP sessions are limited to the number of DSPs allocated for MTP.
- DSPs can be configured as MTP resources and can also be used to transcode.

MTPs are used to extend supplementary services to H.323 endpoints that do not support empty capabilities sets. When needed, an MTP is allocated and connected into a call on behalf of an H.323 endpoint. When an MTP is inserted into the RTP streams, the media streaming are connected between the MTP and H323 device, where the RTP stream is not torn down for the duration of the call. The media streaming connected to the other side of the MTP can be connected and torn down as needed to implement features such as hold, transfer, and so forth.

Hardware-Based MTPs

A hardware-based MTP support is provided through the use of DSPs. Hardware-based MTPs can support transcoding, however if MTP is configured on a gateway and transcoding is as well and MTP sessions are fully used, additional MTP requests will start using transcoding resources.

Hardware MTP specifications are described here:

- The RTP stream is managed through DSPs
- Provides connections between calls with different codecs; call that require transcoding services
- Provide connections between call legs where packetization time of the codec needs to be changed. For example, G.711 20ms packetization to G.711 30ms packetization
- Max sessions is determined by DSP availability (follows the same rules as voice termination)
- Requires DSP hardware to be present: DSP farm configuration required

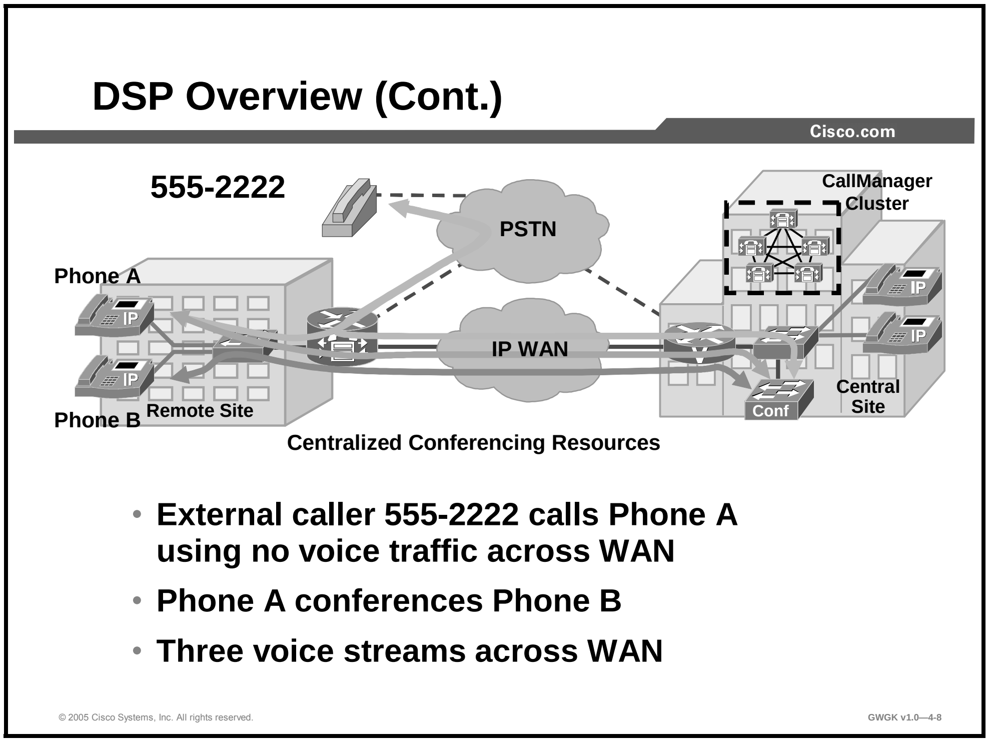
Software-Based MTPs

A software-based MTP is a device that is implemented by Cisco IOS software. A software-based MTP support can be configured. A single software-based MTP device can handle many more sessions that its hardware-based counterpart, and can support various codec connections. Although software MTP can support multiple codecs, the codec connections on both call legs must be same.

Software MTP specifications are described here:

- No DSP involved, connections manipulated by Cisco IOS software.
- Provide connections between call legs that have the following codecs: G.711alaw, G.711ulaw, G.729abr8, G.729ar8, G.729br8, G.729r8, GSMEFR, and GSMFR. The caveat is that both call leg codecs must be the same.
- MTP sessions possible 1 to 500.
- Can be configured in IOS software without the need for DSP hardware to be present.

As mentioned in the previous figures relative to DSP allocation, knowing how many DSPs will be needed to support hardware MTP sessions is important. Although MTP support can use transcoding resources, allocating a certain number of DSPs for MTP is best practice.



DSP Overview (Cont.)

Cisco.com

Centralized Conferencing Resources

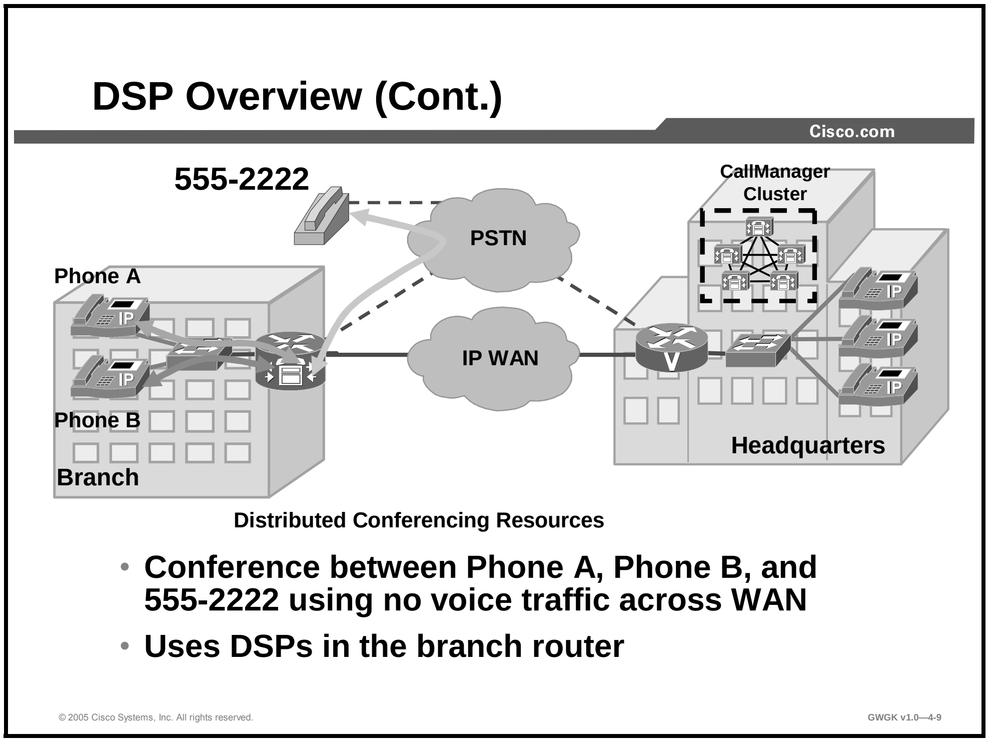
- **External caller 555-2222 calls Phone A using no voice traffic across WAN**
- **Phone A conferences Phone B**
- **Three voice streams across WAN**

GWGK v1.0—4-8

When there are no DSP resources at the remote site, bandwidth use over the IP WAN can become an issue. This figure discusses some issues relative to hosting conferencing at the central site as opposed to deploying DSP resources at the remote site.

This figure shows a conference call being established between an external caller and two phones at the remote site. This conference will require three voice streams of voice traffic to cross the IP WAN because no DSP resources were used at the remote site. This is considered a centralized conferencing model. This is not the most effective model for conferencing. If DSP resources were deployed at the remote site, this call would not have to tie up additional IP WAN bandwidth.

The DSPs used in this figure come from hardware conferencing resources located on a Cisco Catalyst software platform. Do not to point out the Cisco hardware platform. Rather, show what happens to the IP WAN when DSP resources located at a central site.



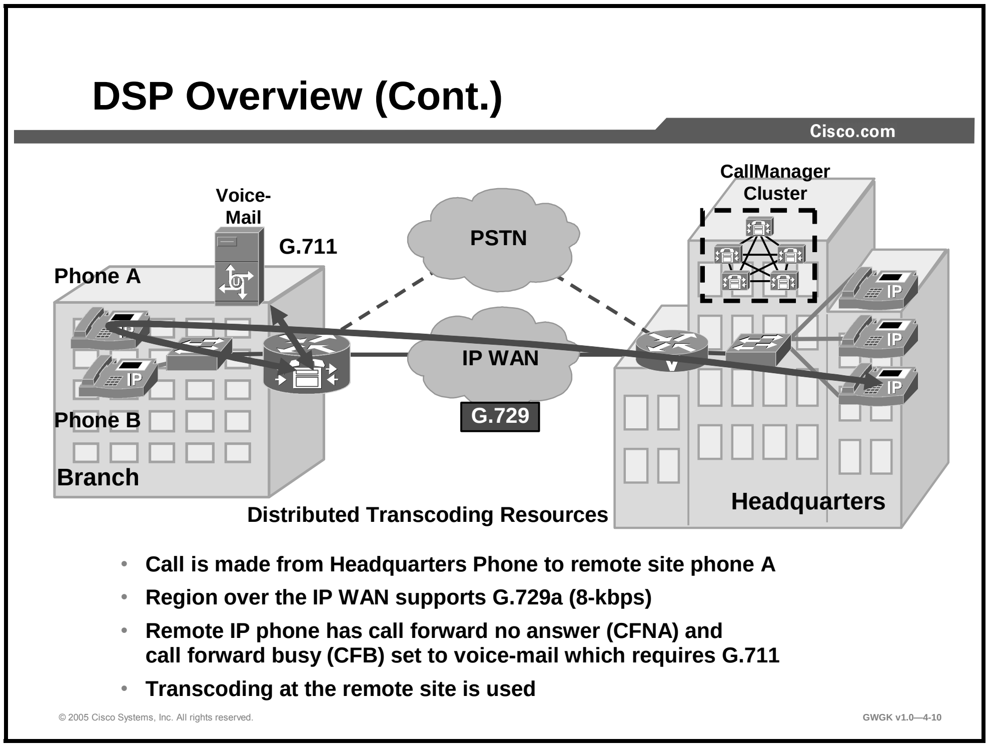
DSP Overview (Cont.)

Distributed Conferencing Resources

- **Conference between Phone A, Phone B, and 555-2222 using no voice traffic across WAN**
- **Uses DSPs in the branch router**

GWGK v1.0—4-9

This DSP deployment module is considered a distributed conferencing model where, unlike the previous scenario, voice traffic will not across the IP WAN. DSP resources have been deployed and invoked by Cisco CallManager preventing unnecessary IP WAN bandwidth consumption.



DSP Overview (Cont.)

Cisco.com

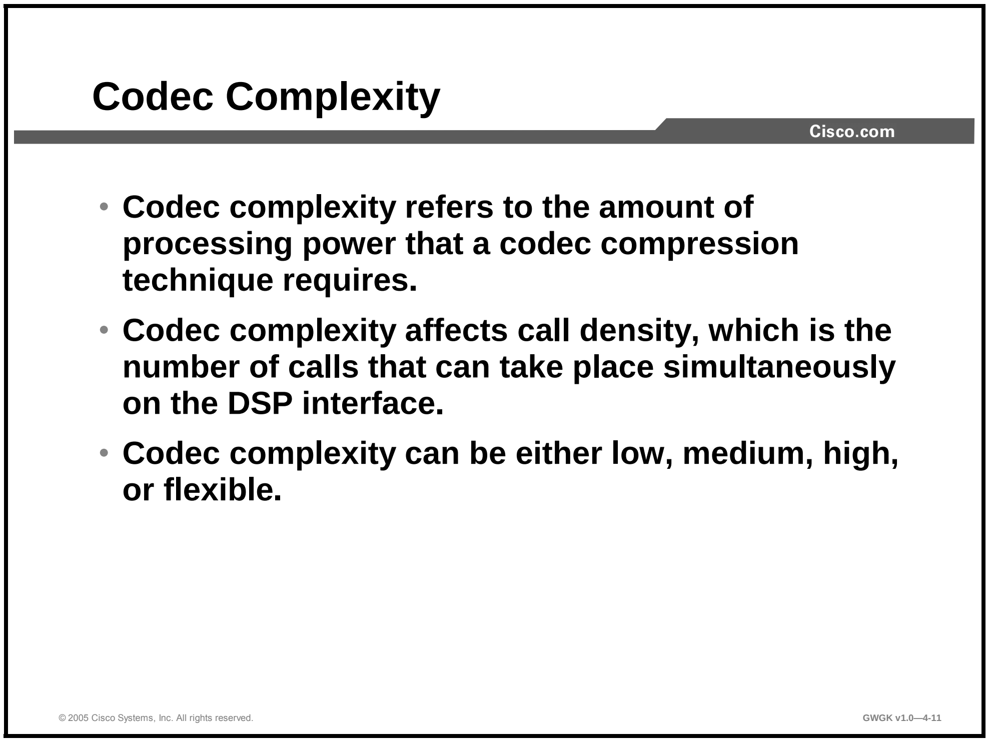
- Call is made from Headquarters Phone to remote site phone A
- Region over the IP WAN supports G.729a (8-kbps)
- Remote IP phone has call forward no answer (CFNA) and call forward busy (CFB) set to voice-mail which requires G.711
- Transcoding at the remote site is used

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—4-10

As the previous figure showed, a distributed conferencing model of DSP resource deployment at the remote, this figure shows a distributed transcoding module. In this figure a call is being made from a headquarters IP phone to a remote office IP phone. The remote branch IP phone device is configured so that call forward no answer (CFNA) and call forward busy (CFB) go to voice mail. In this scenario, the Cisco CallManager recognizes that there is a codec mismatch with voice mail. Cisco CallManager discovered by remote sites gateway capabilities negotiations capabilities exchange and requests transcoding services from the gateway of the remote office, which results in the call from the headquarters side staying at G.729A and the audio stream connecting to voice mail at G.711. It is important to note that the distributed deployment module relative to deploying conferencing, transcoding, and MTP services is to provide this service local to the site that can use them.

Codec Complexity

This topic describes DSP codec complexity.



Codec Complexity

Cisco.com

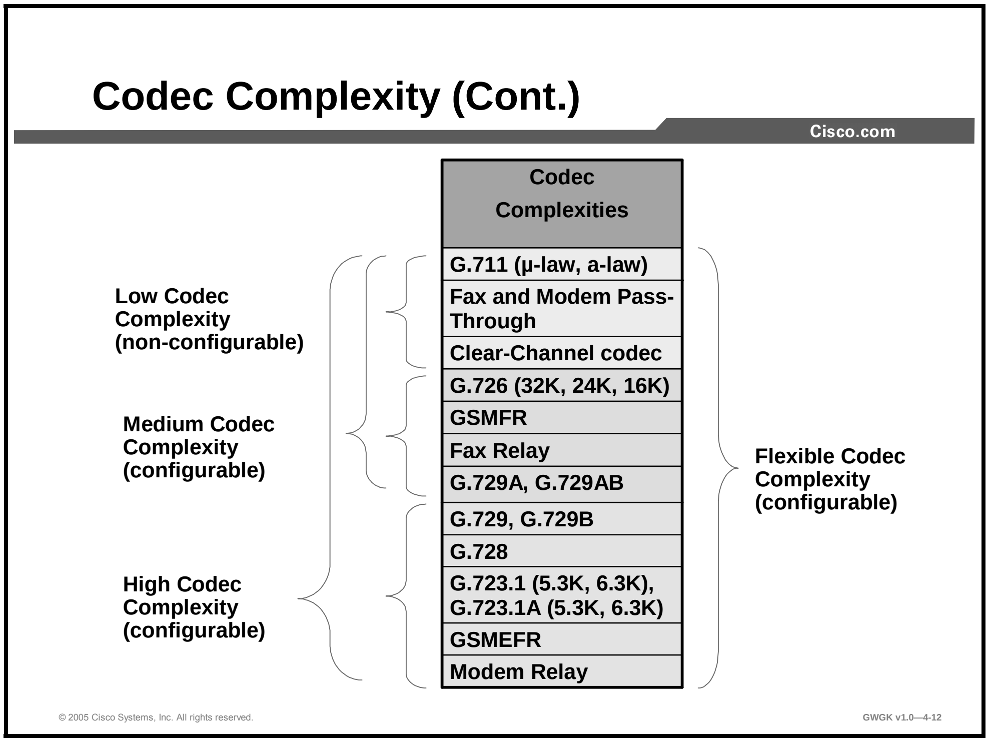
- Codec complexity refers to the amount of processing power that a codec compression technique requires.
- Codec complexity affects call density, which is the number of calls that can take place simultaneously on the DSP interface.
- Codec complexity can be either low, medium, high, or flexible.

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—4-11

To understand DSP allocation and deployment, understanding codec complexity and how the various levels of codec complexity impacts DSP use is important.

The number of DSPs available for voice termination, transcoding, conferencing, and MTP depends the level of codec complexity. There are specific codec compressions that reside under each complexity.



Codec Complexity (Cont.)

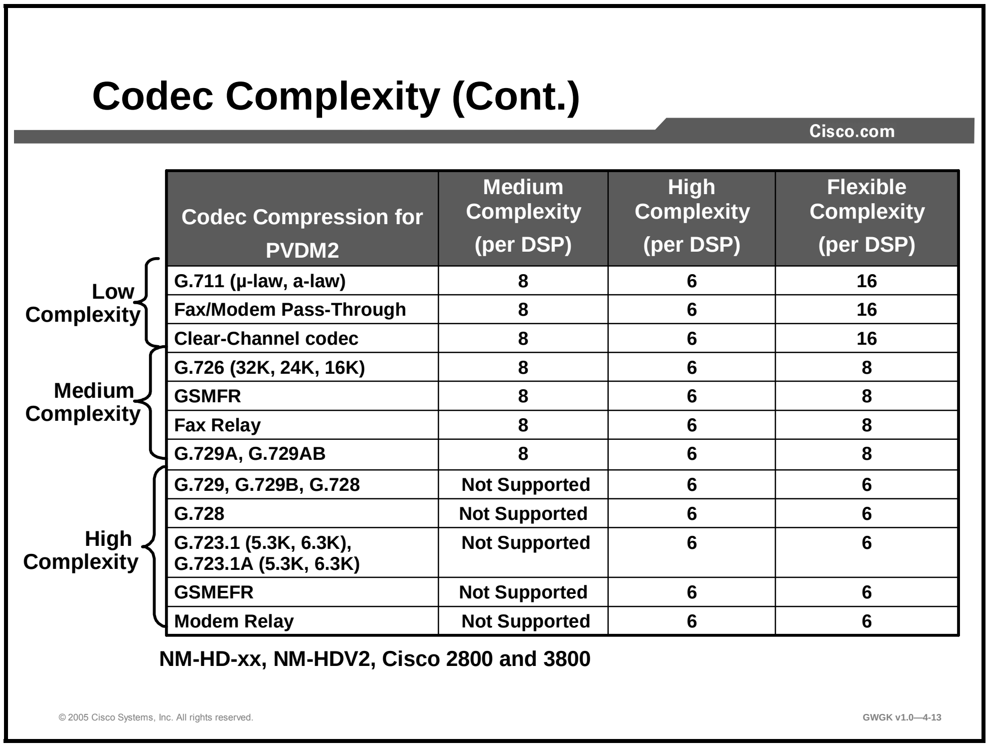
Codec Complexities
G.711 (μ-law, a-law)
Fax and Modem Pass-Through
Clear-Channel codec
G.726 (32K, 24K, 16K)
GSMFR
Fax Relay
G.729A, G.729AB
G.729, G.729B
G.728
G.723.1 (5.3K, 6.3K), G.723.1A (5.3K, 6.3K)
GSMEFR
Modem Relay

Low Codec Complexity (non-configurable)
Medium Codec Complexity (configurable)
High Codec Complexity (configurable)
Flexible Codec Complexity (configurable)

GWGK v1.0—4-12

This figure illustrates the various codecs supported and what codecs reside in what complexity. The main point with this figure is to point out that certain codec compressions reside within various codec complexities. For example to connect a call with one call leg being G.711ulaw and the other call leg being a variation of G.726, this connection require a medium complexity design or high complexity design. Conversely, a G.711ulaw to G.711ulaw call would be considered low complexity. Although low complexity is not a configurable option, medium complexity design would work in this case. Here is an example of where high complexity design would be required; one call leg that uses G.728 calls a far end user where the call leg uses G729. This call would require a high complexity design due to the codec compressions used for the call.

Medium codec complexity supports low complexity codecs and medium codec complexity compressions. High codec complexity supports low codec complexity and all medium complexity codecs, and requires the highest CPU use. Flex codec complexity supports all codec compressions. In reality, this complexity is not restricted to any one codec complexity (low, medium, or high), but is flexible enough to connect calls legs in the low, medium, or high codec range.



Codec Complexity (Cont.)

Cisco.com

	Codec Compression for PVDM2	Medium Complexity (per DSP)	High Complexity (per DSP)	Flexible Complexity (per DSP)
Low Complexity	G.711 (µ-law, a-law)	8	6	16
	Fax/Modem Pass-Through	8	6	16
	Clear-Channel codec	8	6	16
Medium Complexity	G.726 (32K, 24K, 16K)	8	6	8
	GSMFR	8	6	8
	Fax Relay	8	6	8
	G.729A, G.729AB	8	6	8
High Complexity	G.729, G.729B, G.728	Not Supported	6	6
	G.728	Not Supported	6	6
	G.723.1 (5.3K, 6.3K), G.723.1A (5.3K, 6.3K)	Not Supported	6	6
	GSMEFR	Not Supported	6	6
	Modem Relay	Not Supported	6	6

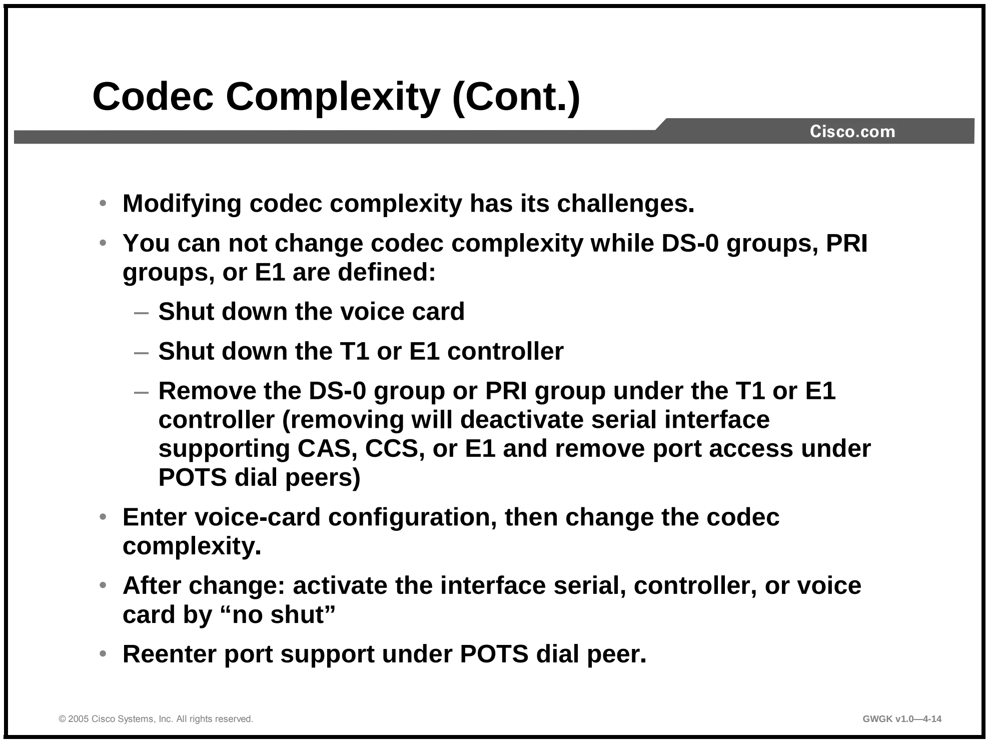
NM-HD-xx, NM-HDV2, Cisco 2800 and 3800

GWGK v1.0—4-13

This figure gives more detail about the various complexities shown in the previous figure. This figure outlines the different codec complexities and the number voice channels per DSP at the three configurable codec complexity levels (medium, high, and flex). This figure is specific only to the high density voice network module 2 (NM-HDV2), NM-HD-xx, and onboard slots on the Cisco 2800 and 3800 series routers and packet voice/data module 2 (PVDM2) SIMMs.

It takes two channels per call.

Note Low codec complexity is not configurable.



Codec Complexity (Cont.)

- Modifying codec complexity has its challenges.
- You can not change codec complexity while DS-0 groups, PRI groups, or E1 are defined:
  - Shut down the voice card
  - Shut down the T1 or E1 controller
  - Remove the DS-0 group or PRI group under the T1 or E1 controller (removing will deactivate serial interface supporting CAS, CCS, or E1 and remove port access under POTS dial peers)
- Enter voice-card configuration, then change the codec complexity.
- After change: activate the interface serial, controller, or voice card by “no shut”
- Reenter port support under POTS dial peer.

When modifying codec complexity on a router, make sure that you follow these steps as you will not be able to change the complexity as long as DS-0 or PRI groups are defined on the router. Trying to change codec complexity while DS-0s are active will result in the following errors:

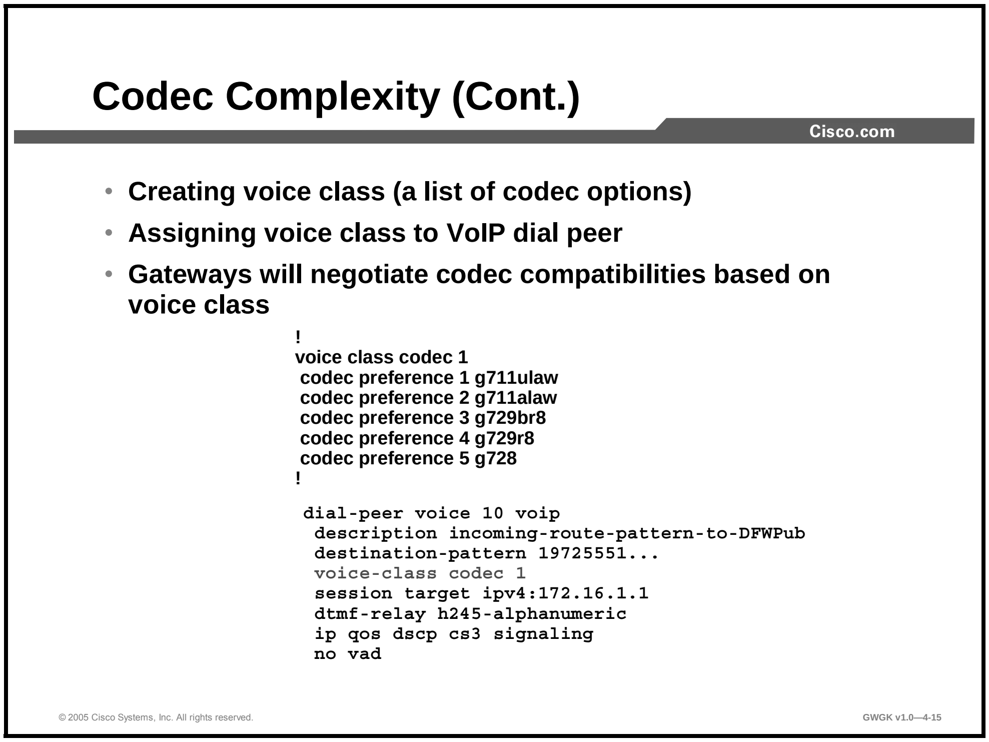
Example of error received from router console:

- % cannot change codec complexity while voice port exists.
- % please remove all DIGITAL voice ports on this voice card first
- % before changing codec complexity

Trying to change codex complexity while transcoding and conference bridging is active will generate this error message: “Cannot change codec complexity while transcoding sessions are configured on the card.”

Note This is an expected error that will appear from the router console.

The procedure for changing codec complexity does not apply to analog voice ports.



Codec Complexity (Cont.)

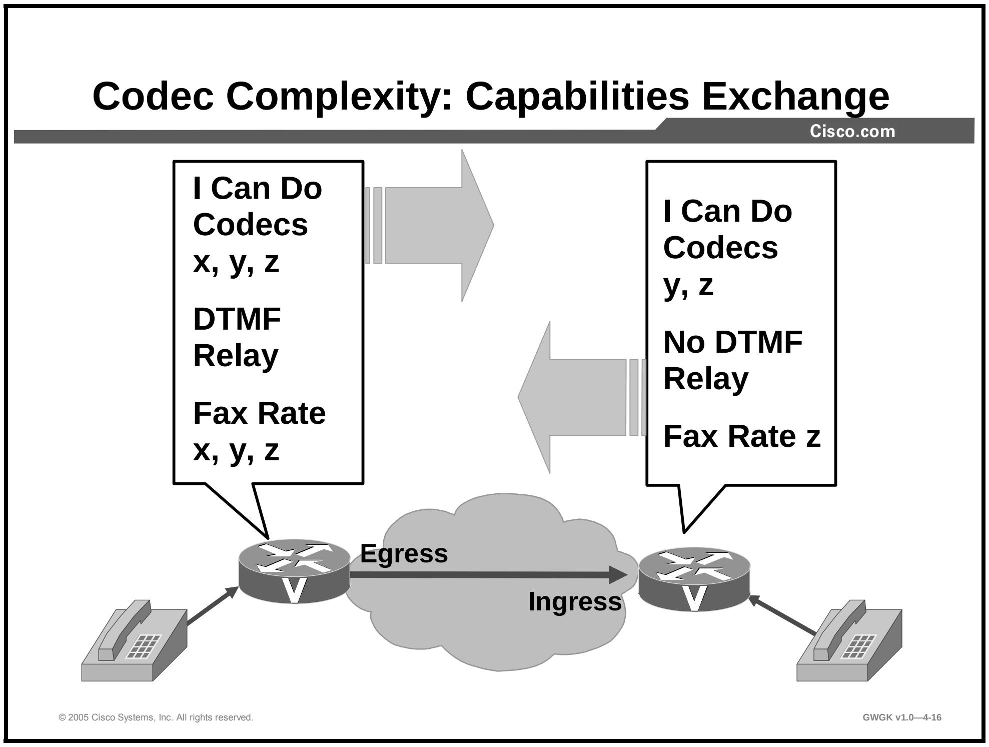
- Creating voice class (a list of codec options)
- Assigning voice class to VoIP dial peer
- Gateways will negotiate codec compatibilities based on voice class

```
!
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g711alaw
 codec preference 3 g729br8
 codec preference 4 g729r8
 codec preference 5 g728
!
 dial-peer voice 10 voip
  description incoming-route-pattern-to-DFWPub
  destination-pattern 19725551...
  voice-class codec 1
  session target ipv4:172.16.1.1
  dtmf-relay h245-alphanumeric
  ip qos dscp cs3 signaling
  no vad
```

Expanding on the previous figure, this figure shows the codec preference menu which refers to what gateways use to select or agree upon relative to codec selection. This menu is configurable and when used through the VoIP network is very effect in enduring gateways quickly agree upon a preferred codec for a VoIP call.

The **voice class codec (tag)** command shown in this figure sets up a menu of codec this gateway will support and communicate to other gateways upon call set. This menu will prefer G.711ulaw codec first, but has the options for other codec support. If for example the far end gateway only supports G.728, then the call would set up as a G.728 call.

Codecs used for PSTN calls are typically G.711. This does not always apply to PBX connections, where the PBX has the option to support other codec compressions.



Codec Complexity: Capabilities Exchange

Cisco.com

I Can Do Codecs x, y, z

DTMF Relay

Fax Rate x, y, z

I Can Do Codecs y, z

No DTMF Relay

Fax Rate z

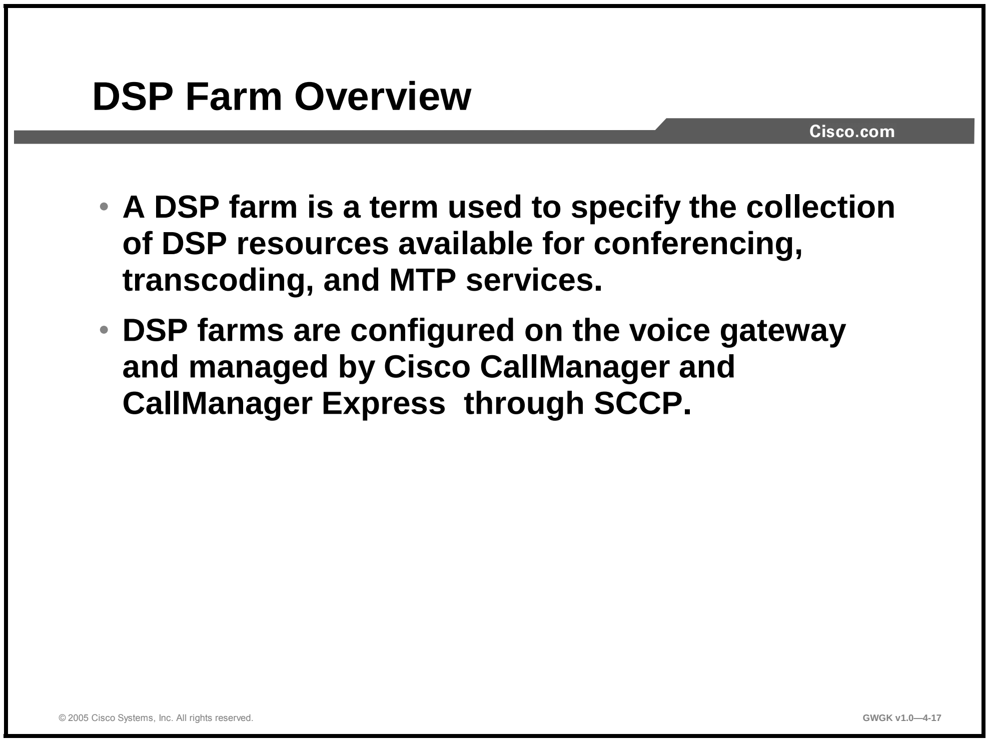
GWGK v1.0—4-16

The process of how gateways agree upon a selected codec during call setup is described here:

- Gateways can negotiate what codec they would rather use by providing a menu with a preferred compression. Providing a menu allows the far end gateway the choice to see if it can comply or agree on a codec that both gateways can live with. This codec negotiation process occurs in the H.245 capabilities exchange, as depicted in this figure. The following is a little more detail on the process.
- Codec negotiation allows the gateway to offer several codecs during the H.245 capability exchange phase and to ultimately settle on a single common codec during the call establishment phase. Offering several codecs increases the probability of establishing a connection because there will be a greater chance of overlapping voice capabilities between endpoints. Normally, only one codec can be specified when a dial peer is configured, but codec negotiation allows a prioritized list of codecs associated with a dial peer to be specified. During the call establishment phase the originating router will use the highest priority codec from a configured list. The far end gateway will either comply with the codec preferred or offer another at which time the near end gateway will adjust to comply.
- When a call is originated, all the codecs associated with the dial peer are sent to the terminating endpoint in the H.245 terminal capability set message. At the terminating endpoint, the gateway will advertise all the codecs that are available in firmware in its terminal capability set. If there is a need to limit the codecs advertised to a subset of the available codecs, a terminating dial peer must be matched that includes this subset. The **incoming called-number** command in dial-peer configuration mode can be used to force this match.

DSP Farm Overview

This topic gives an overview of DSP farming.



DSP Farm Overview

Cisco.com

- A DSP farm is a term used to specify the collection of DSP resources available for conferencing, transcoding, and MTP services.
- DSP farms are configured on the voice gateway and managed by Cisco CallManager and CallManager Express through SCCP.

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—4-17

The DSP farm uses the DSP resources in network modules on Cisco routers to provide voice-conferencing, transcoding, and hardware MTP services. DSP farming differs from the DSP sharing in that DSP sharing is a method where one network module can borrow DSP resources for another network module over the backplane of a gateway.

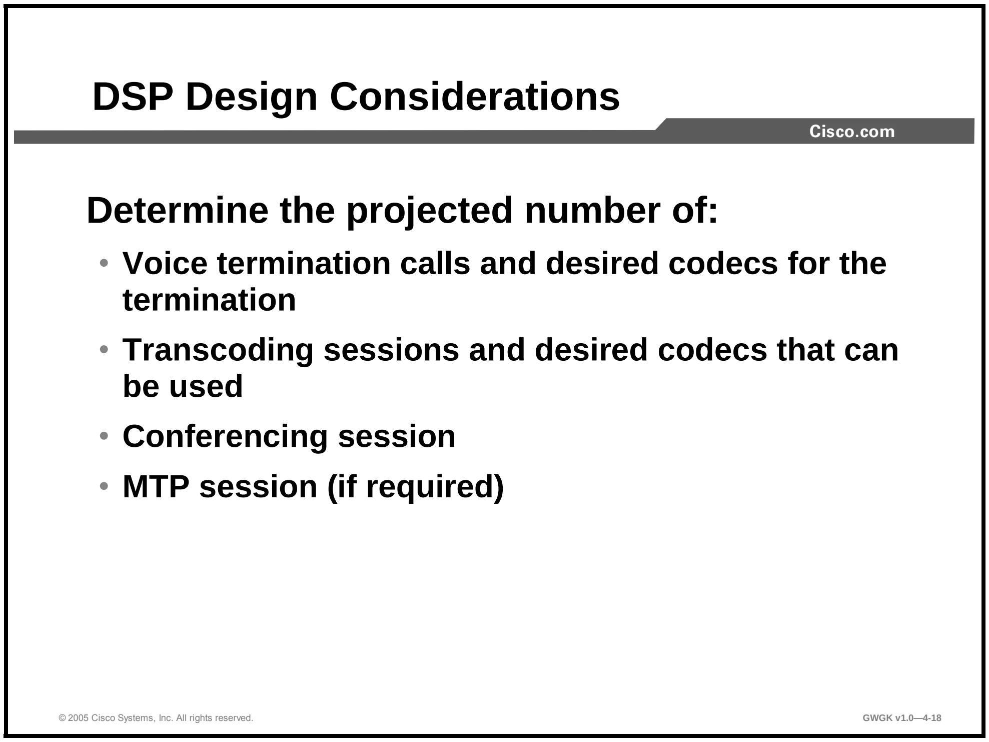
Restrictions for conferencing and transcoding for voice gateway routers are described here:

- DSP farm services communicate with Cisco CallManager using Skinny Client Control Protocol (SCCP); other protocols are not supported.
- DSP farm services are not supported for Cisco SRST
- Conferencing is not supported on the PVDM2-8. Transcoding and voice termination however are supported on the PVDM2-8. Conferencing, transcoding, and voice termination are supported on the PVDM2-16, PVDM2-32, PVDM2-48, and PVDM2-64.
- Conferencing is not supported on a Cisco 3640 using the NM-HD-1V, NM-HD-2V, or NM-HD-2VE.
- Simultaneous use of DSP farm services on the NM-HDV and NM-HDV2 is not supported.
- MTP services are not supported on the NM-HDV or NM-HDV-FARM.
- Dynamic conference and transcoding resource allocation is not supported.
- Fax is not supported for transcoding.
- Only one codec is supported for each MTP profile. To support multiple codecs, you must define a separate MTP profile for each codec.

- Hardware MTPs support only G.711a-law and G.711u-law. If you configure a profile as a hardware MTP, and you want to change the codec to other than G.711, you must first remove the hardware MTP by using the **no maximum sessions hardware** command.
- If an MTP call is received but MTP is not configured, transcoding DSP can be used, if resources are available.

DSP Design Considerations

This topic describes DSP design requirements.



DSP Design Considerations

Cisco.com

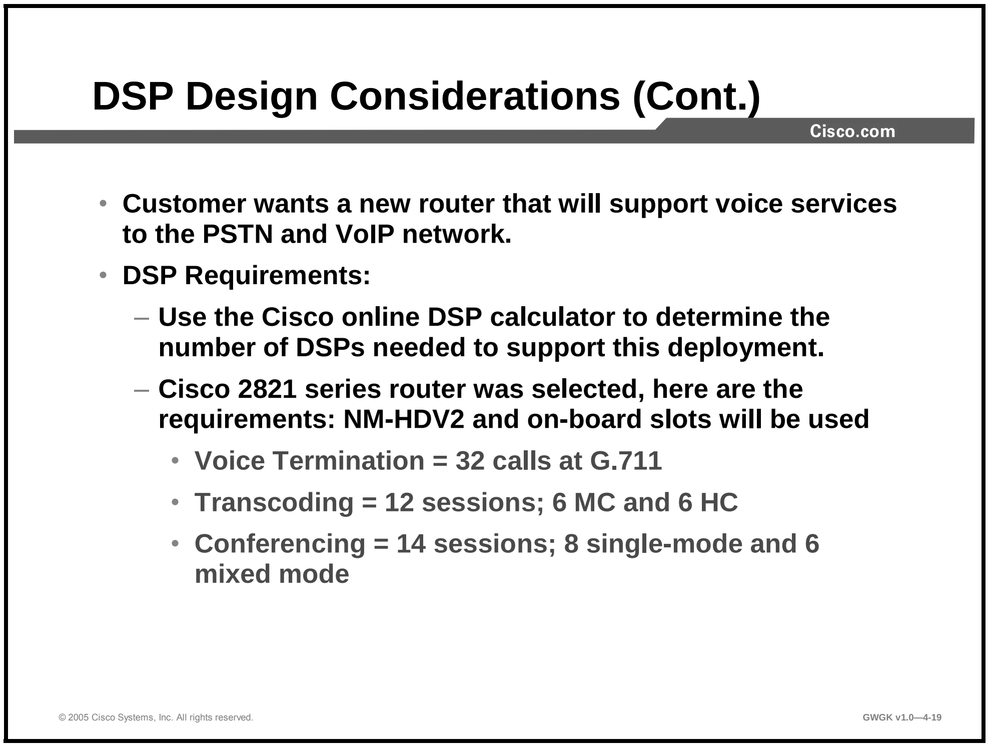
Determine the projected number of:

- **Voice termination calls and desired codecs for the termination**
- **Transcoding sessions and desired codecs that can be used**
- **Conferencing session**
- **MTP session (if required)**

GWGK v1.0—4-18

You must allocate DSP resources on two levels:

- **Level One:** This level is within the voice network module and occurs between the DSP farm and your voice trunk group that handles standard voice termination (for example, PRI group and or DS-0).
- **Level Two:** This level is within the DSP farm and occurs between transcoding and voice-conferencing services (transcoding is also used for MTP services).



DSP Design Considerations (Cont.)

Cisco.com

- **Customer wants a new router that will support voice services to the PSTN and VoIP network.**
- **DSP Requirements:**
  - **Use the Cisco online DSP calculator to determine the number of DSPs needed to support this deployment.**
  - **Cisco 2821 series router was selected, here are the requirements: NM-HDV2 and on-board slots will be used**
    - **Voice Termination = 32 calls at G.711**
    - **Transcoding = 12 sessions; 6 MC and 6 HC**
    - **Conferencing = 14 sessions; 8 single-mode and 6 mixed mode**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—4-19

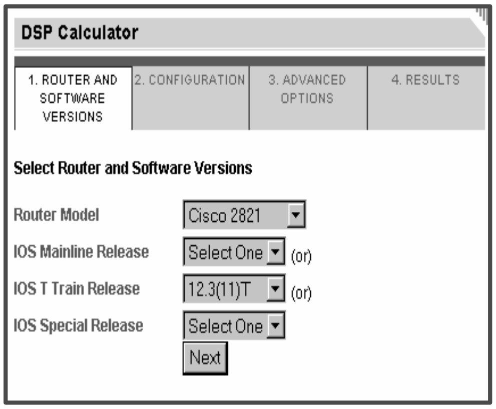
Cisco has made it easy to determine the number of DSPs required by providing a web based tool where the desired number of voice termination, transcoding, conferencing, and MTP sessions can be entered. The output of the data entered into this tool provides the combination of DSP resources to use along with a recommended configuration to support optimal, normal and worst case solutions.

This figure provides a scenario where a client wants to purchase a router and use the router to deploy voice services. The client wants to have two PRIs installed for voice termination; one PRI out of the two will used, the other will be used in the future. The client wants to have analog lines installed; eight FXS lines. The total voice termination channels needed is 32. The client also wants to support conferencing and transcoding. The client has indicated that they need six transcoding channels using high codec complexity, six channels using medium codec complexity, 8 single mode and 6 mixed mode conferences. The router of choice for the client is a Cisco 2821 running 12.3(11) T Cisco IOS software.

Using the Cisco online calculator the support person needs to determine what to purchase relative to DSPs for the client. For transcoding and conferencing sessions use the optional on-board option.

DSP Calculator

Cisco.com



Select Router and Software Versions

Router Model: Cisco 2821

IOS Mainline Release: Select One (or)

IOS T Train Release: 12.3(11)T (or)

IOS Special Release: Select One

- **Step 1: Router and software versions selection:**
  - **Select router model and IOS T train release**

Cisco DSP Calculator:
http://www.cisco.com/cgi-bin/Support/DSP/cisco_prodsel.pl

GWGK v1.0—4-20

This figure shows the starting webpage for determining DSP requirements for a specific router platform. This calculator tool will not provide configuration errors during the date entry mode. If entered data exceeds the platform DSP configuration, an error will be provided on the page showing a summary of the data entered. So it is important to know the router platform DSP limitations before starting the calculator.

Perform the following steps to determine DSP requirements for your router platform:

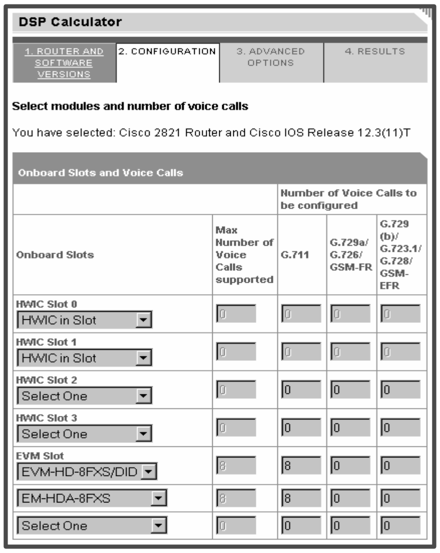
Step 1 Access the DSP Calculator.

Step 2 From the Router Model menu, select the platform.

Step 3 Select the IOS software that supports the platform.

Step 4 Select “Next.”

DSP Calculator (Cont.)



DSP Calculator

Select modules and number of voice calls

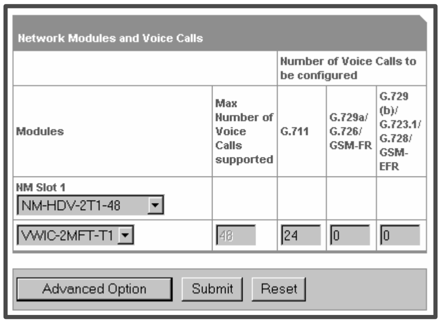
You have selected: Cisco 2821 Router and Cisco IOS Release 12.3(11)T

Onboard Slots and Voice Calls

		Number of Voice Calls to be configured		
Onboard Slots	**Max Number of Voice Calls supported**	**G.711**	**G.729a/ G.726/ GSM-FR**	**G.729 (b)/ G.723.1/ G.728/ GSM-EFR**
HWIC Slot 0 HWIC in Slot	0	0	0	0
HWIC Slot 1 HWIC in Slot	0	0	0	0
HWIC Slot 2 Select One	0	0	0	0
HWIC Slot 3 Select One	0	0	0	0
EVM Slot EVM-HD-8FXS/DID	8	8	0	0
EM-HDA-8FXS	8	8	0	0
Select One	0	0	0	0

- **Step 2: Configuration**
  - **Select the number of voice termination channels for on-board slots, voice cards, and NMs for Cisco 2821 platform using 12.3(11)T**

32 voice termination channels



Network Modules and Voice Calls

		Number of Voice Calls to be configured		
Modules	**Max Number of Voice Calls supported**	**G.711**	**G.729a/ G.726/ GSM-FR**	**G.729 (b)/ G.723.1/ G.728/ GSM-EFR**
NM Slot 1 NM-HDV-2T1-48				
VWIC-2MFT-T1	48	24	0	0

This figure shows the second step in determining the DSP requirements for voice termination on a Cisco 2821 series router. There two locations on this router for setting voice termination support, on-board slots and on the network modules. Follow these steps to complete scenario for DSP support for voice termination:

Step 1 Under the "On-Board Slots" column, use the pull down menu to select the voice card hardware.

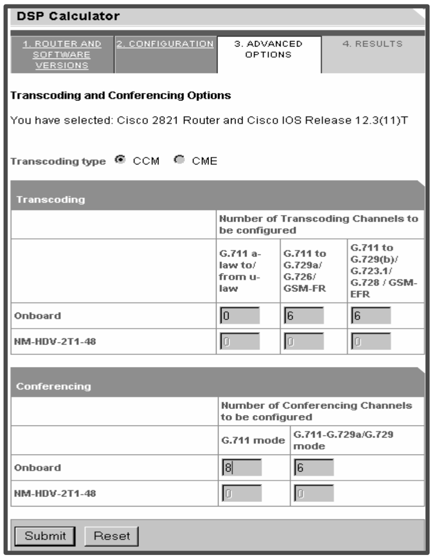
Step 2 Enter the "Number of Voice Calls to be configured."

Step 3 If a NM will be installed, use the pull down menu to select he appropriate hardware followed by selecting the "Number of Voice Calls to be configured."

Step 4 Go to setting up transcoding and conferencing by clicking on the Advanced Options button.

DSP Calculator (Cont.)

Cisco.com



Transcoding and Conferencing Options

You have selected: Cisco 2821 Router and Cisco IOS Release 12.3(11)T

Transcoding type ● CCM ○ CME

Transcoding

	Number of Transcoding Channels to be configured		
	G.711 a-law to/ from u-law	G.711 to G.729a/ G.726/ GSM-FR	G.711 to G.729(b)/ G.723.1/ G.728 / GSM-EFR
Onboard	0	6	6
NM-HDV-2T1-48	0	0	0

Conferencing

	Number of Conferencing Channels to be configured	
	G.711 mode	G.711-G.729a/G.729 mode
Onboard	8	6
NM-HDV-2T1-48	0	0

- **Step 3: Advanced options:**
  - **Transcoding Type: Cisco CallManager**
  - **Six high and six medium codec complexity**
  - **Eight single mode and six mixed mode conferences**
- **Submit to go to the Results page or reset the data entered**

GWGK v1.0—4-22

In continuing with the scenario, this figure shows the Advanced Option page for setting up the DSP requirements for transcoding and conferencing.

Step 1 Enter the “Number of Transcoding Channels to be configured.”

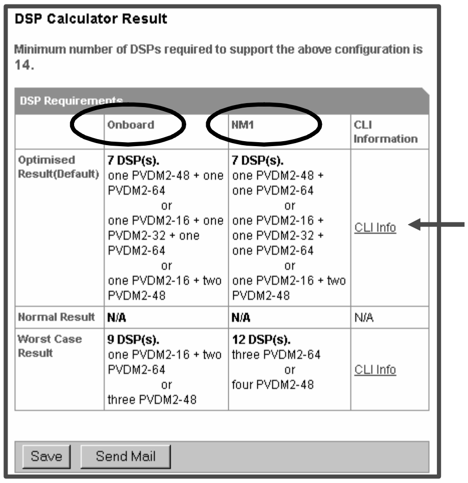
Step 2 Enter the “Number of Conferencing Channels to be configured.”

Step 3 Click-on “Submit.”

The requirements are to use the optional onboard slots for transcoding and conferencing.

DSP Calculator (Cont.)

Cisco.com



DSP Calculator Result

Minimum number of DSPs required to support the above configuration is 14.

DSP Requirements

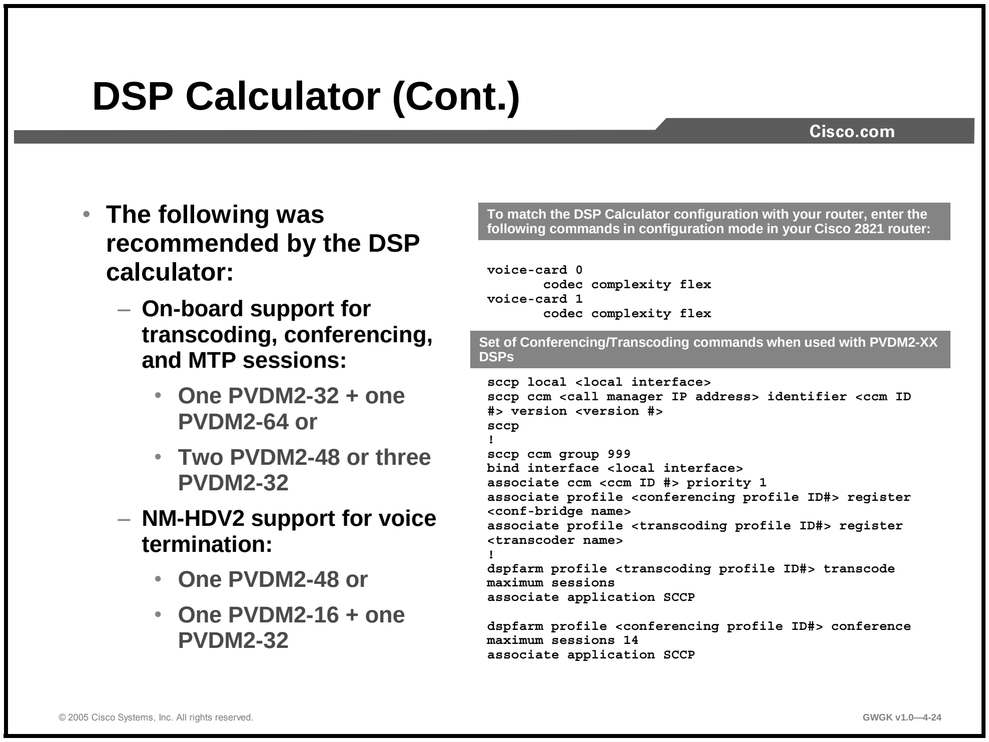
	Onboard	NM1	CLI Information
Optimised Result(Default)	**7 DSP(s).** one PVDM2-48 + one PVDM2-64 or one PVDM2-16 + one PVDM2-32 + one PVDM2-64 or one PVDM2-16 + two PVDM2-48	**7 DSP(s).** one PVDM2-48 + one PVDM2-64 or one PVDM2-16 + one PVDM2-32 + one PVDM2-64 or one PVDM2-16 + two PVDM2-48	CLI Info
Normal Result	**N/A**	**N/A**	N/A
Worst Case Result	**9 DSP(s).** one PVDM2-16 + two PVDM2-64 or three PVDM2-48	**12 DSP(s).** three PVDM2-64 or four PVDM2-48	CLI Info

- **Step 4: Results**
  - **This output provides PVDM2 recommendations for on-board slots and for the network module**
- **Select CLI Info to display the actual IOS configuration entered on the router**

GWGK v1.0—4-23

This figure shows the last step in determining the DSP requirements for the specific platform as outlined in the scenario.

The DSP Calculator tries to provide the best solution for DSP use with ix based on the data entered. Presented here are three options to choose from this page: Optimal, Worst Case. Normal Results was not offered, but typically, this offering uses medium complexity and the solution depends on the platform data entry. Optimized Result (default) will offer an optimized number of DSPs hardware to use as well as the optimal configuration to enter in IOS software to support the DSPs. This is typically flexible complexity on the newer platforms. Worst Case Results gives the worst case for DSP use. Typically, Worst Case this is high complexity.



DSP Calculator (Cont.)

Cisco.com

- **The following was recommended by the DSP calculator:**
  - **On-board support for transcoding, conferencing, and MTP sessions:**
    - **One PVDM2-32 + one PVDM2-64 or**
    - **Two PVDM2-48 or three PVDM2-32**
  - **NM-HDV2 support for voice termination:**
    - **One PVDM2-48 or**
    - **One PVDM2-16 + one PVDM2-32**

To match the DSP Calculator configuration with your router, enter the following commands in configuration mode in your Cisco 2821 router:

```
voice-card 0
       codec complexity flex
voice-card 1
       codec complexity flex
```

Set of Conferencing/Transcoding commands when used with PVDM2-XX DSPs

```
sccp local <local interface>
sccp ccm <call manager IP address> identifier <ccm ID
#> version <version #>
sccp
!
sccp ccm group 999
bind interface <local interface>
associate ccm <ccm ID #> priority 1
associate profile <conferencing profile ID#> register
<conf-bridge name>
associate profile <transcoding profile ID#> register
<transcoder name>
!
dspfarm profile <transcoding profile ID#> transcode
maximum sessions
associate application SCCP

dspfarm profile <conferencing profile ID#> conference
maximum sessions 14
associate application SCCP
```

GWGK v1.0—4-24

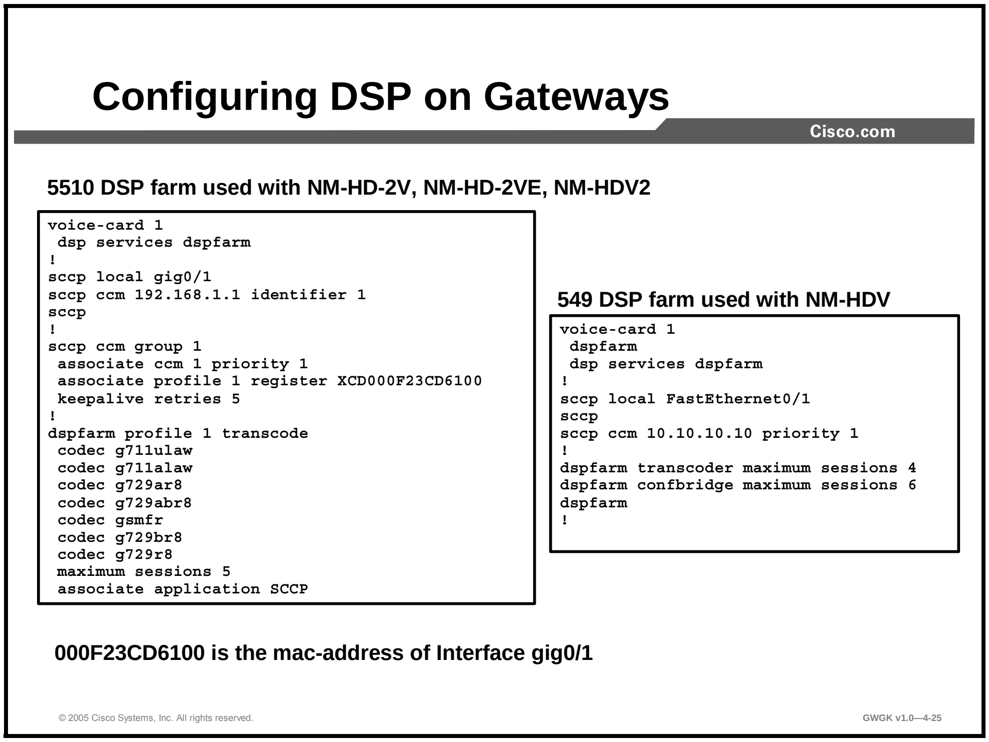
This figure shows what is needed from a PVDM2-xx perspective to meet the requirements for the client. This is the Optimal Result option. Although there is ample DSP resources for voice termination, transcoding will share resources and vice versa if needed. Conferencing will use dedicated resources. Although MTP support is not an option in the DSP Calculator, MTP requirements will share DSP resources with transcoding resource.

In this figure, flexible complexity is displayed as being part of the IOS software output. This output will not be seen in the router configuration as this is the default configuration.

One comment on using flexible complexity; with oversubscription in flex mode, you can connect or configure in the case of DS-0 groups and PRI groups more voice channels to the module than the DSPs can accommodate. If all voice channels should go active simultaneously, the DSPs will be oversubscribed and calls that are unable to allocate a DSP resource will fail to connect. This is very important to consider because emergency calls could possibly get blocked. The alternative to flex mode is of course to set your complexity to medium or high. There are no oversubscription issues with medium or high complexity that could cause calls from connecting.

Configuring DSPs on a Gateways

This topic describes how to configure DSP farms on gateways.



Configuring DSP on Gateways

5510 DSP farm used with NM-HD-2V, NM-HD-2VE, NM-HDV2

```
voice-card 1
 dsp services dspfarm
!
sccp local gig0/1
sccp ccm 192.168.1.1 identifier 1
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 1 register XCD000F23CD6100
 keepalive retries 5
!
dspfarm profile 1 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec gsmfr
 codec g729br8
 codec g729r8
 maximum sessions 5
 associate application SCCP
```

549 DSP farm used with NM-HDV

```
voice-card 1
 dspfarm
 dsp services dspfarm
!
sccp local FastEthernet0/1
sccp
sccp ccm 10.10.10.10 priority 1
!
dspfarm transcoder maximum sessions 4
dspfarm confbridge maximum sessions 6
dspfarm
!
```

000F23CD6100 is the mac-address of Interface gig0/1

There various ways to configure DSP Farms on a gateway. Presented in this figure are two. These gateway configurations assume the gateways are using network voice modules NM-HDV and NM-HDV2. 549 Texas Instrument DSPs are used with NM-HDV and 5510 Texas Instrument DSPs are used with NM-HDV2 voice modules. As you can see each are configured differently.

Configuring a DSP Farm—Common Steps

Perform this task to enable SCCP on the local interface that a DSP farm uses to register with Cisco CallManager. This step is the same for either DSP type.

Step 1 **enable**

Step 2 **configure terminal**

Step 3 sccp ccm {***ip-address*** | ***dns***} identifier ***identifier-number*** [port ***port-number***] [version ***version-number***] or sccp ccm {*ip-address* | *dns*} priority *priority* [port *port-number*] [version *version-number*]

Step 4 sccp local ***interface-type interface-number***

Step 5 **sccp**

Step 6 **sccp ip precedence** ***value***

Step 7 **exit**

Configuring a DSP Farm on the NM-HDV2 or NM-HD-1V/2V/2VE

Perform this procedure to define a DSP farm on the NM-HDV2, NM-HD-1V, NM-HD-2V, or NM-HD-2VE. You must configure each conferencing, transcoding, and MTP profile separately.

Note This procedure requires Cisco IOS Release 12.3(8)T or later.

Step 1 **enable**

Step 2 **configure terminal**

Step 3 voice-card ***slot***

Step 4 **dsp services dspfarm**

Step 5 **exit**

Step 6 dspfarm profile ***profile-identifier*** {conference | mtp | transcode}

Step 7 description ***text***

Step 8 codec ***codec-type***

Step 9 maximum sessions ***number*** or maximum sessions {hardware | software} *number*

Step 10 **associate application sccp**

Step 11 **no shutdown**

Step 12 **exit**

Step 13 **gateway**

Step 14 timer receive-rtp ***seconds***

Step 15 end or return to step 6 to continue configuring DSP farm profiles

Associating a DSP Farm Profile to a Cisco CallManager Group

You must configure the Cisco CallManager group and create an association between the DSP farm profile and the Cisco CallManager group. Do so by performing the following steps.

Note This procedure requires Cisco IOS Release 12.3(8)T or later.

Step 1 **enable**

Step 2 **configure terminal**

Step 3 sccp ccm group ***group-number***

Step 4 associate ccm ***identifier-number*** priority ***priority-number***

Step 5 associate profile ***profile-identifier*** register ***device-name***

Step 6 bind interface ***interface-type interface-number***

Step 7 description ***string***

Step 8 **end**

Modifying Default Settings for SCCP Connection to Cisco CallManager

Perform these steps to tune the performance of the SCCP connection between the DSP farm and Cisco CallManager.

Note The optimum settings for these commands depend on your platform and individual network characteristics. Modify the defaults to meet your performance requirements.

Step 1 **enable**

Step 2 **configure terminal**

Step 3 sccp ccm group ***group-number***

Step 4 connect interval ***seconds***

Step 5 connect retries ***number***

Step 6 keepalive retries ***number***

Step 7 keepalive timeout ***seconds***

Step 8 registration retries ***retry-attempts***

Step 9 registration timeout ***seconds***

Step 10 switchover method {graceful **|** immediate}

Step 11 switchback method {graceful **|** guard [***timeout-value***] | immediate **|** uptime ***uptime-value***}

Step 12 switchback interval ***seconds***

Step 13 **end**

Configuring Conferencing and Transcoding on NM-HVD voice modules

To configure conferencing and transcoding on NM-HVD voice modules, perform the following steps:

Step 1 **enable**

Step 2 **configure terminal**

Step 3 **voice-card** ***slot***

Step 4 **dsp services dspfarm**

Step 5 **exit**

Step 6 **dspfarm confbridge maximum sessions** ***number***

Step 7 **dspfarm transcoder maximum sessions** ***number***

Step 8 **dspfarm**

Step 9 **exit**

Verifying DSP Farm Configuration

To verify conferencing, transcoding, and MTP services, perform the following steps.

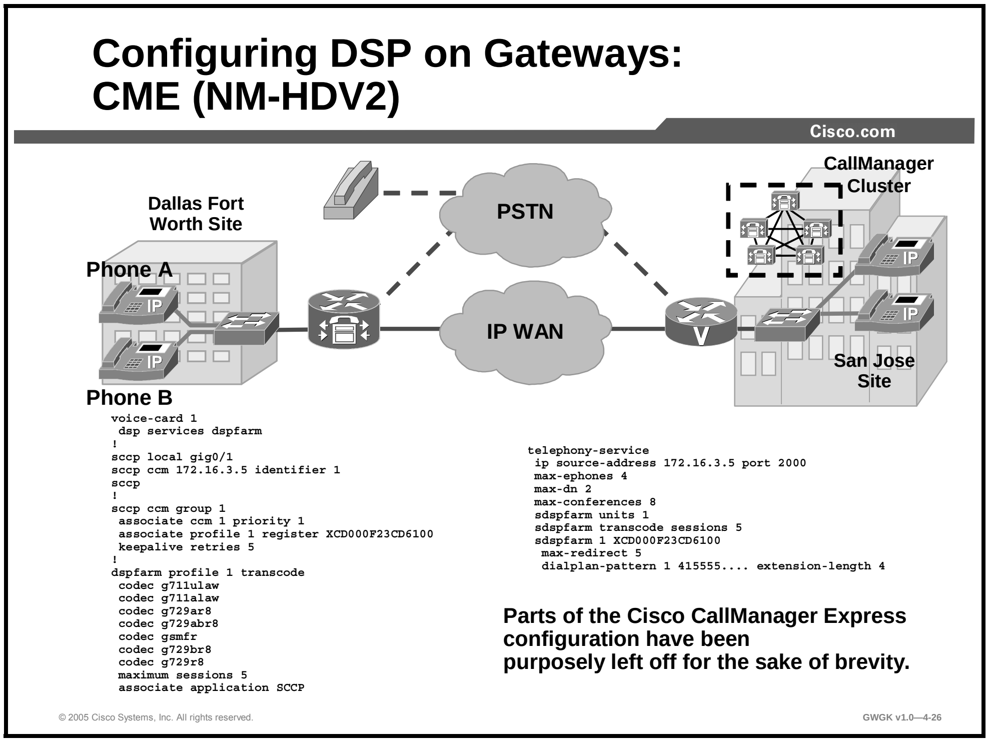
Step 1 Enter **show sccp connections** to show the number of active calls.

Step 2 Enter **show dspfarm all** to show the number of DSP channels.

Step 3 Enter **show media resource status** to show the types of services used and whether those services are registered with Cisco CallManager Express or Cisco CallManager.

Step 4 Enter **show sccp ccm group** to show the specifics relative to the status of what was configured under SCCP configuration on the gateway.

Step 5 Enter **show dspfarm profile [*profile-identifier*]** to show the DSP farm configuration as it relates to the profiles you configured. This command will show whether the services are registered to Cisco CallManager Express or Cisco CallManager.



Configuring DSP on Gateways: CME (NM-HDV2)

```
voice-card 1
 dsp services dspfarm
!
sccp local gig0/1
sccp ccm 172.16.3.5 identifier 1
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 1 register XCD000F23CD6100
 keepalive retries 5
!
dspfarm profile 1 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec gsmfr
 codec g729br8
 codec g729r8
 maximum sessions 5
 associate application SCCP
```

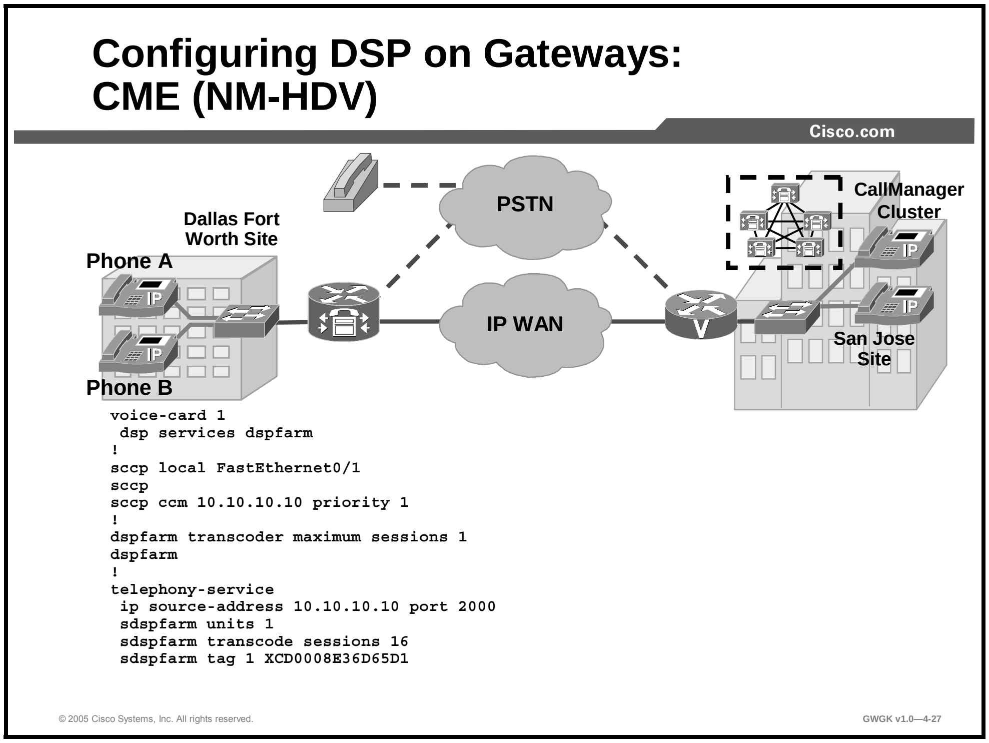
```
telephony-service
 ip source-address 172.16.3.5 port 2000
 max-ephones 4
 max-dn 2
 max-conferences 8
 sdspfarm units 1
 sdspfarm transcode sessions 5
 sdspfarm 1 XCD000F23CD6100
  max-redirect 5
  dialplan-pattern 1 415555.... extension-length 4
```

Parts of the Cisco CallManager Express configuration have been purposely left off for the sake of brevity.

GWGK v1.0—4-26

This figure shows the configuration setup for Cisco CallManager Express that has a NM-HVD2. If the gateway used a NM-HDV module the configuration is slightly different.

- **sdspfarm units:** Specifies the maximum number of DSP farms that can be registered to Cisco CallManager Express. A maximum of 5 DSP farms can be configured.
- **sdspfarm transcode sessions:** Specifies maximum transcoding sessions supported across all DSP farms registered to Cisco CallManager Express. A maximum of 128 transcoding sessions can be configured.
- **sdspfarm tag:** Specifies device name of DSP farm. The device name is “MTP” followed by MAC address of DSP source interface.



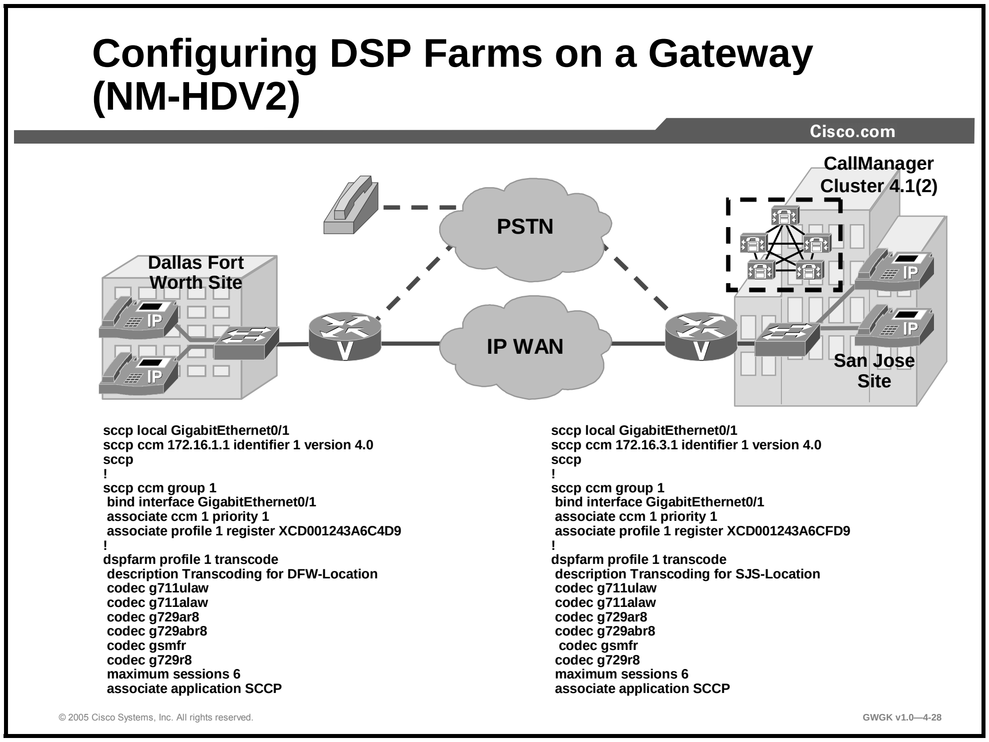
Configuring DSP on Gateways: CME (NM-HDV)

```
voice-card 1
 dsp services dspfarm
!
sccp local FastEthernet0/1
sccp
sccp ccm 10.10.10.10 priority 1
!
dspfarm transcoder maximum sessions 1
dspfarm
!
telephony-service
 ip source-address 10.10.10.10 port 2000
 sdspfarm units 1
 sdspfarm transcode sessions 16
 sdspfarm tag 1 XCD0008E36D65D1
```

GWGK v1.0—4-27

This figure shows a configuration sample of a DSP farm configured on a gateway using NM-HDV voice module. You would use the same configuration shown above on non-Cisco CallManager Express gateways except for the configuration under the telephony-service. This is specific to Cisco CallManager Express only.

If at anytime you are configuring your DSP Farm and show a maximum session number to be zero and you know you have enough DSPs you might recheck the codec complexity mode and make sure you have the correctly DSP configurations.



Configuring DSP Farms on a Gateway (NM-HDV2)

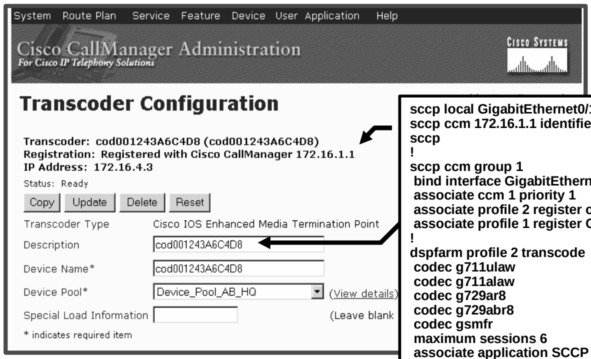
```
sccp local GigabitEthernet0/1
sccp ccm 172.16.1.1 identifier 1 version 4.0
sccp
!
sccp ccm group 1
 bind interface GigabitEthernet0/1
 associate ccm 1 priority 1
 associate profile 1 register XCD001243A6C4D9
!
dspfarm profile 1 transcode
 description Transcoding for DFW-Location
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec gsmfr
 codec g729r8
 maximum sessions 6
 associate application SCCP
```

```
sccp local GigabitEthernet0/1
sccp ccm 172.16.3.1 identifier 1 version 4.0
sccp
!
sccp ccm group 1
 bind interface GigabitEthernet0/1
 associate ccm 1 priority 1
 associate profile 1 register XCD001243A6CFD9
!
dspfarm profile 1 transcode
 description Transcoding for SJS-Location
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
  codec gsmfr
 codec g729r8
 maximum sessions 6
 associate application SCCP
```

The figure shows two sites: Dallas and San Jose. Each site has its own hardware transcoding services located on their gateways. Both transcoding services are registered with the centralized Cisco CallManager cluster. Depending on whether gateway has a NM-HDV or NM-HDV2 depends on how you configure DSP farms in Cisco IOS software.

Configuring DSP Farms in Cisco CallManager

Cisco.com



Transcoder Configuration

Transcoder: cod001243A6C4D8 (cod001243A6C4D8)
Registration: Registered with Cisco CallManager 172.16.1.1
IP Address: 172.16.4.3

Status: Ready

Transcoder Type: Cisco IOS Enhanced Media Termination Point
Description: cod001243A6C4D8
Device Name*: cod001243A6C4D8
Device Pool*: Device_Pool_AB_HQ (View details)
Special Load Information: (Leave blank

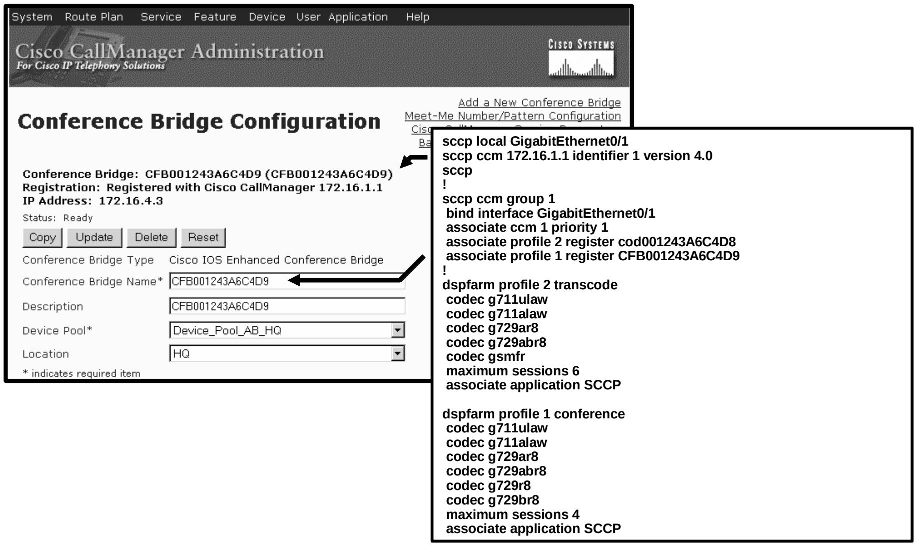
* indicates required item

```
sccp local GigabitEthernet0/1
sccp ccm 172.16.1.1 identifier 1 version 4.0
sccp
!
sccp ccm group 1
 bind interface GigabitEthernet0/1
 associate ccm 1 priority 1
 associate profile 2 register cod001243A6C4D8
 associate profile 1 register CFB001243A6C4D9
!
dspfarm profile 2 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec gsmfr
 maximum sessions 6
 associate application SCCP
!
dspfarm profile 1 conference
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec g729r8
 codec g729br8
 maximum sessions 4
 associate application SCCP
```

This figure shows a Cisco IOS Enhanced Media Termination Point transcoder configuration setup. The name used in this setup matched that on the gateway listed under **sccp ccm group**.

To determine what transcoder type to use per hardware, use the Cisco CallManager Help page. The Help page per "For this Page" provides the configuration variables associated with the various transcoder types.

Configuring DSP Farms in Cisco CallManager (Conference Bridge)


System
Route Plan
Service
Feature
Device
User
Application
Help
Cisco CallManager Administration
For Cisco IP Telephony Solutions
Cisco Systems
Add a New Conference Bridge
Meet-Me Number/Pattern Configuration
Copy
Update
Delete
Reset

Conference Bridge Configuration

Conference Bridge: CFB001243A6C4D9 (CFB001243A6C4D9)
Registration: Registered with Cisco CallManager 172.16.1.1
IP Address: 172.16.4.3
Status: Ready

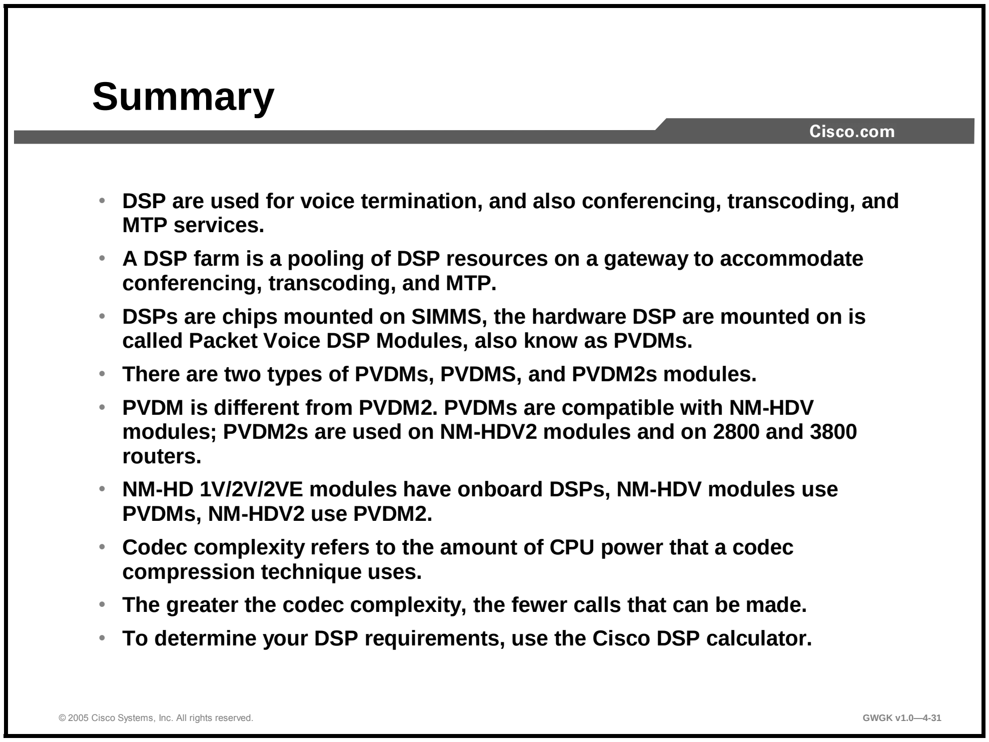
Conference Bridge Type: Cisco IOS Enhanced Conference Bridge
Conference Bridge Name*: CFB001243A6C4D9
Description: CFB001243A6C4D9
Device Pool*: Device_Pool_AB_HQ
Location: HQ
* indicates required item

```
sccp local GigabitEthernet0/1
sccp ccm 172.16.1.1 identifier 1 version 4.0
sccp
!
sccp ccm group 1
 bind interface GigabitEthernet0/1
 associate ccm 1 priority 1
 associate profile 2 register cod001243A6C4D8
 associate profile 1 register CFB001243A6C4D9
!
dspfarm profile 2 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec gsmfr
 maximum sessions 6
 associate application SCCP

dspfarm profile 1 conference
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec g729r8
 codec g729br8
 maximum sessions 4
 associate application SCCP
```

This figure shows the Cisco IOS Enhanced Conference Bridge configuration in Cisco CallManager. Notice the DSP farm configuration on the gateway and how it corresponds to the configuration in Cisco CallManager. When configuring hardware conference bridges in Cisco CallManager use the Help page “For this Page” to assist you in the naming and configuration setup for the various gateways network module types.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

- DSP are used for voice termination, and also conferencing, transcoding, and MTP services.
- A DSP farm is a pooling of DSP resources on a gateway to accommodate conferencing, transcoding, and MTP.
- DSPs are chips mounted on SIMMS, the hardware DSP are mounted on is called Packet Voice DSP Modules, also know as PVDMs.
- There are two types of PVDMs, PVDMS, and PVDM2s modules.
- PVDM is different from PVDM2. PVDMs are compatible with NM-HDV modules; PVDM2s are used on NM-HDV2 modules and on 2800 and 3800 routers.
- NM-HD 1V/2V/2VE modules have onboard DSPs, NM-HDV modules use PVDMs, NM-HDV2 use PVDM2.
- Codec complexity refers to the amount of CPU power that a codec compression technique uses.
- The greater the codec complexity, the fewer calls that can be made.
- To determine your DSP requirements, use the Cisco DSP calculator.

GWGK v1.0—4-31

References

For additional information, refer to these resources:

Configuring Conferencing and Transcoding (NM-HDV):

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/ccm_c/intcnf2.htm#wp1052086

Configuring Enhanced Conferencing and Transcoding (NM-HDV2 or NM-HD-1V/2V/2VE)

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/ccm_c/intcnf2.htm#wp1059545

Configuring Conferencing and Transcoding (PVDM-256K):

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/ccm_c/intcnf2.htm#wp1051497

CallManager 4.0(1) and above and IOS Gateway DSP Farm Configuration Example:

- http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/products_configuration_example09186a0080334294.shtml

Cisco DSP Calculator Tool:

- http://www.cisco.com/cgi-bin/Support/DSP/cisco_prodsel.pl

Connecting Network Module in Gateway Routers:

- http://cco/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/nm_inst/nm-doc/conntvoi.htm

IP Communications High-Density Digital Voice/Fax Network Module:

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/hdd_vfnm.htm#wp1049156

DSP on NM-HDV2 Functionality Verification for 2600XM/2691/2800/3700/3800 Platforms:

- http://www.cisco.com/en/US/partner/tech/tk652/tk653/technologies_tech_note09186a008039c316.shtml

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) What are the two purposes of transcoding? (Choose two.) (Source:)

A) improve SCCP support

B) save on bandwidth

C) enable communications between different devices

D) PBX phone support

Q2) Which is a valid transcoding operation? (Source:)

A) G.723.1 to G.729a

B) G.729a to G.723.1

C) G.729a to G.729a

D) G.711 to G.729a

Q3) The NM-HDV network module can be populated with up to five PVDMs. Which of the following is not true regarding the DSPs used for the NM-HDV? (Choose two.) (Source:)

A) The NM-HDV can only use the PVDM-12 SIMM.
B) The DSPs use the C549 technology.
C) A single DSP can be shared for multiple functions.
D) Each PVDM SIMM provides three DSPs.

Q4) The NM-HDV supports up to how many transcoding sessions? (Source:)

A) 45
B) 60
C) 90
D) The NM-HDV does not support transcoding.

Q5) The NM-HDV uses which kind of DSP? (Source:)

A) TI-549
B) PVDM
C) NM-FARM-C36, C54, and C90
D) The NM-HDV does not support DSPs.

Q6) Medium codec complexity for NM-HDV (TI-549) supports how many voice channels per DSP? (Source:)

A) 8
B) 6
C) 16
D) 4

Q7) Medium codec complexity for NM-HDV2 (TI-5510) supports how many voice channels per DSP? (Source:)

A) 8
B) 6
C) 16
D) 4

Q8) High codec complexity for NM-HDV (TI-549) supports how many voice channels per DSP? (Source:)

A) 8
B) 6
C) 2
D) 4

Q9) Flex codec complexity for NM-HDV (TI-549) supports how many voice channels per DSP? (Source:)

A) 8
B) 6
C) 16
D) NM-HDV (TI-549) does not support DSP.

Q10) Terminal endpoint capabilities are exchanged through H.245 capabilities exchange process. When does this negotiation of codecs take place? (Source:)

A) before the establishment of call setup
B) just before the open logical channels are sent and received
C) after RTP streams have been established, assuming caps are not renegotiated
D) during the Cisco CallManager setup of transcoding

Q11) When one NM-HVD2 requests that another NM-HVD2 use DSP resources, what is this action called? (Choose two.) (Source:)

A) **network-clock-participate**
B) **no dspfarm**
C) codec complexity match
D) This action is not supported.

Lesson Self-Check Answer Key

Q1)	B, C
Q2)	D
Q3)	B, D
Q4)	B
Q5)	A, B, C, D
Q6)	D
Q7)	A
Q8)	C
Q9)	D
Q10)	B
Q11)	A, C

Lesson 3

Toolkit Command Language

Overview

This lesson discusses what Toolkit Command Language (TCL) interactive voice response (IVR) is. You will learn how to configure TCL scripts on a gateway, how to apply the scripts to the gateway, what commands to use to tell if the TCL scripts are running correctly.

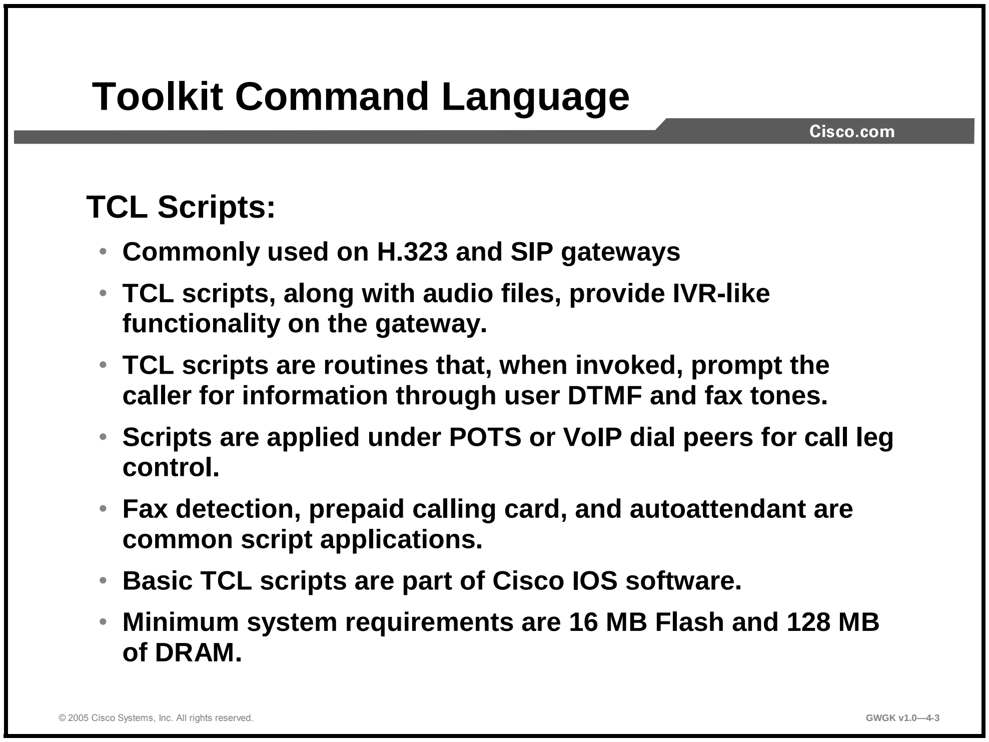
Objectives

Upon completing this lesson, you will be able to configure TCL scripts on a gateway. This ability includes being able to meet these objectives:

- Describe the function of TCL and how a TCL script is used in a gateway
- Describe common applications of TCL scripts
- Configure a TCL script and implement it on a gateway
- Verify TCL scripts for proper operation

Toolkit Command Language

This topic gives an overview of TCL.



Toolkit Command Language

TCL Scripts:

- **Commonly used on H.323 and SIP gateways**
- **TCL scripts, along with audio files, provide IVR-like functionality on the gateway.**
- **TCL scripts are routines that, when invoked, prompt the caller for information through user DTMF and fax tones.**
- **Scripts are applied under POTS or VoIP dial peers for call leg control.**
- **Fax detection, prepaid calling card, and autoattendant are common script applications.**
- **Basic TCL scripts are part of Cisco IOS software.**
- **Minimum system requirements are 16 MB Flash and 128 MB of DRAM.**

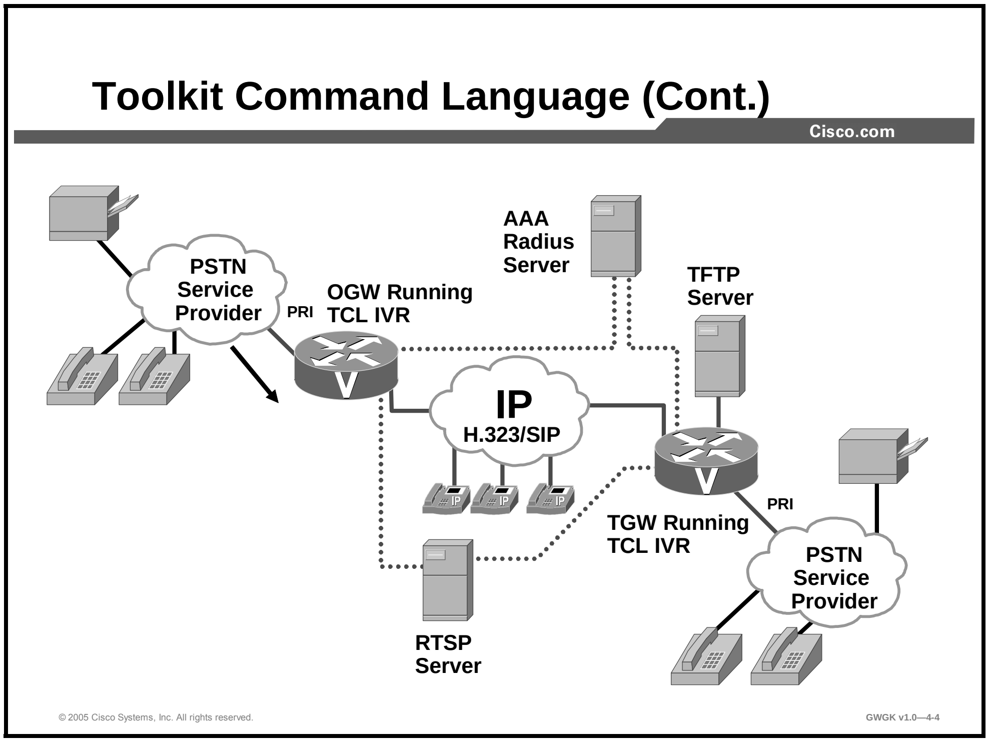
GWGK v1.0—4-3

TCL scripts along with applicable audio files turn a Cisco H.323 or session initiation protocol (SIP) gateway into IVR server. TCL scripts are small routines that when configured play out a certain functions. The main function is to interact with a caller. The caller could an actual person or a fax machine.

TCL scripts run a routine that launch audio prompts for callers to interact with. These small routines carry out a specific set of instructions, which include the playing out of audio prompts. These audio prompts queue the caller to enter a variety of information such as account numbers, passwords, calling card information and more in the form of dual tone multifrequency (DTMF) tones. The TCL scripts take the user entered information and carry out the rest of the instructions. For example, a caller calls into a remote office and is greeted by an Auto Attendant. The Auto Attendant TCL script is launch from the plain old telephone service (POTS) dial peer upon receiving the incoming call. The script launches a series of audio files, but only after the user enters digits as per instructed. The caller hears a prompt “Welcome to company ABC. If you know your party’s extension number please enter it now. Otherwise, stay on the line and a company operator will be with you shortly.” The caller heard these prompts because the script instructed the audio prompts to play. The caller then enters an extension number, which is matched to a destination pattern outgoing VoIP dial peer. Once the caller is passed to its destination, the script then closes. There are cases where the scripts can stay open, but in this case, the scripts close.

One key thing to remember, TCL scripts launch audio files and it is through these .au files the users are prompted to enter information and interact with the scripts. Scripts can be programmed to function with Radius servers for authorization and authentication. Billing systems are another application these scripts can be part of. Fax scripts act a little different, however. This lesson will discuss fax detection scripts in more detain later in this lesson as well as debit card TCL scripts.

TCL scripts and audio files are loaded into flash or onto a device to which the router has immediate access.



Toolkit Command Language (Cont.)

GWGK v1.0—4-4

TCL IVR version 2.0 is the fourth release of IVR and TCL scripting on Cisco IOS VoIP gateways. The Cisco IVR feature (first made available in Cisco IOS Release 12.0(3)T and 12.0(7)T) provides IVR capabilities using TCL scripts.

IVR is a term that is used to describe systems that provide information in the form of recorded messages over telephone lines in response to user input in the form of spoken words, or more commonly DTMF signaling. For example, when a user makes a call with a debit card, an IVR application is used to prompt the caller to enter a specific type of information, such as a PIN. After playing the voice prompt, the IVR application collects the predetermined number of touch tones (digit collection), forwards the collected digits to a server for storage and retrieval, and then places the call to the destination phone or system. Call records can be kept and a variety of accounting functions performed.

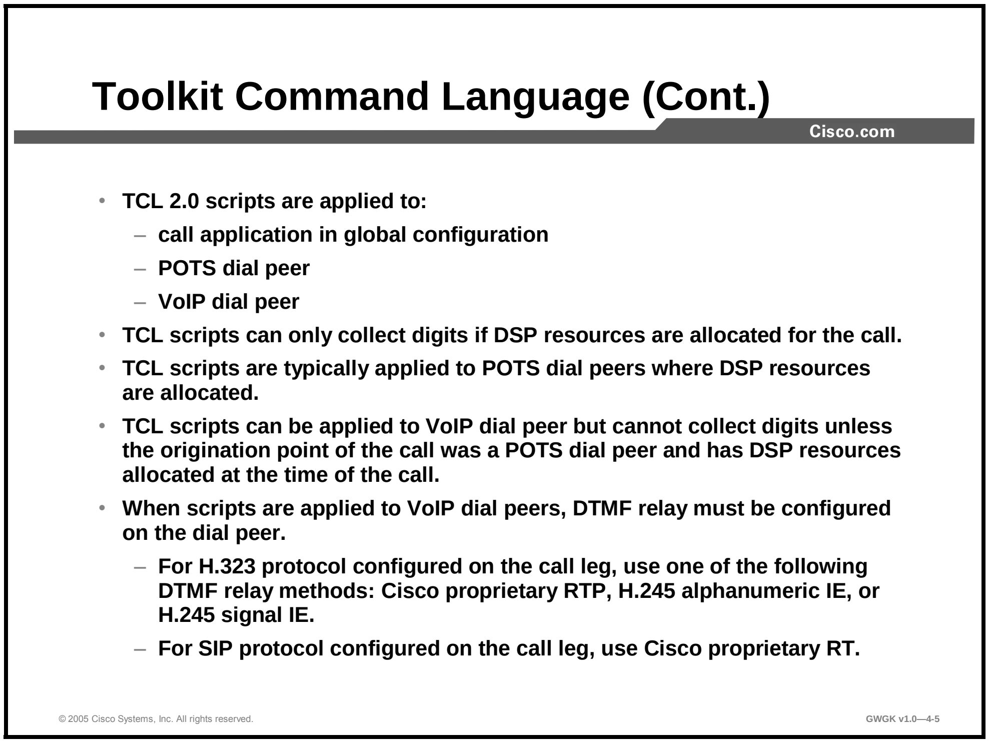
The IVR application (or script) is a voice application designed to handle calls on a voice gateway, which is a router that is equipped with VoIP features and capabilities. The IVR feature allows an IVR script to be used during call processing. The scripts interact with the IVR software to perform the various functions. Typically, IVR scripts contain both executable files and audio files that interact with the system software.

New to TCL IVR version 2.0 is the optional use of Real Time Streaming Protocol (RTSP), which is an application-level protocol used for control over the delivery of data with real-time properties. RTSP provides an extensive framework to enable control, and perform on-demand delivery of real-time data. For example, RTSP is used to control the delivery of audio streams from an audio server.

By implementing an RTSP client on VoIP gateways, an application running on the gateway is able to connect calls with audio streams from an external audio server and also has the following features:

- Reduces the CPU load
- Allows larger prompts to be played
- Allows use of an external audio server

This external audio server removes the limitation on the number of prompts that can be played out and the size of the prompt.



Toolkit Command Language (Cont.)

Cisco.com

- TCL 2.0 scripts are applied to:
  - call application in global configuration
  - POTS dial peer
  - VoIP dial peer
- TCL scripts can only collect digits if DSP resources are allocated for the call.
- TCL scripts are typically applied to POTS dial peers where DSP resources are allocated.
- TCL scripts can be applied to VoIP dial peer but cannot collect digits unless the origination point of the call was a POTS dial peer and has DSP resources allocated at the time of the call.
- When scripts are applied to VoIP dial peers, DTMF relay must be configured on the dial peer.
  - For H.323 protocol configured on the call leg, use one of the following DTMF relay methods: Cisco proprietary RTP, H.245 alphanumeric IE, or H.245 signal IE.
  - For SIP protocol configured on the call leg, use Cisco proprietary RT.

GWGK v1.0—4-5

IVR version 2.0 scripts can be configured for incoming POTS or VoIP call legs to play announcements to the user or collect user input (digits). With IVR version 2.0 the prompts can be triggered from both the public switched telephone network (PSTN) side of the call leg and the IP side of the call leg. This enables the audio files (or prompts) to be played out over the IP network.

IVR scripts played toward a VoIP call leg are subject to the following conditions:

- G.711mu-law encoding must be used when playing prompts.
- G.711mu-law encoding must also be used for the duration of these calls, even after prompt play out has completed.
- There is no DSP on the IP leg, so the script cannot initiate a tone.

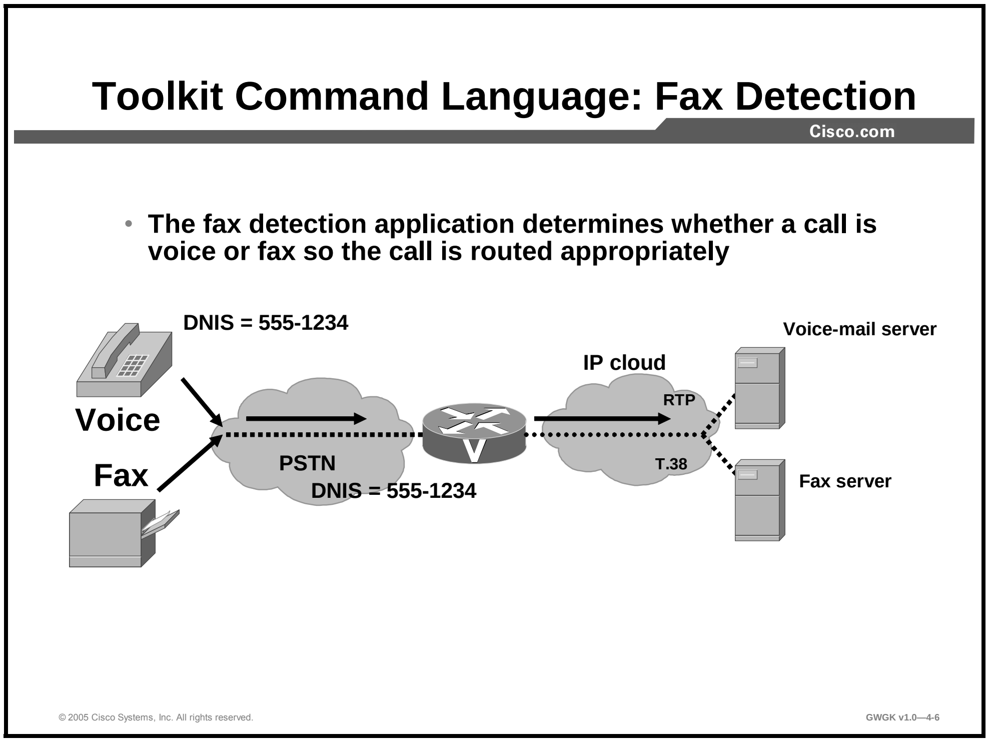
When you are using an IVR script to collect digits on a VoIP call leg, you must use DTMF relay. H.323 protocol configured on the call leg, use DTMF relay method. The following DTMF relay methods are supported:

- **cisco-rtp:** Cisco proprietary Real-Time Transport Protocol (RTP)
- **h245-alphanumeric:** DTMF relay via H.245 alphanumeric information element (IE)
- **h245-signal:** DTMF relay via H.245 signal IE
- **SIP protocol configured on the call leg, use cisco-rtp:** Cisco Proprietary RTP

Caveats

TCL IVR version 1.0 verbs and TCL IVR 2.0 verbs cannot be mixed in a script. You either write a script using version 1.0 verbs in application program interface (API) or using version 2.0 verbs in API.

- H.245-alphanumeric DTMF relay does not accurately report the duration of a key press, for example, holding down the pound (#) key for longer than 1 second to register the “long pound” feature. Doing so only reports a duration of 200 ms. Therefore, if an IVR script is configured on the terminating gateway, Cisco RTP or H.245-signal DTMF relay must be used.
- RTSP multicast sessions are not supported by the Cisco IOS RTSP client.
- DMTF relay (Cisco RTP, H.245-signal or H.245-alphanumeric) must be configured and negotiated on the VoIP call leg to collect digits over a VoIP call leg.
- RTSP is not recommended for dynamic prompt playouts.



Toolkit Command Language: Fax Detection

Cisco.com

- **The fax detection application determines whether a call is voice or fax so the call is routed appropriately**

© 2005 Cisco Systems, Inc. All rights reserved.

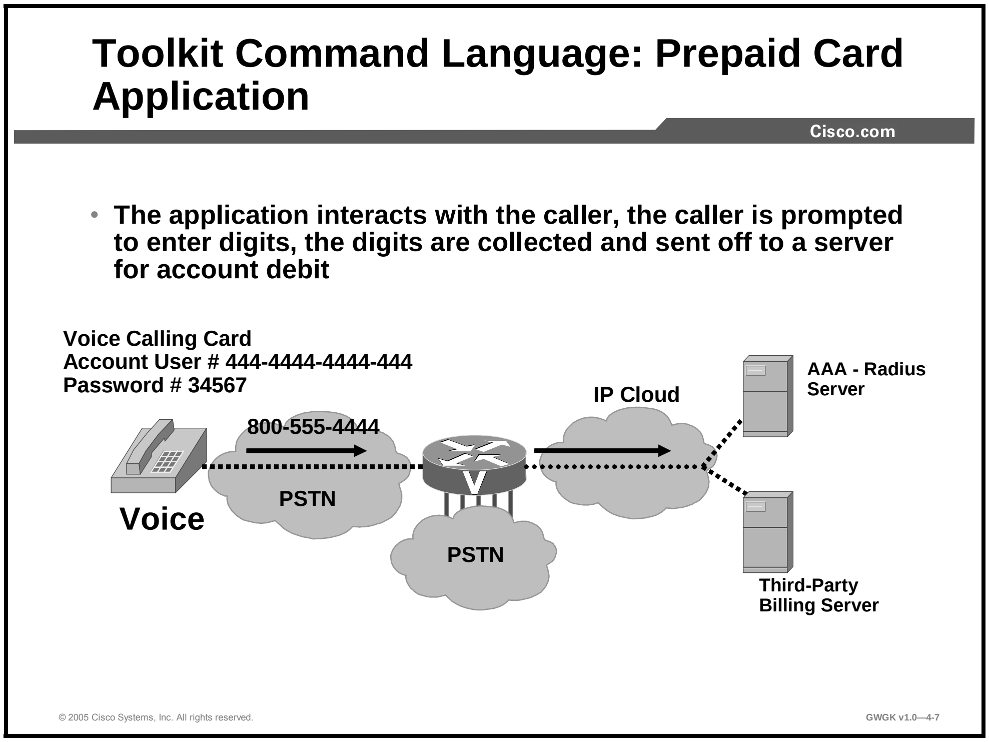
GWGK v1.0—4-6

The fax detection application determines whether a call is voice or fax so that the call is routed appropriately. It is one of the Cisco IVR applications that customers can configure on VoIP gateways to present an interactive interface to callers. IVR applications collect digits, provide authentication, and provide call control when voice interface cards (VICs) or voice WAN interface cards (VWICs) are used.

The fax detection application has several configurable parameters that allow you to create customized versions of the application for different types of calls. For example, you can configure the application to understand a certain manually dialed digit to indicate a voice or fax call. The dialed digit produces tones known as DTMF, which are recognized by the application.

When the fax detection application is configured on the gateway, callers dial the same E.164 number for both voice and fax calls. The gateway automatically detects that a call is a fax transmission by listening for comfort noise generation (CNG), the distinctive fax “calling” tone; in most cases, calls without CNG are assumed to be voice calls. The detection of CNG requires 9 seconds (two CNG cycles) after a call has been established, during which time the application can play an audio prompt to the caller. CNG detection continues for the entire duration of the call, so it is possible that a caller could first be connected on a voice call, then start to transmit a fax, and the application would automatically switch the call to the fax application. Most newer fax machines generate CNG; however, there are some that do not. Fax detection can be configured to handle non-CNG fax calls as well.

After the application decides whether the call is voice or fax, the call is routed based on the type of call and the dialed number. The gateway uses configuration constructs called dial peers to perform the routing. At its most basic level, the fax detection application makes use of two outgoing dial peers: One for voice and one for fax. If store-and-forward fax is used for the fax calls, the outgoing fax dial peer is also configured with an IVR application that processes the call.



Toolkit Command Language: Prepaid Card Application

Cisco.com

- **The application interacts with the caller, the caller is prompted to enter digits, the digits are collected and sent off to a server for account debit**

GWGK v1.0—4-7

The debit card application works in conjunction with the Cisco IVR software, authentication, authorization, and accounting (AAA), RADIUS, and an integrated third-party billing system. The IVR software infrastructure allows prerecorded audio files to be combined dynamically to play the dollar amount of credit remaining on a customer debit card, the time and date, and other information.

The integrated third-party billing system maintains per-user credit balance information. The AAA and RADIUS vendor-specific attributes (VSAs) communicate per-user credit balance information using the billing system. The billing system and Cisco IOS software enable a carrier to authorize voice calls and debit individual user accounts in real time at the edges of a VoIP network without requiring external service nodes.

The debit Card TCL Application is rather a comprehensive application. Here is an example of a debit card call flow:

1. A customer calls the access number of the ITSP The application begins with a welcome message

2. The customer is prompted to select a preferred language

3. The customer is prompted for an account number.

4. The prompt returns the amount of credit available on the customer account.

5. The next prompt asks for a destination number.

6. A second authorization phase then occurs, authorizing a call to the number entered.

7. If the customer is authorized, the prompt returns the amount of time left in the customer account for a call to that destination.

8. The call is completed when a caller hangs up.

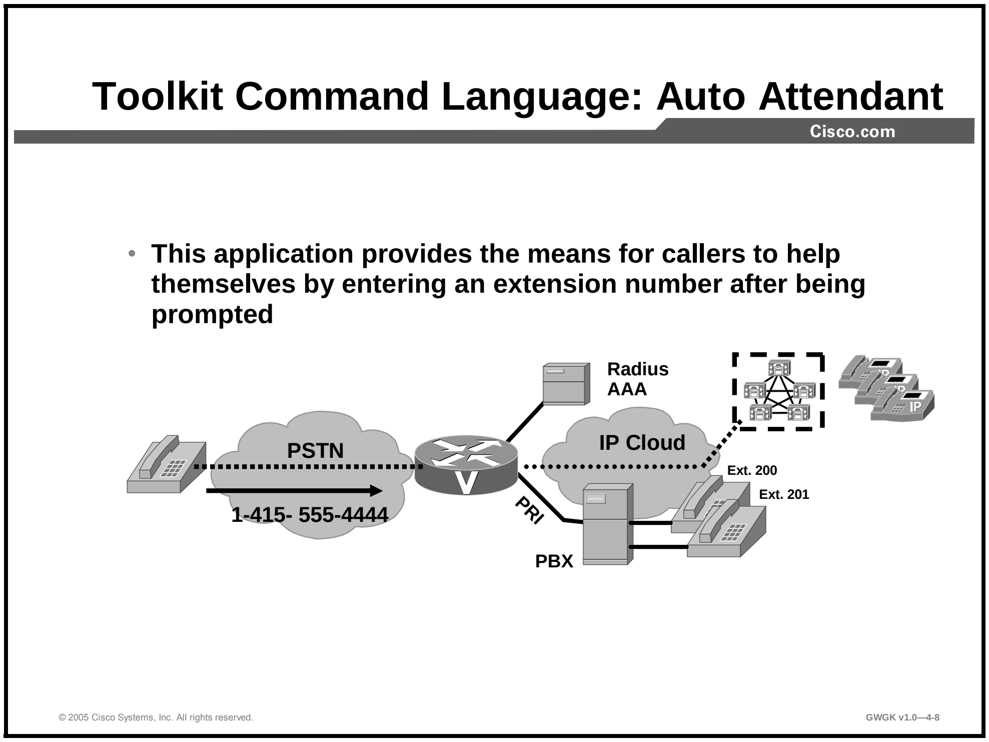
9. If instead the caller presses and holds the pound (#) button on the telephone keypad for more than 2 seconds, the authorization process begins again at the second authorization phase.

10. The prompt returns a new credit amount to the caller, and the call to the new destination begins.

11. If the customer does not disconnect, repeated calls can be made without having to repeat first-phase authentication.

12. If at any time during a call, the credit amount left in the customer account reaches the preconfigured warning amount (typically, 1 minute of service left), a warning prompt is played.

13. If a caller continues to talk until all the time is consumed, a disconnect message is played.



Toolkit Command Language: Auto Attendant

Cisco.com

- **This application provides the means for callers to help themselves by entering an extension number after being prompted**

GWGK v1.0—4-8

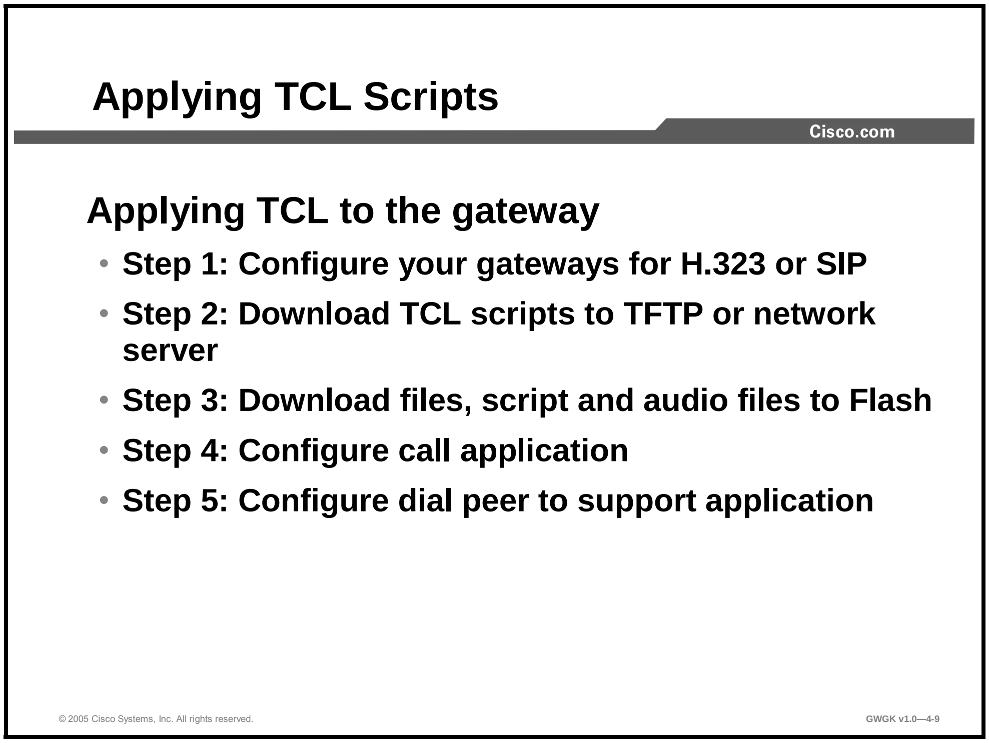
At the remote field office, you do not need a live person to answer and transfer calls to extensions, use the gateway and Auto Attendant scripts to do the job.

The common application for Auto Attendant is deployed mostly commonly in the remote offices. Central sites usually have a Cisco CallManager with a four-port Auto Attendant. With TCL Auto Attendant, each remote site can have an Auto Attendant functionality not needing to rely on the central site Auto Attendant functionality and keeping unnecessary voice traffic off the IP WAN.

In the TCL Auto Attendant application, callers are prompted to simply enter a destination number. The caller can be authenticated if required or not.

Applying TCL Scripts

This topic describes how to apply TCL scripts to a gateway.



Applying TCL Scripts

Cisco.com

Applying TCL to the gateway

- Step 1: Configure your gateways for H.323 or SIP
- Step 2: Download TCL scripts to TFTP or network server
- Step 3: Download files, script and audio files to Flash
- Step 4: Configure call application
- Step 5: Configure dial peer to support application

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—4-9

Before you configure your Cisco gateway to support TCL IVR, you must perform the following prerequisite tasks:

Step 1 Configure the gateway to support H.323 or SIP.

Step 2 Download appropriate TCL Script from TCLWare from http://www.cisco.com/cgi-bin/tablebuild.pl/tclware to a location on the network.

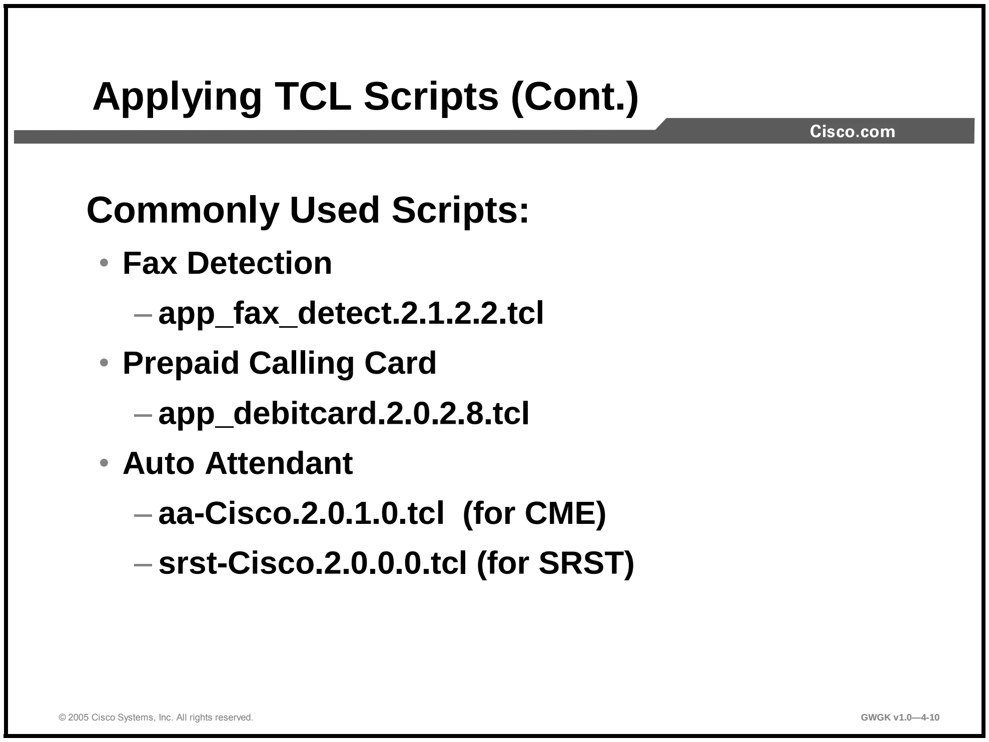
Step 3 Download the TCL script to an accessible server or download the script to flash, and download the supporting audio files.

Step 4 Configure the **call application voice statements** on the gateway.

Step 5 Configure the call application name defined under the appropriate dial peers.

Note If a TFTP server is used configure a TFTP sever to perform storage and retrieval of the audio files, which are required by the Debit Card gateway or other features requiring TCL IVR scripts and audio files.

Make sure that your access platform has a minimum of 16 MB flash and 128 MB of DRAM memory.



Applying TCL Scripts (Cont.)

Cisco.com

Commonly Used Scripts:

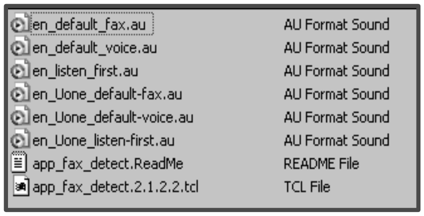
- **Fax Detection**
  - **app_fax_detect.2.1.2.2.tcl**
- **Prepaid Calling Card**
  - **app_debitcard.2.0.2.8.tcl**
- **Auto Attendant**
  - **aa-Cisco.2.0.1.0.tcl (for CME)**
  - **srst-Cisco.2.0.0.0.tcl (for SRST)**

GWGK v1.0—4-10

This figure shows three common TCL scripts, each presented in more detail in the following figures. The versions of these scripts can change as the scripts are updated and posted under TCLware on Cisco.com. The Auto Attendant scripts as well as the audio files are not on TCLware but under the Cisco CallManager Express and SRST software downloads links off Cisco.com. You will need to download the individual scripts for Auto Attendant.

Applying TCL Scripts: Fax Detect Application

Cisco.com



en_default_fax.au	AU Format Sound
en_default_voice.au	AU Format Sound
en_listen_first.au	AU Format Sound
en_Uone_default-fax.au	AU Format Sound
en_Uone_default-voice.au	AU Format Sound
en_Uone_listen-first.au	AU Format Sound
app_fax_detect.ReadMe	README File
app_fax_detect.2.1.2.2.tcl	TCL File

- **Zip file contains audio and TCL required for basic fax detect solution.**
- **Audio files are called up by the TCL scripts.**
- **Always take time read through the ReadMe file. This file is has configuration information and states any bug caveats.**

Customers who install VoIP networks often need a mechanism at the gateway to present an interactive interface to callers, to collect digits or provide authentication. The Cisco IVR feature allows the creation of applications for customized caller interfaces and for call control when voice feature cards (VFCs) are used. Fax detection is an IVR application.

The fax detection application determines whether a call is voice or fax so the call is routed appropriately. The application has several configurable parameters that allow you to create customized versions of the application for different types of calls. For example, you can configure the application to recognize a certain manually dialed digit (DTMF) to indicate a voice or fax call.

When the fax detection application is configured on the gateway, callers dial the same E.164 number for both voice and fax calls. The gateway automatically detects that a call is a fax transmission by listening for CNG, the distinctive fax “calling” tone. In most cases, calls without CNG are assumed to be voice calls. The detection of CNG requires 9 seconds (two CNG cycles) after a call has been established, during which time the application can play an audio prompt to the caller. CNG detection continues for the duration of the call, so it is possible that a caller first could be connected to a voice-mail server, leave a voice message, and start to transmit a fax, then the application would automatically switch the call to the fax application. Most newer fax machines generate CNG; however, there are some that do not. You can configure fax detection to handle these fax calls that do not generate CNG.

After the application decides whether the call is voice or fax, it routes the call based on the type of call and the dialed number. The gateway uses the configuration constructs, called dial peers, to perform the routing. At its most basic level, the fax detection application makes use of two outgoing dial peers: One for voice, and one for fax. If store-and-forward fax is used for the fax calls, the outgoing fax dial peer is also configured with an IVR application that processes the call. However, at a more complex level, by configuring more dial peers on the router, you can have different voice or fax handling for different dialed numbers, or you can have different modes of the fax detection application configured for different dialed number patterns. For example, calls to 818-555-7xxx could be automatically routed to the fax application upon the detection of CNG tones, while callers who dial 818-555-8xxx would have to press a certain digit to route a call to the fax application.

Four modes of operation are available to customize the fax detection application:

- Connect-first mode
  - (Default) When you configure connect-first mode on the gateway, incoming calls are connected immediately to the voice-mail server, which plays a greeting or audio prompt based upon the number called. Because this greeting is generated by the voice-mail application and not by the gateway, each E.164 number can have its own custom prompt.
  - The gateway listens for distinctive CNG, or fax, tones during the prompt and for the remainder of the call. If the gateway hears CNG at any time, then the voice-mail application is disconnected and the call is passed on to the fax relay or store-and-forward fax application, depending on which was configured on the gateway. Note that non-CNG faxes are not supported in this mode.
  - If any dialed digits, or DTMF tones, are detected during the call, they are relayed to the voice-mail server using the DTMF signaling protocol configured on the dial peer. The gateway does not listen for DTMF and does not interpret DTMF.
  - The connect-first mode is useful when you expect that most incoming calls will be voice. This mode adds load to the voice-mail application, which is now required to answer fax calls also. This mode is the default if no mode is configured.
- Listen-first mode
  - When listen-first mode is configured on the gateway and an incoming call is received, the gateway can play a configurable audio prompt to greet the caller or provide instructions.
  - If an audio file for this prompt has not been specified during configuration, the caller will hear 9 seconds of silence. Cisco recommends configuring a prompt.
  - The gateway listens for CNG for 9 seconds before passing the call to an application or server. If CNG is detected, the call is passed to the fax relay or store-and-forward fax application, whichever is configured on the gateway. If CNG is not heard during the first 9 seconds, the call is passed to the voice-mail server.
  - Non-CNG faxes are not supported in this mode.
  - If any DTMF tones are detected, the call is connected to the voice server. Once a call is connected to the voice server, DTMF tones are relayed using the DTMF signaling protocol that has been configured on the dial peer.
  - In listen-first mode, CNG fax calls are never automatically connected to the voice-mail server, and so this mode is useful when CNG fax calls constitute a significant proportion of the calls to this E.164 number.
- Default-voice mode
  - When default-voice mode is configured on the gateway and an incoming call is received, the gateway can play a configurable audio prompt to greet the caller or provide instructions.
  - If the audio file for this prompt has not been specified during configuration, the caller will hear 9 seconds of silence. Cisco recommends configuring a prompt.
  - In default-voice mode, you can specify during configuration a DTMF digit for incoming callers to press to select the voice-mail server and another digit they can press to select the fax application. When the gateway detects either of these configured DTMF digits, the call is connected as requested.

  - The gateway listens for CNG for 9 seconds before passing the call to an application. If CNG is detected, the call is passed to the fax relay or store-and-forward fax application, whichever is configured on the gateway.
  - If CNG is not heard during the first 9 seconds, the call is passed to the voice-mail server.
  - If any DTMF tones are detected, the gateway interprets the DTMF. If the tones match the DTMF digit configured for voice, the call is passed to the voice-mail server. If the tones match the DTMF digit configured for fax, the call is passed to the fax application. If the tones do not match either the voice or fax digit, the prompt is replayed. Once a call has been connected to the voice server, subsequent DTMF tones are relayed using the DTMF signaling protocol that has been configured on the dial peer.
  - Non-CNG-compliant faxes are supported in the default-voice mode when the caller manually selects the fax application by pressing the keypad key designated for fax.

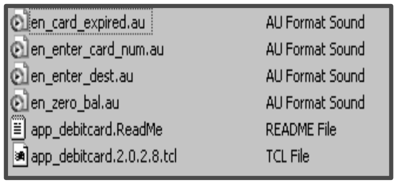
- Default-fax mode
  - When default-fax mode is configured on the gateway and an incoming call is received, the gateway can play a configurable audio prompt to greet the caller, provide instructions, or both.
  - If the audio file for this prompt has not been specified during configuration, the caller will hear 9 seconds of silence. Cisco recommends configuring a prompt.
  - In default-fax mode, you can specify during configuration a DTMF digit that incoming callers can press to select the voice-mail server and another digit they can press to select the fax application. When the gateway detects either of these configured DTMF digits, the call will be immediately connected as requested.
  - The gateway listens for CNG for 9 seconds before passing the call to an application. If CNG is detected, the call is passed to the fax relay or store and forward fax application, whichever is configured on the gateway.
  - If CNG is not heard during the first 9 seconds, the call is passed to the fax relay or store-and-forward fax application.
  - If any DTMF tones are detected, the gateway interprets the DTMF. If the tones match the DTMF digit configured for voice, the call is passed to the voice-mail server. If the tones match the DTMF digit configured for fax, the call is passed to the fax application. If the tones do not match either the voice or fax digit, the prompt is replayed. After a call has been connected to the voice server, subsequent DTMF tones are relayed using the DTMF signaling protocol that has been configured on the dial peer.
  - The default-fax mode is useful when fax calls constitute a significant proportion of the calls. In addition, this mode supports non-CNG compliant faxes without requiring the manual activation of a DTMF tone.

The following is a fax detection configuration example. Note that there are many more variables that can be added to this application than those that are seen here.

```
call application voice fax_detect tftpboot://10.1.1.1/
fax_detect_2.1.2. 0.tcl
call application voice fax_detect mode listen-first

dial-peer voice 1 pots
 application fax_detect
 incoming called-number 9T
 direct-inward-dial
 port 0/1/0:23

dial-peer voice 2 voip
 destination-pattern 75..
 session target ipv4:192.168.44.21
 dtmf-relay h245-signal
 fax rate disable
```

Applying TCL Scripts: Prepaid Card Application

Cisco.com



en_card_expired.au	AU Format Sound
en_enter_card_num.au	AU Format Sound
en_enter_dest.au	AU Format Sound
en_zero_bal.au	AU Format Sound
app_debitcard.ReadMe	README File
app_debitcard.2.0.2.8.tcl	TCL File

- **This is a sample of the files that are contained in the zip file.**
- **Zip file contains audio and the TCL scripts required for basic prepaid card solution.**
- **Audio files are called up by the TCL scripts.**
- **Always read through the ReadMe file. This file has configuration information and states bug caveats.**

The debit card application allows a user to select the language mode based on the languages that are configured through Cisco IOS software. The application then prompts and collects the card number. The card number consists of a user ID and PIN, both configured through the IOS software. Authentication is done with the card number. If the card number passes authentication, the application plays the amount available on debit card to the user. It then prompts and collects the destination number.

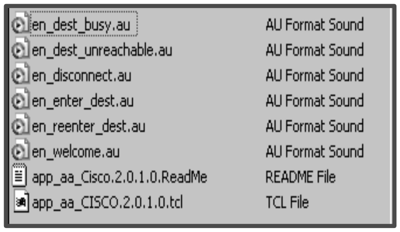
If authentication fails, the application allows user to retry the call, and the number of retries is configured through the OS software. Authorization is done with the destination number. If authorization is successful, the application plays the amount of talk time available in the debit card account and places the call. If authorization fails, the application allows users to retry the call.

The following is a debit card application configuration example:

```
call application voice debitcard
tftp://bboc/scripts/app_debitcard.2.0.0.tcl

call application voice debitcard uid-len 6

call application voice debitcard language 1 en

call application voice debitcard language 2 sp

call application voice debitcard set-location en 0
tftp://bboc/prompts/en/

call application voice debitcard set-location sp 0
tftp://bboc/prompts/sp/

call application voice conrad tftp://bboc/scripts/conrad_1.tcl

call application voice no_answer
tftp://bboc/scripts/no_answer.2.0.0.tcl


dial-peer voice 300 pots

 application debitcard

 destination-pattern 300..

 port 0/1/0:23

 prefix 300
```

Applying TCL Scripts: AA Application

Cisco.com



en_dest_busy.au	AU Format Sound
en_dest_unreachable.au	AU Format Sound
en_disconnect.au	AU Format Sound
en_enter_dest.au	AU Format Sound
en_reenter_dest.au	AU Format Sound
en_welcome.au	AU Format Sound
app_aa_Cisco.2.0.1.0.ReadMe	README File
app_aa_CISCO.2.0.1.0.tcl	TCL File

- **Zip file contains the audio and TCL scripts required for basic AA solution.**
- **Audio files are called up by the TCL scripts.**
- **Always read the ReadMe file. This has deployment information and any bug caveats.**

GWGK v1.0—4-13

During call setup, play the welcome prompt en_welcome.au and ask the user to enter the destination number by playing en_enter_dest.au prompt. If the user does not dial any number or dials 0 connect to the operator. If the user dials an invalid destination number, ask the user to reenter the destination number by playing the en_reenter_dest.au prompt. This can be done up to three times, and, after the busy prompt en_dest_busy.tcl is played, the call will be disconnected. If the user dials a valid destination number, the call is connected. When the parties hang up, the calls legs will be disconnected. If the user dials a valid destination number and if the destination is busy or unreachable, the user will be prompted to reenter the same destination number or to try a different destination number. This script was downloaded from the Cisco CallManager Express software download site. There are currently no Auto Attendant zip files under TCLware.

The following is a Cisco CallManager Express configuration example:

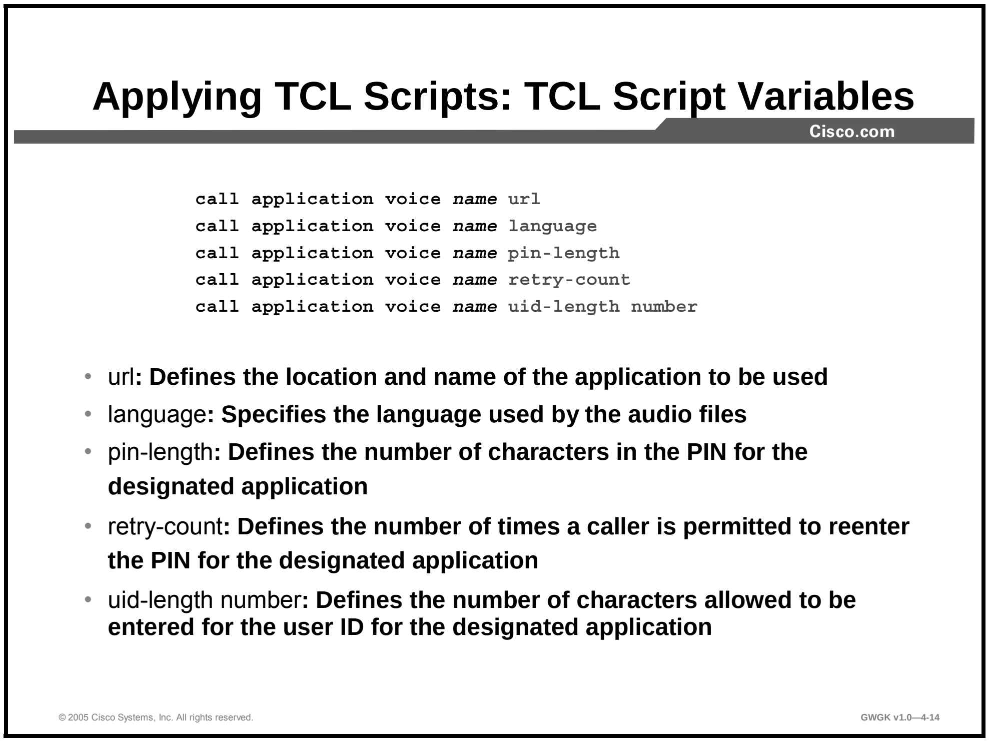
```
call application voice autoatt tftp://tftpserv/scripts/app_aa-CISCO.2.0.0.tcl

call application voice autoatt language 1 en

call application voice autoatt language 2 sp

call application voice autoatt set-location en 0 tftp://bboc/prompts/en/

call application voice autoatt set-location sp 0 tftp://bboc/prompts/sp/

!

dial-peer voice 9 pots

 application autoatt

 destination-pattern 9T

 port 0/1/0 :23
```

The following is a Cisco SRST configuration example:

```
call application voice srst-aa flash:// srst_Cisco.2.0.0.0.tcl
call application voice srst-aa language 1 en
call application voice srst-aa cm-pilot 1400
call application voice srst-aa aa-pilot 1010
call application voice srst-aa operator 1001 (an ephone-dn)
call application voice srst-aa set-location en 0 flash://
```

If PSTN callers are to hear the SRST Auto Attendant, you need to set up POTS dial peers with an incoming called-number **aa-pilot** number. When callers hit the POTS dial peer, the script will launch. For ephone access to the Auto Attendant, VoIP dial peers with destination patterns of, the **aa-pilot** numbers are required. The following example shows a sample **aa-pilot** number configuration:

```
dial-peer voice 5000 pots
    application srst-aa
 incoming called-number 1400
 preference 1
    port 0/1/0:23
    forward-digits all

dial-peer voice 3000 voip
    application srst-aa
 destination-pattern 1010
```



Applying TCL Scripts: TCL Script Variables

```
call application voice name url
call application voice name language
call application voice name pin-length
call application voice name retry-count
call application voice name uid-length number
```

- url**: Defines the location and name of the application to be used**
- language**: Specifies the language used by the audio files**
- pin-length**: Defines the number of characters in the PIN for the designated application**
- retry-count**: Defines the number of times a caller is permitted to reenter the PIN for the designated application**
- uid-length number**: Defines the number of characters allowed to be entered for the user ID for the designated application**

GWGK v1.0—4-14

You must configure the application that interacts with the dial peer before you configure the dial peer. The dial peer collects digits from the caller and uses the application you have created. Use the **call application voice** command as shown in the “Dial-Peer Call Application Configuration Procedure” table. Each command line is optional depending on the type of action desired or the digits to be collected.

To configure the application, enter these commands in global configuration mode. You might not use all of these commands for your TCL script installation.

Dial-Peer Call Application Configuration Procedure

Step	Command	Purpose
1.	`Router(config)# call application voice` ***`name url`***	Defines the name of the application to be used with your TCL IVR script. The *url* argument specifies the location of the file and the access protocol. An example is as follows: ■ flash:scripts/session.tcl ■ tftp://dirt/sarvi/scripts/session.tcl ■ ftp://sarvi-ultra/scripts/session.tcl ■ slot0:scripts/tcl/session..tcl **Note:** You can only configure *url* if the application named *name* has not been configured.

Step	Command	Purpose
2.	`Router(config)# call application voice name language digit language`	Specifies the language used by the audio files. An example is: call application voice test language 1 en. The arguments are as follows: ■ *digit*: Specifies 0 through 9. ■ *language:* Specifies two characters that represent a language. For example, "en" for English, "sp" for Spanish, and "ch" for Mandarin. Enter **aa** to represent all.
3.	`Router(config)# call application voice name pin-length number`	Defines the number of characters in the PIN for the designated application. Values are from 0 through 10.
4.	`Router(config)# call application voice name retry-count number`	Defines the number of times a caller is permitted to reenter the PIN for the designated application. Values are from 1 through 5.
5.	`Router(config)# call application voice name uid-length number`	Defines the number of characters that are allowed to be entered for the user ID for the designated application. Values are from 1 through 20.
6.	`Router(config)# call application voice name set-location language category location`	Defines the location, language, and category of the audio files for the designated application. An example is "set-location en 1 tftp://server dir/audio filename".

TCL script names and the corresponding parameters that are required for each TCL scripts are shown in the "TCL Scripts Descriptions and Parameters" table.

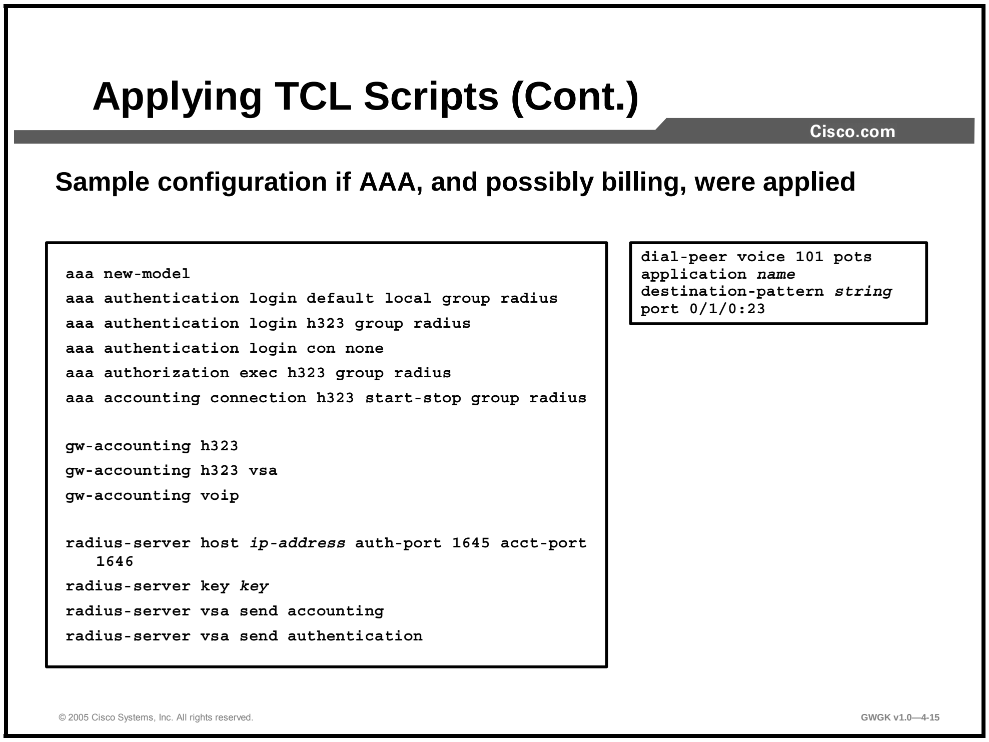
TCL Scripts Descriptions and Parameters

Script Name	Description	Parameters

`clid_4digits_npw_3_cli.tcl`	Authenticates the account number and PIN using automatic number identification (ANI) and null. The allowed length of digits is configurable through the command-line interface (CLI). If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	**call application voice uid-len**
		min = 1, max = 20, default = 10
		call application voice pin-len
		min = 0, max - 10, default = 4
		call application voice retry-count
		min = 1, max = 5, default = 3

`clid_authen_col_npw_cli.tcl`	Authenticates the account number and PIN using ANI and null. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	**call application voice retry-count** min = 1, max = 5, default = 3
`clid_authen_collect_cli.tcl`	Authenticates the account number and PIN using ANI and dialed number identification service (DNIS). If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	**call application voice retry-count** min = 1, max = 5, default = 3

Script Name	Description	Parameters
`clid_col_npw_3_cli.tcl`	Authenticates using ANI and null for account and PIN. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	**call application voice retry-count** min = 1, max = 5, default = 3
`clid_col_npw_npw_cli.tcl`	Authenticates using ANI and null for account and PIN. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected at the same time.	**call application voice retry-count** min = 1, max = 5, default = 3



Applying TCL Scripts (Cont.)

Cisco.com

Sample configuration if AAA, and possibly billing, were applied

```
aaa new-model
aaa authentication login default local group radius
aaa authentication login h323 group radius
aaa authentication login con none
aaa authorization exec h323 group radius
aaa accounting connection h323 start-stop group radius

gw-accounting h323
gw-accounting h323 vsa
gw-accounting voip

radius-server host ip-address auth-port 1645 acct-port
   1646
radius-server key key
radius-server vsa send accounting
radius-server vsa send authentication
```

```
dial-peer voice 101 pots
application name
destination-pattern string
port 0/1/0:23
```

GWGK v1.0—4-15

Configuring gateway accounting and AAA are not always required for POTS dial-peer configuration. Whether or not these features are required is dependent upon the type of application that is being used with TCL IVR. For example, the debit card application requires accounting and the authentication caller ID application does not.

To configure the inbound POTS dial peer, use the commands in the “Inbound POTS Dial-Peer Configuration Procedure” table, beginning in global configuration mode:

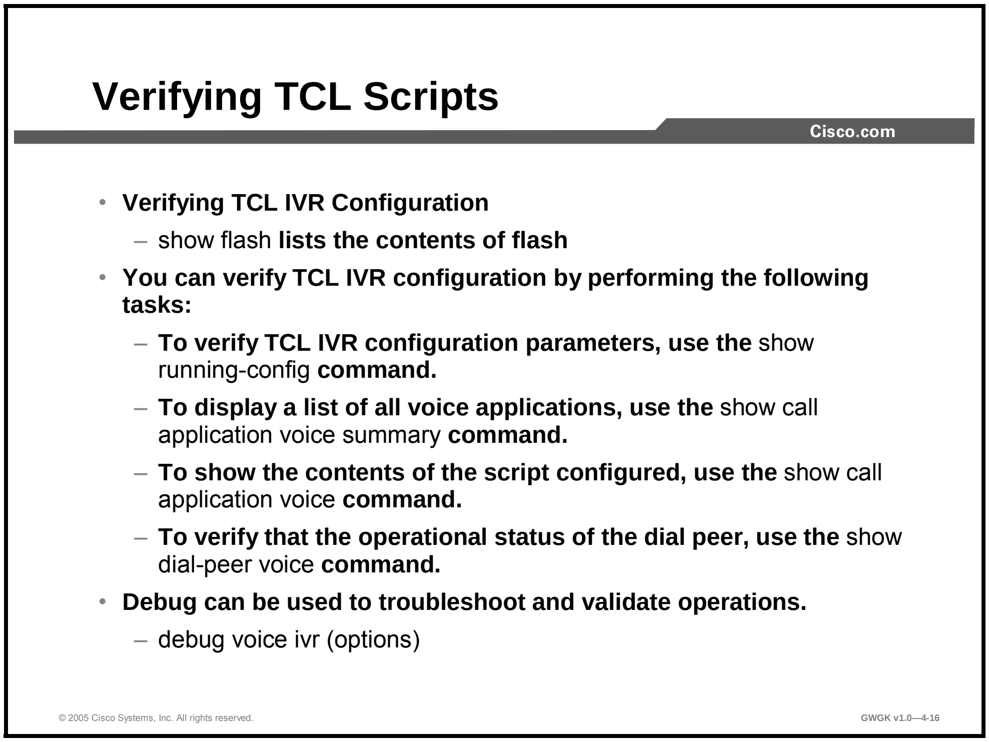
Inbound POTS Dial-Peer Configuration Procedure

Step	Command	Purpose
1.	`Router(config)#` **`aaa new-model`**	(Optional) Enables AAA security and accounting services.
2.	`Router(config)#` **`gw-accounting h323`**	(Optional) Enables gateway-specific H.323 accounting.
3.	`Router(config)#` **`aaa authentication login h323 radius`**	(Optional) Defines a method list called H.323 where RADIUS is defined as the only method of login authentication.
4.	`Router(config)#` **`aaa accounting connection h323 start-stop radius`**	(Optional) Defines a method list called H.323 where RADIUS is used to perform connection accounting, providing start-stop records.
5.	`Router(config)#` **`radius-server host`** ***`ip-address`*** **`auth-port`** ***`number`*** **`acct-port`** ***`number`***	Identifies the RADIUS server and the ports that will be used for authentication and accounting services.
6.	`Router(config)#` **`radius-server key`** ***`key`***	Specifies the password used between the gateway and the RADIUS server.

Step	Command	Purpose
7.	`Router(config)# dial-peer voice *number* pots`	Enters dial-peer configuration mode to configure the incoming POTS dial peer. The *number* argument is a tag that uniquely identifies the dial peer.
8.	`Router(dial-peer)# application *name*`	Associates the TCL IVR application with the incoming POTS dial peer. Enter the selected TCL IVR application name.
9.	`Router(config-dial-peer)# destination-pattern *string*`	Enters the telephone number associated with this dial peer. The *pattern* argument is a series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are numbers from zero (0) through nine and letters from A through D. The following special characters can be entered in the string: ■ Plus sign (+): (Optional) Indicates an E.164 standard number. The plus sign (+) is not supported on the Cisco MC3810 multiservice concentrator. ■ *string*: Specifies the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: — Asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads — Comma (,), which inserts a pause between digits — Period (.), which matches any entered digit (used as a wildcard) ■ T: (Optional) Indicates that the destination-pattern value is a variable length dial-string.
10.	`Router(config-dial-peer)# session target`	Specifies the session target IP address.

Verifying TCL Scripts

This topic describes how to verify the TCL scripts that are deployed on your gateways.



Verifying TCL Scripts

Cisco.com

- **Verifying TCL IVR Configuration**
  - show flash **lists the contents of flash**
- **You can verify TCL IVR configuration by performing the following tasks:**
  - **To verify TCL IVR configuration parameters, use the** show running-config **command.**
  - **To display a list of all voice applications, use the** show call application voice summary **command.**
  - **To show the contents of the script configured, use the** show call application voice **command.**
  - **To verify that the operational status of the dial peer, use the** show dial-peer voice **command.**
- **Debug can be used to troubleshoot and validate operations.**
  - debug voice ivr (options)

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—4-16

Use these steps to verify your configuration.

Step 1 Enter the **show call application voice summary** command to verify that the newly created applications are listed. The example output follows:

```
name                 description


DEFAULT              NEW::Basic app to do DID, or supply
dialtone.
fax_hop_on           Script to talk to a fax redialer
clid_authen          Authenticate with (ani, dnis)
clid_authen_collect  Authenticate with (ani, dnis), collect if
that fails
clid_authen_npw      Authenticate with (ani, NULL)
clid_authen_col_npw  Authenticate with (ani, NULL), collect if
that fails
clid_col_npw_3       Authenticate with (ani, NULL), and 3
tries collecting
clid_col_npw_npw     Authenticate with (ani, NULL) and 3 tries
without pw
SESSION              Default system session application
hotwo
tftp://hostname/scripts/nb/nb_handoffTwoLegs.tcl
```

```
hoone
tftp://hostname/scripts/nb/nb_dohandoff.tcl
hodest                tftp://hostname/scripts/nb/nb_handoff.tcl
clid
tftp://hostname/scripts/tcl_ivr/clid_authen_collect.tcl
db102
tftp://hostname/scripts/1.02/debitcard.tcl
*hw                   tftp://171.69.184.xxx/tr_hello.tcl
*hw1                  tftp://san*tr_db
tftp://171.69.184.235/tr_debitcard.answer.tcl


TCL Script Version 2.0 supported.
TCL Script Version 1.1 supported.
```

Note In the output shown, an asterisk (*) in an application indicates that this application was not loaded successfully. Use the **show call application voice** command with the *name* argument to view information for a particular application.

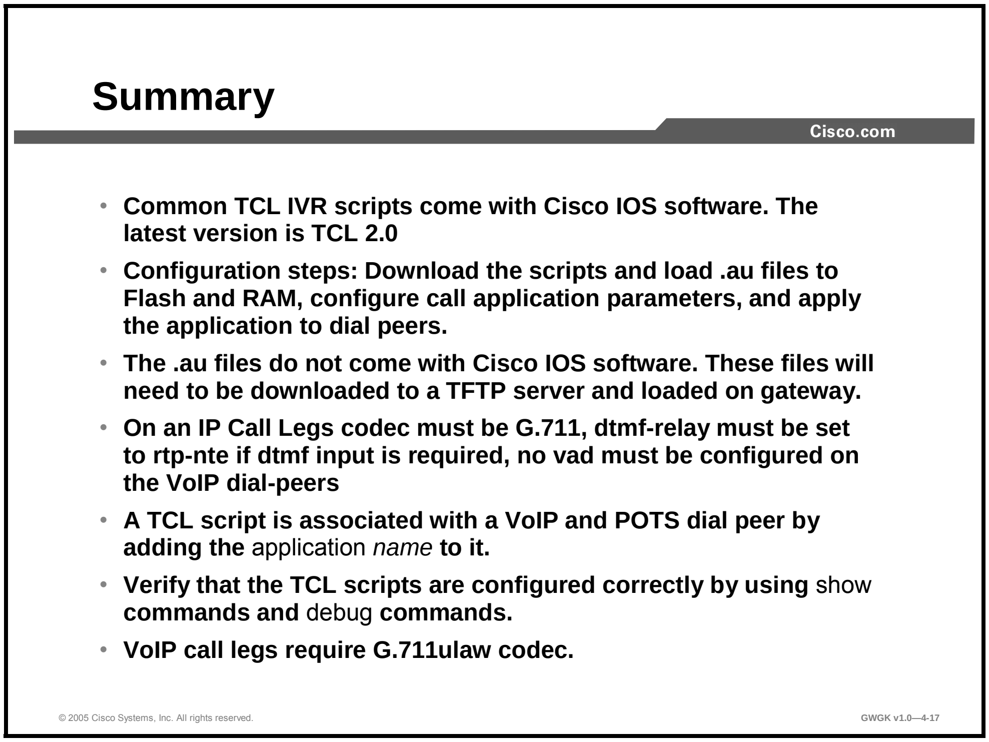
Step 2 Enter the **show dial-peer voice** command with the *peer tag* argument and verify that the application associated with the dial peer is correct, as shown in this example:

```
dial-peer voice 9 pots
 application autoatt
 destination-pattern 9T
 port 0/1/0 :23
```

Step 3 Enter the **show running-config** command to display the entire configuration.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

Cisco.com

- **Common TCL IVR scripts come with Cisco IOS software. The latest version is TCL 2.0**
- **Configuration steps: Download the scripts and load .au files to Flash and RAM, configure call application parameters, and apply the application to dial peers.**
- **The .au files do not come with Cisco IOS software. These files will need to be downloaded to a TFTP server and loaded on gateway.**
- **On an IP Call Legs codec must be G.711, dtmf-relay must be set to rtp-nte if dtmf input is required, no vad must be configured on the VoIP dial-peers**
- **A TCL script is associated with a VoIP and POTS dial peer by adding the** application *name* **to it.**
- **Verify that the TCL scripts are configured correctly by using** show **commands and** debug **commands.**
- **VoIP call legs require G.711ulaw codec.**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—4-17

References

For additional information, refer to these resources:

Cisco IOS TCL IVR 2.0 User Guide

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/tcl_c/index.htm

Configuring TCL IVR Applications

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_c/vvfivr.pdf

Cisco CallManager Express and SRST TCL Scripts

- http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp

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) TCL IVR version 2.0 ____. (Source:)

A) is backward compatible with TCL IVR
B) and TCL IVR 1.0 are not backward compatible
C) app_aa_CISCO.2.0.2.1.tcl script
D) is only supported on 12.3T IOS

Q2) TCL IVR version 2.0 is designed for which environment? (Source:)

A) H323 and SIP
B) Cisco CallManager
C) MGCP only
D) H.323, SIP, and Cisco CallManager

Q3) TCL IVR scripts played toward a VoIP call leg must use? (Source:)

A) G.711ulaw encoding
B) G.728 and G.711ulaw encoding
C) DSP high codec complexity
D) G.711ulaw codec encoding for the entire call VoIP leg

Q4) What are audio files used for in TCL IVR applications? (Source:)

A) Audio files are used as collectors of digits for the .au file.
B) Audio files are used as prompts toward the caller for gathering information.
C) Audio files are not supported with TCL IVR version 1.0.
D) They are launched by the script.

Q5) What are the most common TCL IVR version 2.0 applications? (Source:)

A) Auto Attendant
B) Auto Attendant, fax detection, debit card
C) Debit card, Auto Attendant
D) Fax detection

Q6) After you load .au files into flash, what happens? (Source:)

A) You need to reload the .au files into RAM.
B) TCL scripts call up .au files, so you do not need to load .au files anywhere.
C) The .au files are part of the embedded IOS TCL scripts, so there is no need to load the files.
D) You need to configure call application voice commands.

Q7) How would you apply a script name **debitcard** so it launches when an inbound dial peer is matched? (Source:)

A) use the **application-scripts <name>** command
B) use the **application debitcard in-bound** command
C) use the **application debit card in-bound** command
D) use the **application debitcard** command

Q8) If you wanted to increase the PIN a user needs to enter when authenticating, what is a possible solution? (Source:)

A) Set the retry-count to the length of PIN.
B) Set the pin-length to the desired length.
C) Set the uid-length to the desired length.
D) You are required to set both the uid-length and pin-length.

Q9) What is the command to set the password that is used between the gateway and RADIUS? (Source:)

A) **gw-accounting voip**
B) **aaa authentication login h323 radius**
C) **aaa new-model**
D) **aaa accounting connection h323 start-stop radius**

Q10) Which command defines the name of the application app_aa_CISCO.tcl script to be used with your TCL IVR script? (Source:)

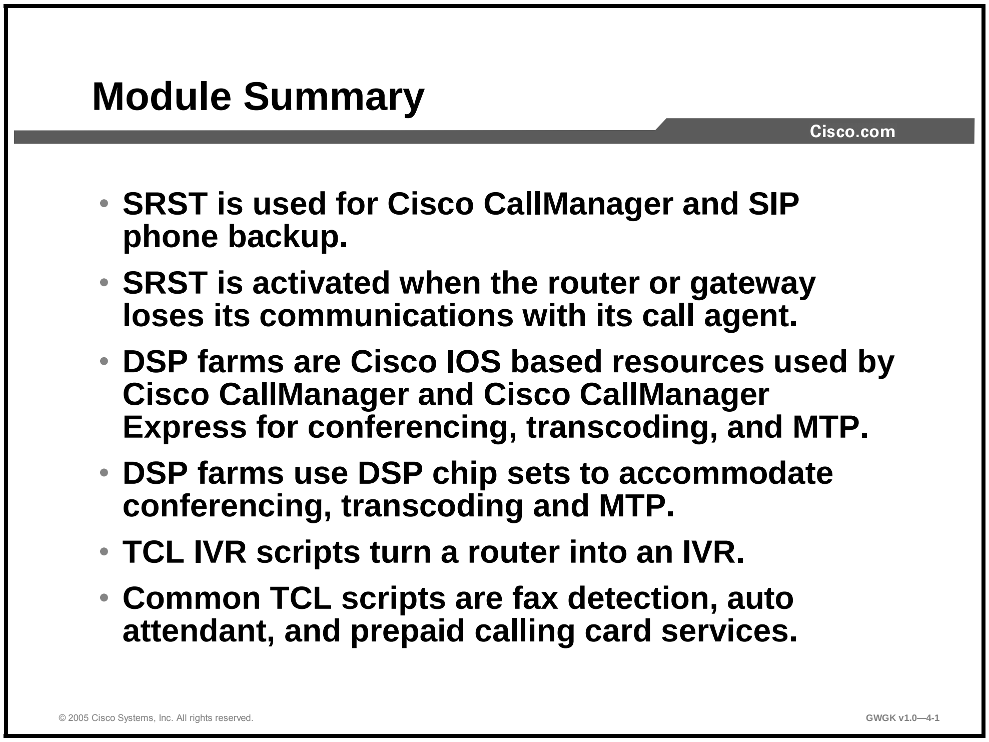
A) **call application voice autoatt app_aa_CISCO.tcl**
B) **call application voice autoatt tftp://scripts/session.tcl**
C) **call application voice autoatt flash:app_aa_CISCO.tcl**
D) **call application voice autoatt tclscripts/app_aa_CISCO.tcl**

Lesson Self-Check Answer Key

Q1)	A
Q2)	A
Q3)	D
Q4)	B
Q5)	B
Q6)	B
Q7)	D
Q8)	B
Q9)	D
Q10)	C

Module Summary

This topic summarizes the key points discussed in this module.



Module Summary

Cisco.com

- SRST is used for Cisco CallManager and SIP phone backup.
- SRST is activated when the router or gateway loses its communications with its call agent.
- DSP farms are Cisco IOS based resources used by Cisco CallManager and Cisco CallManager Express for conferencing, transcoding, and MTP.
- DSP farms use DSP chip sets to accommodate conferencing, transcoding and MTP.
- TCL IVR scripts turn a router into an IVR.
- Common TCL scripts are fax detection, auto attendant, and prepaid calling card services.

GWGK v1.0—4-1

This module discussed configuring Cisco Survivable Remote Site Telephony (SRST), deploying digital signal processor (DSP) farms to employ conferencing, transcoding, and media termination point (MTP), and using Tool Command Language (TCL) to offer interactive voice response (IVR) on a gateway. Knowing how to configure the gateway using the Cisco IOS software feature is important to scaling the voice network.

References

For additional information, refer to these resources:

- *Cisco IOS SRST Version 3.2 System Administrator Guide*. http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_administration_guide_book09186a00802d3ca5.html.
- *Cisco CallManager Express/ITS and SRST*. http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp.
- *Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers (NM-HDV)*. http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/ccm_c/intcnf2.htm#wp1052086.
- *Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers (NM-HDV2 or NM-HD-1V/2V/2VE)*. http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/ccm_c/intcnf2.htm#wp1059545.

- *Configuring Enhanced Conferencing and Transcoding (PVDM-256K)*. http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/ccm_c/intcnf2.htm#wp1051497.
- *CallManager 4.0(1) and above and IOS Gateway DSP Farm Configuration Example*. http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/products_configuration_example09186a0080334294.shtml.
- Cisco DSP Calculator Tool. http://www.cisco.com/cgi-bin/Support/DSP/cisco_prodsel.pl.
- *Connecting Network Module in Gateway Routers*. http://cco/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/nm_inst/nm-doc/conntvoi.htm.
- *IP Communications High-Density Digital Voice/Fax Network Module*. http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/hdd_vfnm.htm#wp1049156.
- *DSP on NM-HDV2 Functionality Verification for 2600XM/2691/2800/3700/3800 Platforms*. http://www.cisco.com/en/US/partner/tech/tk652/tk653/technologies_tech_note09186a008039c316.shtml.
- *Cisco IOS Tcl IVR and VoiceXML Application Guide - 12.3(14)T and later*. http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/tcl_c/index.htm.
- *Configuring TCL IVR Applications*. http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_c/vvfivr.pdf.

Module 5

Deploying 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 what a gatekeeper does and what a directory gatekeeper is and how it serves gatekeepers. Additionally, you will learn how to configure gatekeepers to interoperate with gateways.

Module Objectives

Upon completing this module, you will be able to implement gatekeepers and directory gatekeepers in an H.323 VoIP environment. This ability includes being able to meet these objectives:

- Identify the features and functions of a gatekeeper
- Configure single and multiple zone gatekeepers to provide number resolution and CAC for H.323 gateways
- Configure directory gatekeepers in a multiple-gatekeeper environment
- Implement gatekeeper redundancy

Lesson 1

Cisco Gatekeeper Overview

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 transitional message protocol. This lesson provides the foundation for the "Implementing Cisco Gatekeepers" and "Implementing Cisco Directory Gatekeepers" lessons, where you will start to learn the elements in configuring gatekeepers and directory gatekeepers in different scenarios.

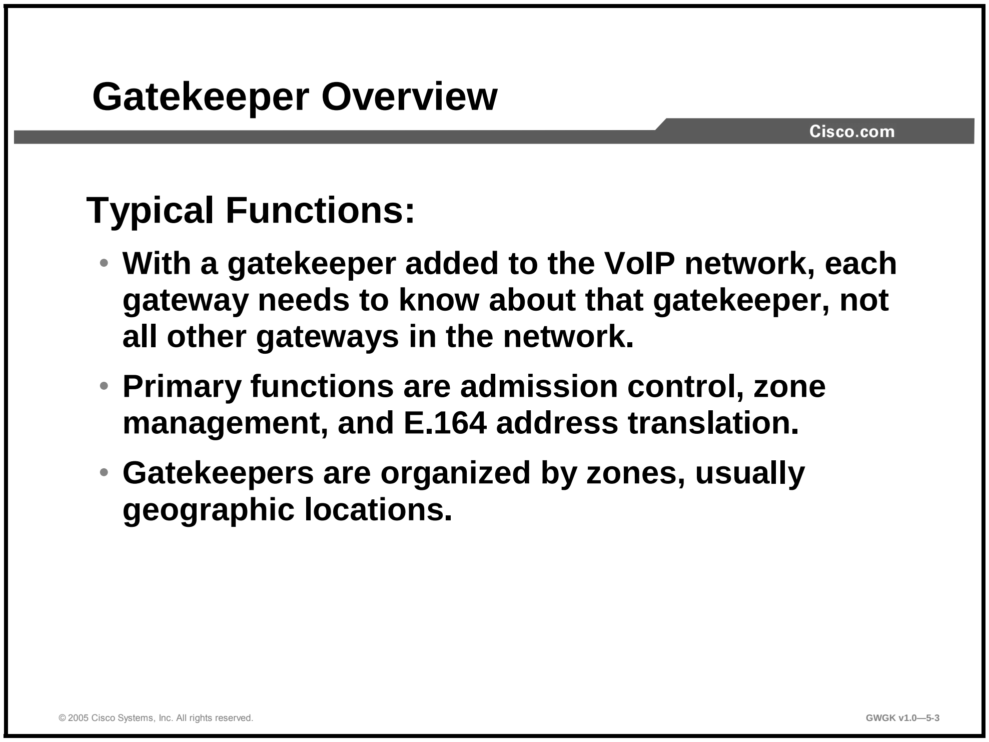
Objectives

Upon completing this lesson, you will be able to identify the features and functions of a gatekeeper. This ability includes being able to meet these objectives:

- Describe the functionality of gatekeepers in an H.323 environment
- Define the hardware and software required to support gatekeeper functions
- Describe the signaling between gateways and gatekeepers
- Describe the function of zones and zone prefixes
- Describe the function of technology prefixes
- Configure a gatekeeper to provide H.323 proxy services
- Describe the function of GKTMP
- Describe the gatekeeper address resolution process

Gatekeeper Overview

This topic gives an overview of gatekeepers and their functions.



Gatekeeper Overview

Cisco.com

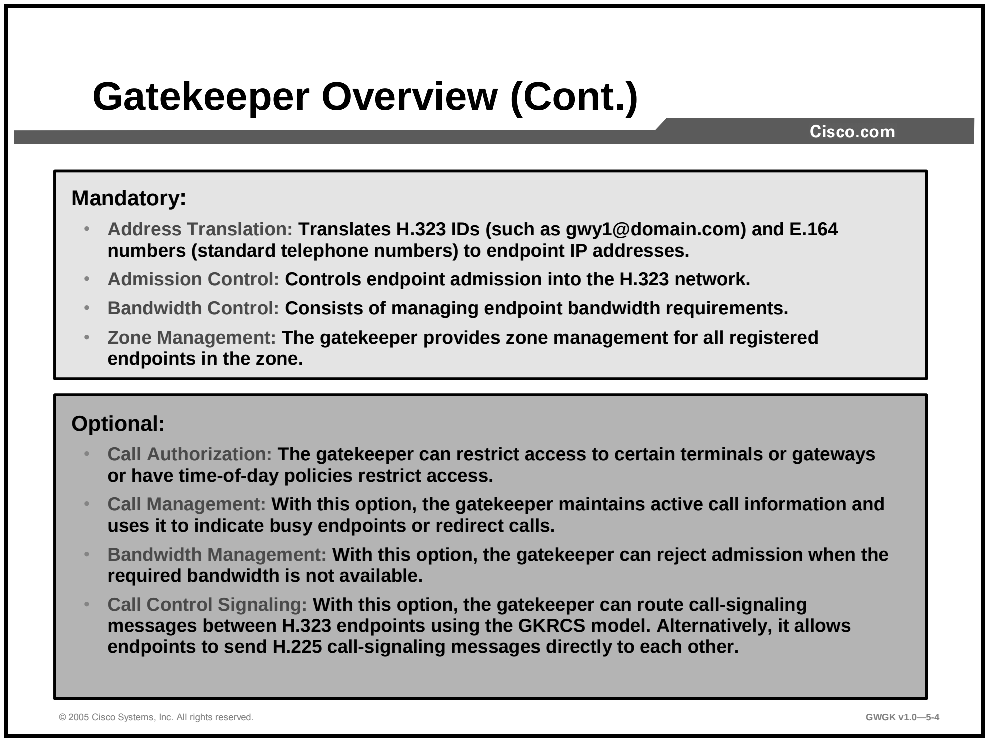
Typical Functions:

- **With a gatekeeper added to the VoIP network, each gateway needs to know about that gatekeeper, not all other gateways in the network.**
- **Primary functions are admission control, zone management, and E.164 address translation.**
- **Gatekeepers are organized by zones, usually geographic locations.**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—5-3

A gatekeeper can maintain a registry of devices in a multimedia network. A gatekeeper provides call control services to the H.323 endpoints. The devices register with the gatekeeper at startup and request admission to a call from the gateway. A gatekeeper is logically separate from the endpoints, but its physical implementation may coexist with a terminal, Multipoint Conference Unit (MCU), gateway, or other non-H.323 LAN device. Use of a gatekeeper is optional in an H.323 network environment.



Gatekeeper Overview (Cont.)

Cisco.com

Mandatory:

- Address Translation: **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: **The gatekeeper 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: **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.**
- Call Control Signaling: **With this option, the gatekeeper can route call-signaling messages between H.323 endpoints using the GKRCS model. Alternatively, it allows endpoints to send H.225 call-signaling messages directly to each other.**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—5-4

Gatekeepers have mandatory and optional responsibilities. The following mandatory responsibilities are those tasks that occur simply because the device is in the network and has been configured.

- **Address Translation:** 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 translate 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 the RAS messages admission request (ARQ), admission confirmation (ACF), and admission rejection (ARJ) to achieve this. Admissions control may also be a null function that admits all requests.
- **Bandwidth Control:** Gatekeepers must support the RAS bandwidth messages. However, the individual policy of the service provider or enterprise manager determines how the gatekeepers provide the bandwidth access or bandwidth management. For instance, if a network manager has specified a threshold for the number of simultaneous connections on the H.323 network, the gatekeeper can refuse to make any more connections once the threshold is reached. The result is to limit the total allocated bandwidth to some fraction of the total available, leaving the remaining bandwidth for data applications. In many cases, any bandwidth requests will be honored, unless the network or particular gateway is congested.
- **Zone Management:** A gatekeeper is required to provide the above functions-address translation, admissions control, and bandwidth control-for terminals, gateways, and MCU located within its zone of control.

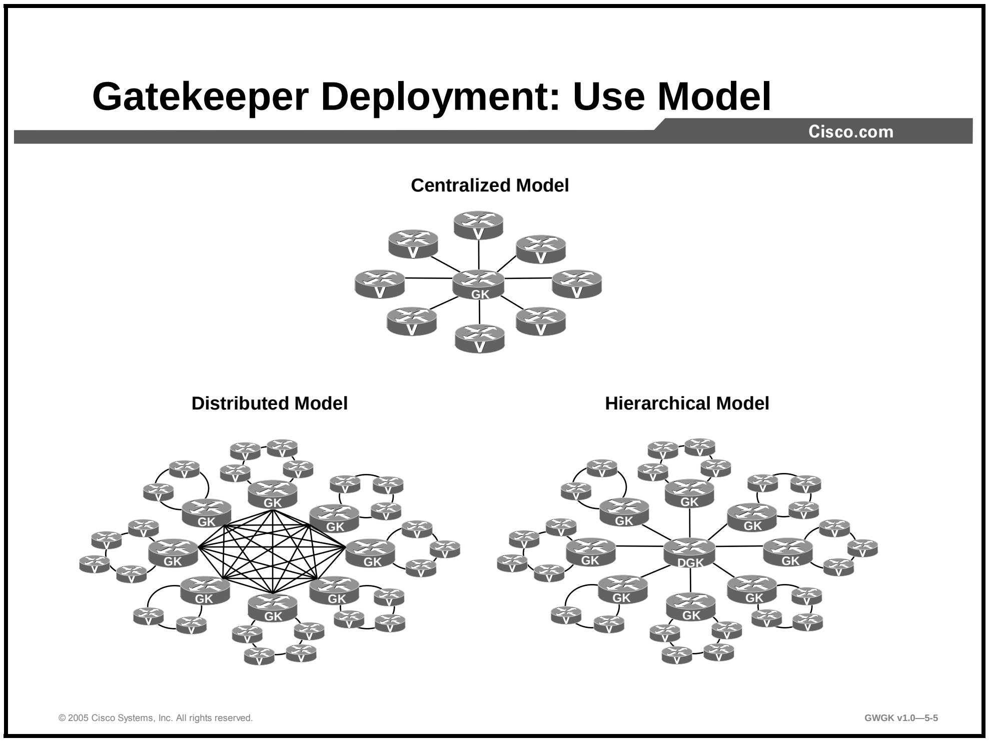
The optional responsibilities are those tasks out side of the gatekeepers expected role; all of which are configurable.

These are just a few of the optional responsibilities the gatekeeper can provide.

- **Call Authorization:** With this option, the gatekeeper can restrict access to certain terminals or gateways, have time-of-day policies restrict access, or both.
- **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.
- **Call Control Signaling:** With this option, the gatekeeper can route call-signaling messages between H.323 endpoints using the gatekeeper routed call signaling (GKRCS) model. Alternatively, it allows endpoints to send H.225 call-signaling messages directly to each other.

Deployment Scenarios

This topic describes gatekeeper deployment models.



Gatekeeper Deployment: Use Model

Cisco.com

Centralized Model

Distributed Model

Hierarchical Model

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—5-5

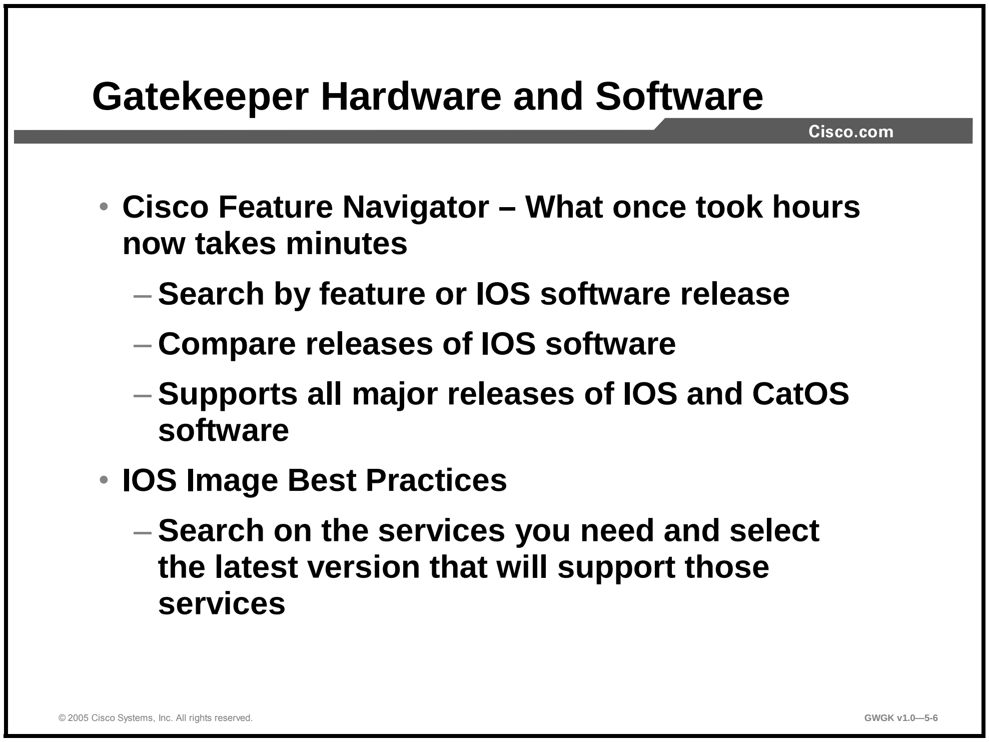
This figure shows three common gatekeeper deployment models The models are described in detail here.

- **Centralized gatekeeper configuration:** A single gatekeeper can support call routing between clusters and call admission control for up to 100 Cisco CallManager clusters.
- **Distributed gatekeeper configuration:** Gatekeepers can be distributed to conserve bandwidth or to provide local call routing for H.323 gateways in case of a WAN failure.
- **Distributed gatekeeper configuration with directory gatekeeper:** Because there is no gatekeeper protocol available to update gatekeeper routing tables, the use of a directory gatekeeper can help make distributed gatekeeper configurations more scalable and more manageable. Implementing a directory gatekeeper makes gatekeeper configurations at each site simpler and moves most of the configuration for interzone communication into the directory gatekeeper.

  Without a directory gatekeeper, you would have to add an entry in every gatekeeper on the network every time you add a new zone on one of the gatekeepers. However, with a directory gatekeeper, you can add the new zone in the local gatekeeper and the directory gatekeeper only. If the local gatekeeper cannot resolve a call request locally, it forwards that request to the directory gatekeeper with a matching zone prefix.

Gatekeeper Hardware and Software Requirements

This topic describes gatekeeper hardware and software requirements.



Gatekeeper Hardware and Software

Cisco.com

- Cisco Feature Navigator – What once took hours now takes minutes
  - Search by feature or IOS software release
  - Compare releases of IOS software
  - Supports all major releases of IOS and CatOS software
- IOS Image Best Practices
  - Search on the services you need and select the latest version that will support those services

GWGK v1.0—5-6

To determine the latest Cisco IOS software version that is needed for the various router platforms, you will need to search the Feature Navigation Tool. For example, you may want to search for which IOS version would be best to support a high-performance gatekeeper. You can find the platform and IOS version for gatekeeper by using the Feature Navigation Tool on Cisco.com at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml.

To start the search, select “high-performance gatekeeper”. The Feature Navigator will return all the versions of IOS that support this feature. This includes General Development (GD), LocalDirector (LD), and Early Deployment (ED) releases as and the release number, platform type, feature set, image name, and DRAM and Flash requirements.

The list complied in this figure was derived from the high-performance gatekeeper IOS feature. Here is the IOS feature definition:

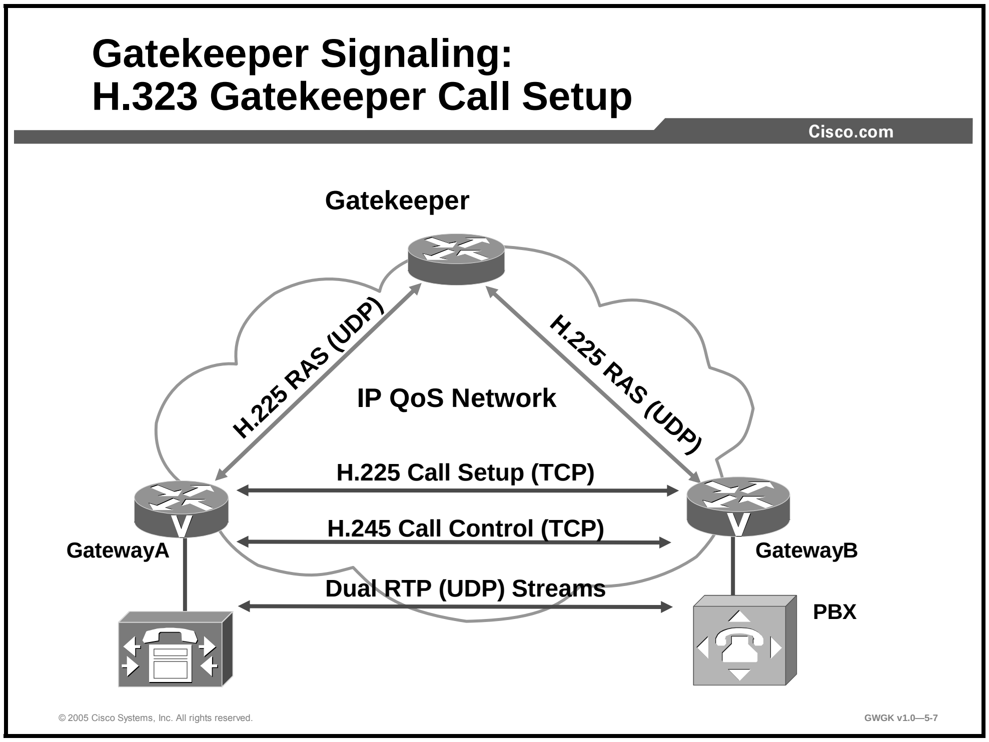
- The high-performance gatekeeper feature introduces new gatekeeper functionality and modifications for facilitating carrier class reliability, security, and performance into the Cisco voice network solution portfolio.
- These H.323 standard-based features have carrier-grade reliability and performance characteristics with a robust open-application protocol interface to enable development of enhanced applications like voice Virtual Private Networks (VPNs) and wholesale voice solutions.

Information on the high-performance gatekeeper can be found at http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm_5/ft_0394.htm.

For more information refer to the *Cisco IOS H.323 Configuration Guide* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/323confg/index.htm

Gatekeeper Signaling

This topic describes gatekeeper signaling.



Gatekeeper Signaling:
H.323 Gatekeeper Call Setup

Cisco.com

GWGK v1.0—5-7

The initial signaling from a gateway to a gatekeeper is done through H.225 RAS. Gateways can discover their gatekeepers through one of two processes.

- **Unicast Discovery:** Uses User Data Protocol (UDP) port 1718. In this process, endpoints are configured with the gatekeeper IP address and can attempt registration immediately. The gatekeeper replies with a gatekeeper confirmation (GCF) or gatekeeper rejection (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 remains silent. A gatekeeper can be configured to respond only to certain subnets.

If a gatekeeper is not available, the gateway periodically attempts to rediscover a gatekeeper. If a gateway discovers the gatekeeper has gone off line, it stops accepting new calls and attempts to rediscover a gatekeeper. Active calls are not affected.

Gateway-to-gateway signaling is H.225 call control, or setup, signaling. 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.

A reliable Transmission Control Protocol [TCP] call control channel is created across an IP network on TCP port 1720. This port initiates the Q.931 call control messages for the purpose of connecting, maintaining, and disconnecting calls.

When a gatekeeper is present in the network zone, H.225 call setup messages are exchanged either via direct call signaling or GKRCS. The gatekeeper decides which method to chose during the RAS admission message exchange.

If no gatekeeper is present, H.225 messages are exchanged directly between the endpoints.

Once 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 of the exchange of end-to-end H.245 messages between communicating H.323 endpoints or terminals. 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 H.245 call control protocol is used to resolve the call media type and establish the media flow, before the call can be established. It also manages the call after it has been established.

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

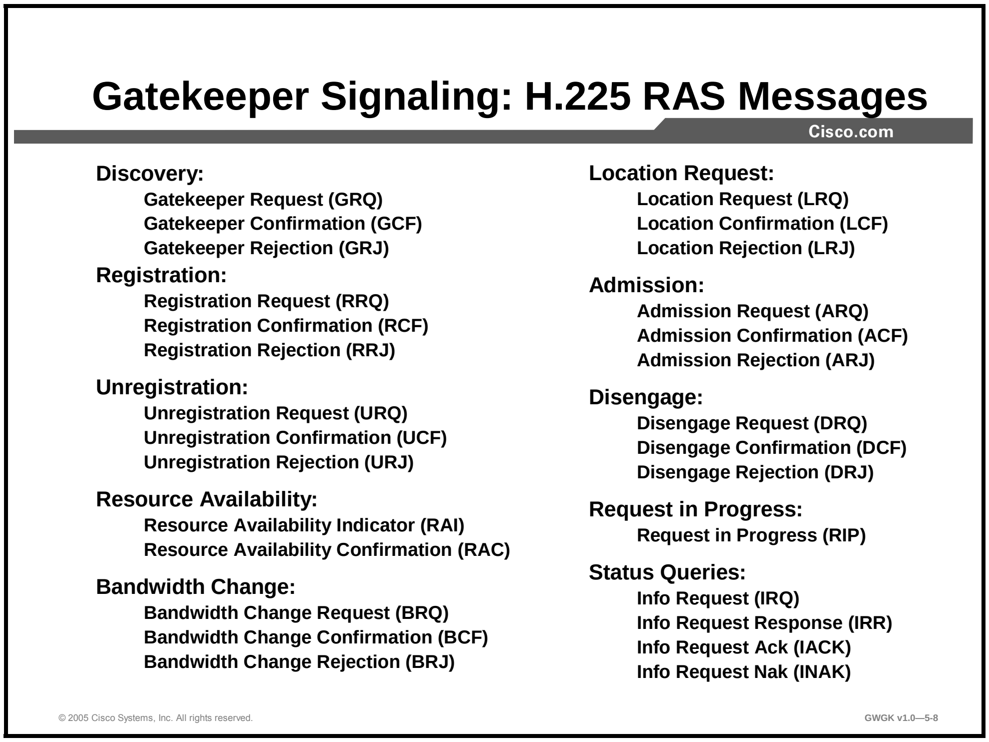
- Real-Time Transport Protocol (RTP) ports are negotiated from the lowest number.
- H.245 TCP port is negotiated during H.225 for H.323 standard connect.
- RTP UDP port range is 16384 to 32768.

Here is an example of a static configuration where unicast is used to discover the gatekeeper:

```
interface FastEthernet0/1
 description Connect to GK via Cat6509
 ip address 172.16.4.3 255.255.255.0
 service-policy input INBOUND
 speed 100
 full-duplex
 h323-gateway voip interface
 h323-gateway voip id GK-FRSW ipaddr 172.16.4.1 1719
 h323-gateway voip h323-id DFW-GW
 h323-gateway voip tech-prefix 1#


H.323 service is up
 Gateway  DFW-GW  is registered to Gatekeeper GK-FRSW
```

Here is an example of a multicast configuration where the gateway discovers the gatekeeper by using an IP multicast address of 224.0.1.41:

```
interface FastEthernet0/1
  ip address 172.16.4.3 255.255.255.0
 speed 100
 full-duplex
 h323-gateway voip interface
 h323-gateway voip id GK-FRSW multicast
 h323-gateway voip h323-id DFW-GW
 h323-gateway voip tech-prefix 1#

router ospf 1
network 224.0.1.41 0.0.0.0 <area#>
ip mulitcast-routing
```



Gatekeeper Signaling: H.225 RAS Messages

Cisco.com

Discovery:
- Gatekeeper Request (GRQ)
- Gatekeeper Confirmation (GCF)
- Gatekeeper Rejection (GRJ)

Registration:
- Registration Request (RRQ)
- Registration Confirmation (RCF)
- Registration Rejection (RRJ)

Unregistration:
- Unregistration Request (URQ)
- Unregistration Confirmation (UCF)
- Unregistration Rejection (URJ)

Resource Availability:
- Resource Availability Indicator (RAI)
- Resource Availability Confirmation (RAC)

Bandwidth Change:
- Bandwidth Change Request (BRQ)
- Bandwidth Change Confirmation (BCF)
- Bandwidth Change Rejection (BRJ)

Location Request:
- Location Request (LRQ)
- Location Confirmation (LCF)
- Location Rejection (LRJ)

Admission:
- Admission Request (ARQ)
- Admission Confirmation (ACF)
- Admission Rejection (ARJ)

Disengage:
- Disengage Request (DRQ)
- Disengage Confirmation (DCF)
- Disengage Rejection (DRJ)

Request in Progress:
- Request in Progress (RIP)

Status Queries:
- Info Request (IRQ)
- Info Request Response (IRR)
- Info Request Ack (IACK)
- Info Request Nak (INAK)

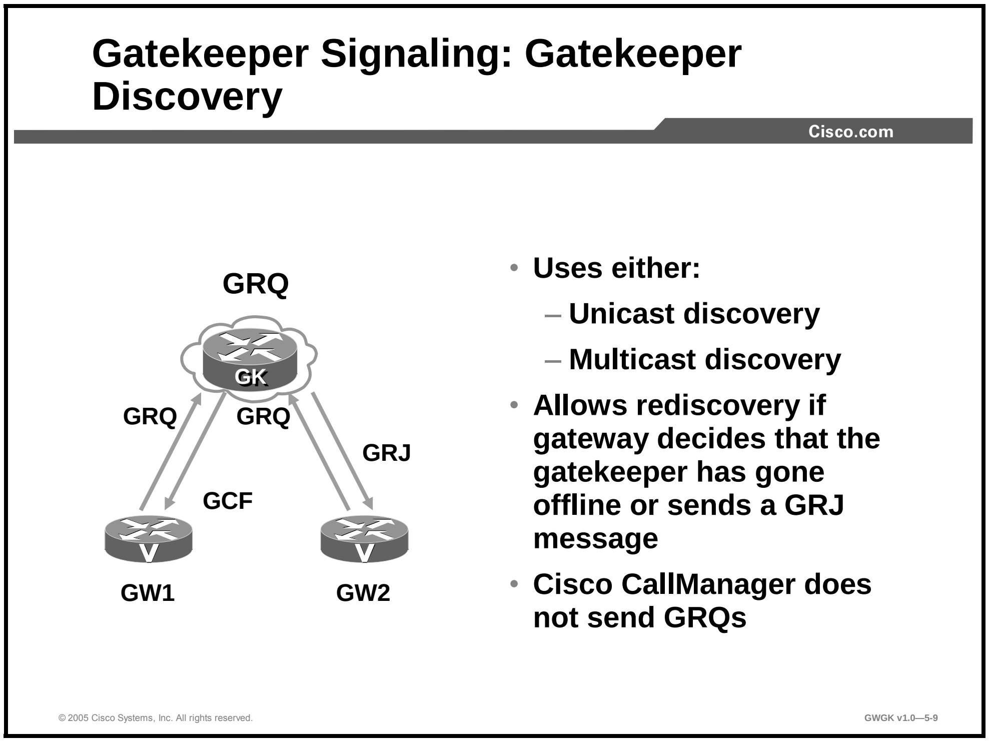
GWGK v1.0—5-8

This figure shows common RAS signals that are initiated by a gateway and gatekeeper. The following is a list of definitions of the common RAS signals.

- **Gatekeeper Discovery Messages:** The gatekeeper request (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.
  - **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.
- **Gateway Registration Request 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 rejection (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.

- **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.
  - **Unregister confirmation (UCF):** Sent from an endpoint or a gatekeeper to confirm an unregistration.
  - **Unregister rejection (URJ):** Indicates that an endpoint was not preregistered with the gatekeeper.
- **Admission Request Messages:** The ARQ message requests that an endpoint be allowed access to the packet-based network by the gatekeeper, which 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.
- **Location Request (LRQ) Messages:** The LRQ messages are commonly used between inter-zone gatekeepers to get the IP addresses of different zone endpoints. Initiated by a gatekeeper to a Directory gatekeeper
  - **LRQ:** Sent by a gatekeeper to the directory gatekeeper to request the contact information for one or more E.164 addresses
  - **Location confirmation (LCF):** Sent by a directory gatekeeper and contains the call signaling channel or RAS channel address of itself or the requested endpoint. It uses the requested endpoint address when directed endpoint call signaling is used.
  - **Location rejection (LRJ):** Sent by gatekeepers that received an LRQ for a requested endpoint that is not registered or that has unavailable resources.
- **Status Request Messages**
  - **Information request (IRQ):** Sent from a gatekeeper to an endpoint requesting status.
  - **Information request response (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.
  - **Information request acknowledge (IACK):** Used by the gatekeeper to respond to IRR messages.
  - **Information request negotiation acknowledge (INACK):** Used by the gatekeeper to respond to IRR messages.

- **Bandwidth Control Messages**: The bandwidth request (BRQ) message requests that an endpoint be granted a changed packet-based network bandwidth allocation by the gatekeeper, which either grants the request with a bandwidth confirmation (BCF) message or denies it with a bandwidth rejection (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 change request.
  - **BRJ:** Sent by the gatekeeper rejecting the bandwidth change request.
- **The Resource Availability Indication (RAI) Message:** The 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.
- **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 a RIP message knows to continue to wait for a gatekeeper response.
- **Disengage Request Messages:** If sent from an endpoint to a gatekeeper, the disengage request (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.



Gatekeeper Signaling: Gatekeeper Discovery

Cisco.com

- Uses either:
  - Unicast discovery
  - Multicast discovery
- Allows rediscovery if gateway decides that the gatekeeper has gone offline or sends a GRJ message
- Cisco CallManager does not send GRQs

GWGK v1.0—5-9

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.

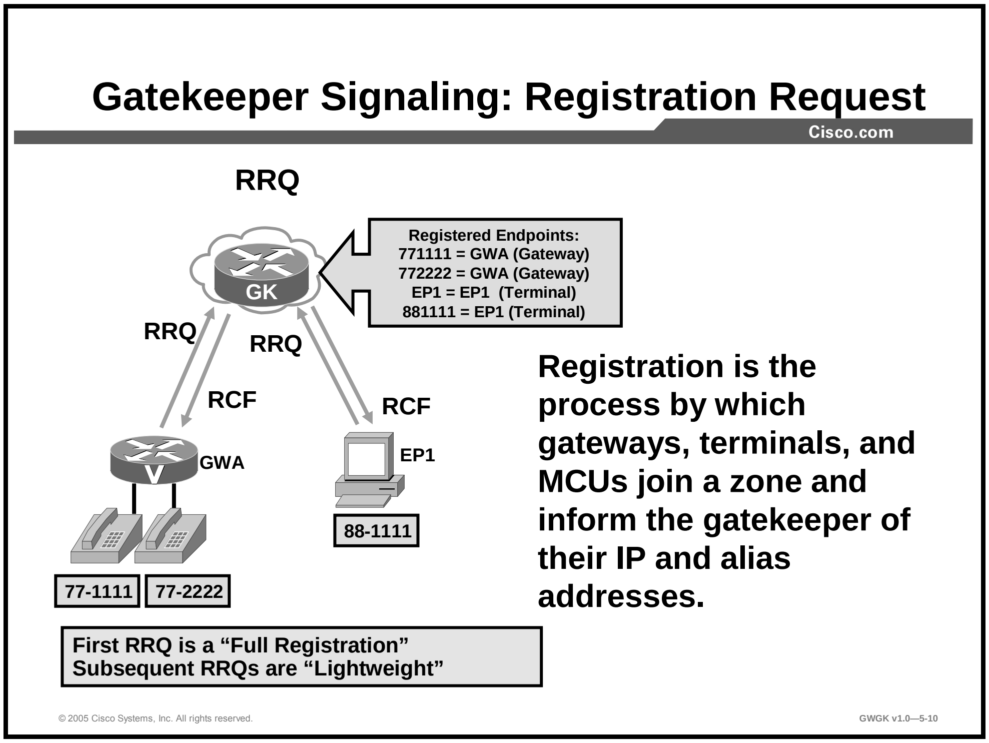
If the message is sent via multicast, the endpoint registers nondeterministically with the first gatekeeper that responds to the message. To enforce predictable behavior, where endpoints on certain subnets are assigned to specific gatekeepers, the **zone subnet** command can be used to define the subnets 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 one 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. If the gateway discovered gatekeeper has gone off line, it will stop accepting new calls and attempt to rediscover a gatekeeper. Active calls are not affected.

There are two processes by which H.323 terminals or gateways discover their zone gatekeepers:

- **Unicast discovery (manual method):** 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. Most gateways are manually configured, so Unicast is the most common way to discover the gateways gatekeeper.
- **Multicast discovery (auto 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 remains silent. A gatekeeper can be configured to respond only to certain subnets.



Gatekeeper Signaling: Registration Request

Registered Endpoints:
771111 = GWA (Gateway)
772222 = GWA (Gateway)
EP1 = EP1 (Terminal)
881111 = EP1 (Terminal)

Registration is the process by which gateways, terminals, and MCUs join a zone and inform the gatekeeper of their IP and alias addresses.

First RRQ is a "Full Registration"
Subsequent RRQs are "Lightweight"

GWGK v1.0—5-10

The RRQ message is a request from a terminal to a gatekeeper to register. 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.

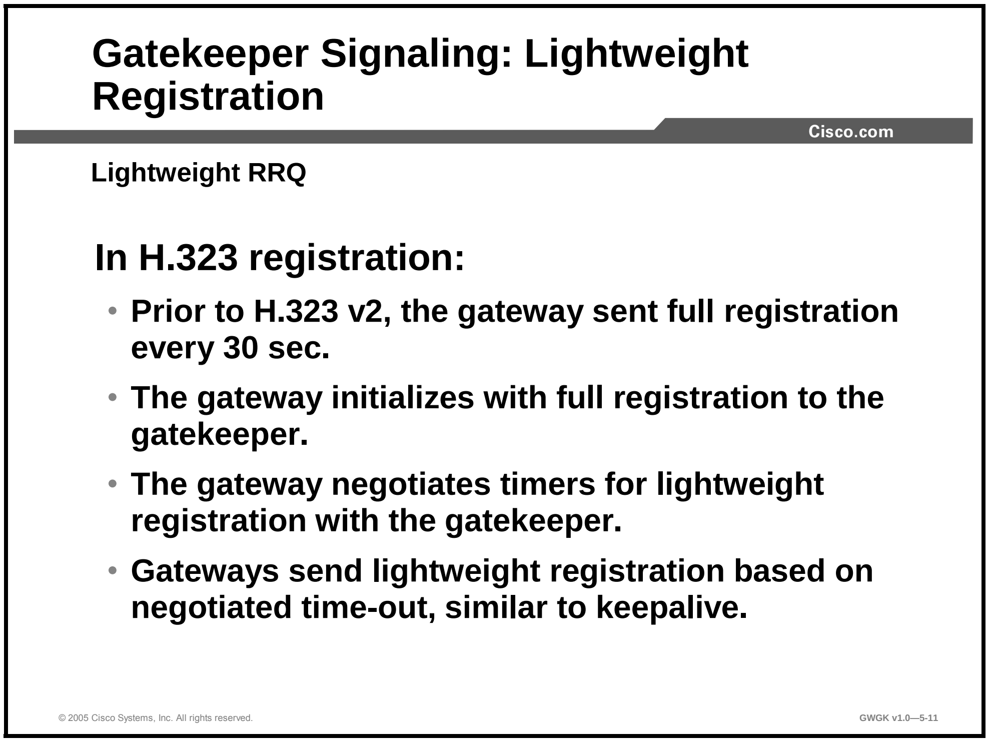
An H.323 gateway learns of a gatekeeper by using a static configuration or dynamic discovery. Static configuration simply means configuring the gatekeeper IP address on an Ethernet interface used for H.323 signaling.

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

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

Every E.164 address can be registered only once. Every gateway can register with only one active gatekeeper, and there can only be one gatekeeper per zone.

In the figure, Gateway A has two plain old telephone service (POTS) phones attached to it. When Gateway A registers with the gatekeeper, these two POTS destination patterns will automatically be registered with the gatekeeper. This registration will occur unless there is a command statement in the POTS dial peer that tells the gateway not to register the destination pattern to the gatekeeper. Endpoint 1 has an extension number of 88-1111 assigned to it. For the endpoint, the gatekeeper will register both the name of the endpoint and the destination pattern with the gatekeeper.



Gatekeeper Signaling: Lightweight Registration

Cisco.com

Lightweight RRQ

In H.323 registration:

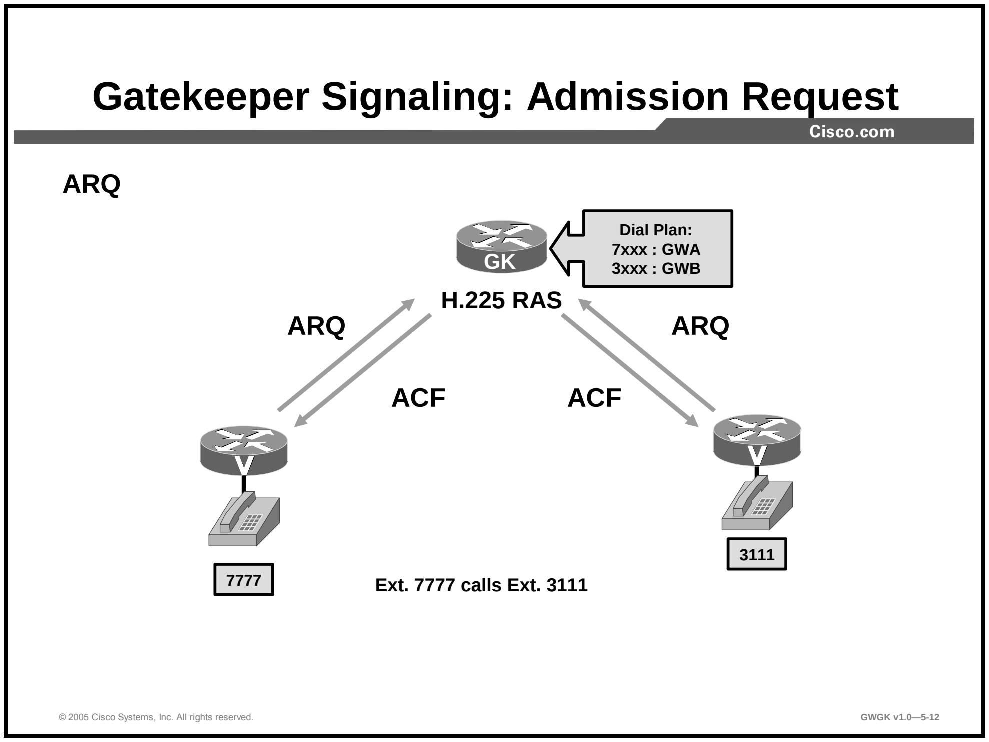
- **Prior to H.323 v2, the gateway sent full registration every 30 sec.**
- **The gateway initializes with full registration to the gatekeeper.**
- **The gateway negotiates timers for lightweight registration with the gatekeeper.**
- **Gateways send lightweight registration based on negotiated time-out,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

GWGK v1.0—5-11

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 a RCF message to the endpoint. Shortly before the TTL timer expires, the endpoint sends an RRQ message with 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.



Gatekeeper Signaling: Admission Request

Cisco.com

ARQ

GWGK v1.0—5-12

This example shows an admission request. After the call is set up, both Gateway A and Gateway B send an RAS IRR message to the gatekeeper. This would occur after the step marked 6—after the user at extension 3111 initiates hook-off. Gateway B sends a Q.931 connect message via H.225 back to gateway B. The remaining steps do not relate to RAS.

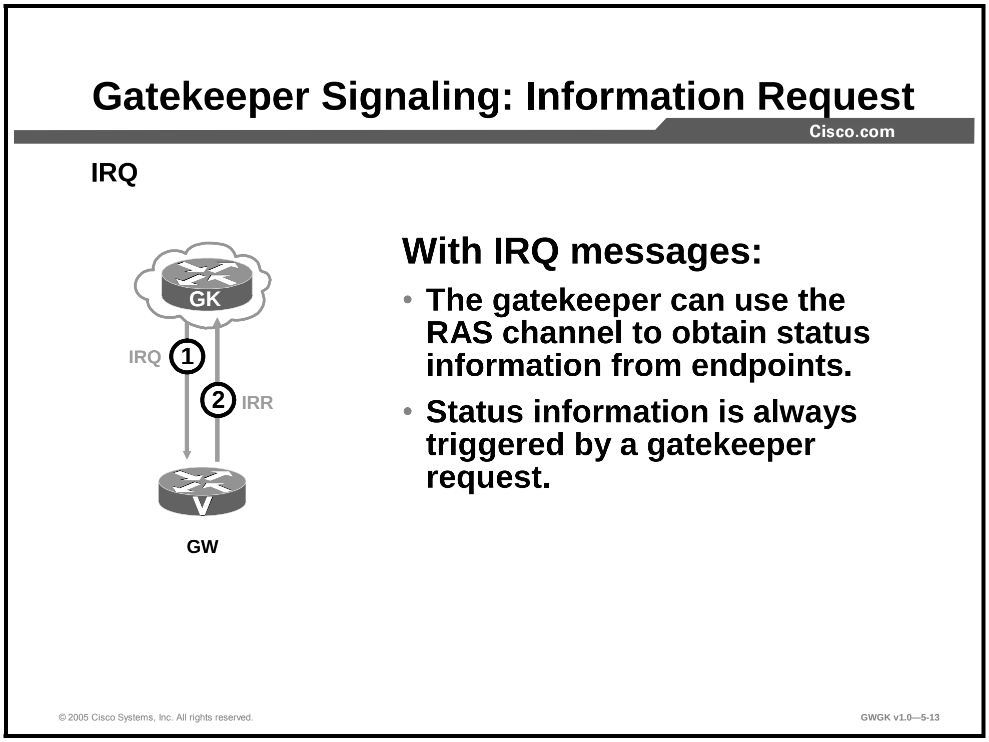
Admission messages between endpoints and gatekeepers provide the basis for call admissions and bandwidth control. Gatekeepers authorize access to H.323 networks by confirming or rejecting an admission request.

Admission Request Message Failures

It may not be clear from the RAS ARJ message why the message was rejected. The following list shows 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.
- **undefinedReason:** This message is used only if none of the other reasons are appropriate.
- **callerNotRegistered:** The endpoint asking for permission to be admitted to the call is not registered with the gatekeeper from which 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 available. 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 **transportQOS** of **gatekeeperControlled** in its ARQ, but the gatekeeper cannot or will not provide QoS for this call.
- **incompleteAddress:** This is used for “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 SCN (or PSTN). This is only used if the ARQ was from an ingress gateway, where **ARQ.terminalType.gateway** was present and **answerCall** was FALSE).
- **aliasesInconsistent: 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**. The destination endpoint does not have the capacity to accept the call. This is primarily intended for use with version 4 or later gateways that report their call capacity to the gatekeeper.



Gatekeeper Signaling: Information Request

Cisco.com

IRQ

With IRQ messages:

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

GWGK v1.0—5-13

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.

During call setup, the frequency of IRQ messages to nodes which are not made by Cisco is increased call state transition times can be inferred more accurately for accounting purposes.

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.

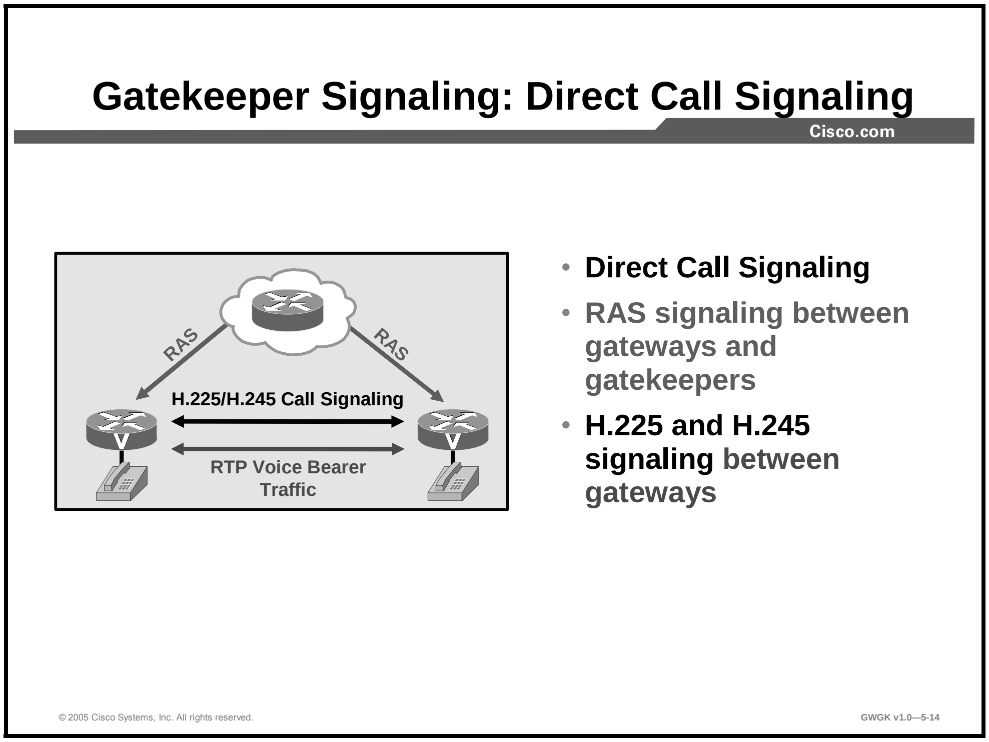
Whenever an IRR is sent, the age tags on the registration information for the endpoint are refreshed. In addition, if the IRR contains Cisco accounting information in its **nonStandardData** field, this information is used to generate authentication, authorization, and accounting (AAA) accounting transactions.

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. ICF is really a version 2 RAS message, but it is being used immediately because of its functionality. If the gateway or proxy does not receive the ICF, the IRR should be resent.

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

The IRQ message includes the following message:

- **requestSeqNum:** This value is a monotonically increasing number unique to the sender. It will be returned by the receiver in any messages associated with this specific message.
- **callReferenceValue:** This message indicates the call reference value (CRV)of the call that the query is about. If zero, this message is interpreted as a request for an IRR for each call the terminal is active on. If the terminal is not active on any calls, an IRR shall be sent in response to a CRV of 0, with all appropriate fields provided.
- **nonStandardData:** This message carries information not defined in this request (for example, proprietary data).
- **replyAddress:** The reply address is a transport address to send the IRR to, which may not be that of the gatekeeper.
- **callIdentifier:** This value is a globally unique call identifier that is set by the originating endpoint that can be used to associate RAS signaling with the modified Q.931 signaling used in this request.
- **integrityCheckValue:** Provides improved message integrity or message authentication of the RAS messages. The sender that is applying a negotiated integrity algorithm and the secret key upon the entire message computes this cryptographically based integrity check value. Prior to the **integrityCheckValue** computation, this field is ignored and is empty. After computation, the sender puts the computed integrity check value in the **integrityCheckValue** field and transmits the message.

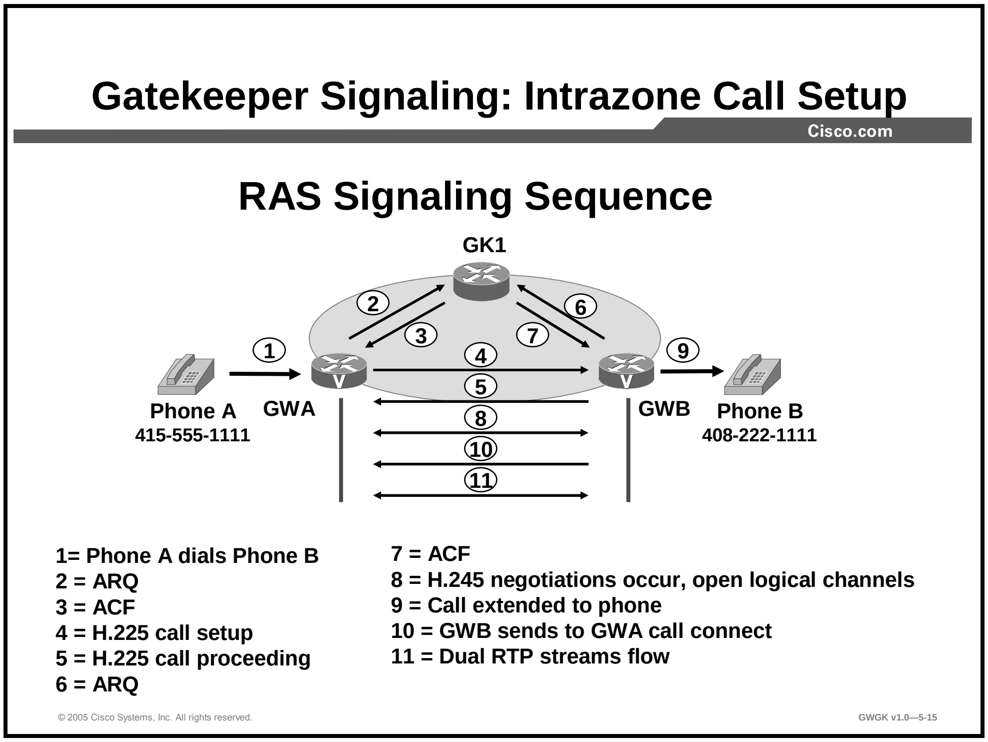


Gatekeeper Signaling: Direct Call Signaling

- **Direct Call Signaling**
- **RAS signaling between gateways and gatekeepers**
- **H.225 and H.245 signaling between gateways**

H.225 messages are exchanged between the endpoints if there is no gatekeeper in the H.323 network. When a gatekeeper exists in the network, the H.225 messages are exchanged either directly between the endpoints or between the endpoints after they are routed through the gatekeeper. is the two types of direct endpoint signaling are called direct call signaling and gatekeeper-routed call signaling. The gatekeeper decides during RAS admission message exchange which method to chose.

For direct call signaling, the gatekeeper indicates that the endpoints can exchange call-signaling messages directly during the admission confirmation. The endpoints exchange the call signaling on the call-signaling channel. With this method, call-setup messages are directed to the terminating gateway or endpoint.



Gatekeeper Signaling: Intrazone Call Setup

Cisco.com

RAS Signaling Sequence

1= Phone A dials Phone B
2 = ARQ
3 = ACF
4 = H.225 call setup
5 = H.225 call proceeding
6 = ARQ

7 = ACF
8 = H.245 negotiations occur, open logical channels
9 = Call extended to phone
10 = GWB sends to GWA call connect
11 = Dual RTP streams flow

GWGK v1.0—5-15

This figure shows the sequence of the signaling events and the basic signaling that takes place between a gateway and gatekeeper. The steps are described in detail here:

Step 1 Phone A dials the phone number 408-222-1111 for Phone B.

Step 2 Gateway A sends Gatekeeper 1 an ARQ, asking permission to call Phone B.

Step 3 Gatekeeper 1 does a look-up and finds Phone B registered to Gateway B and returns an ACF with the IP address of Gateway B.

Step 4 Gateway A sends an H.225 Call-Setup to Gateway B with the phone number of Phone B.

Step 5 Gateway B sends an H.255 Call Proceeding message to Gateway A.

Step 6 Gateway B sends Gatekeeper 1 an ARQ, asking permission to answer Gateway A's call.

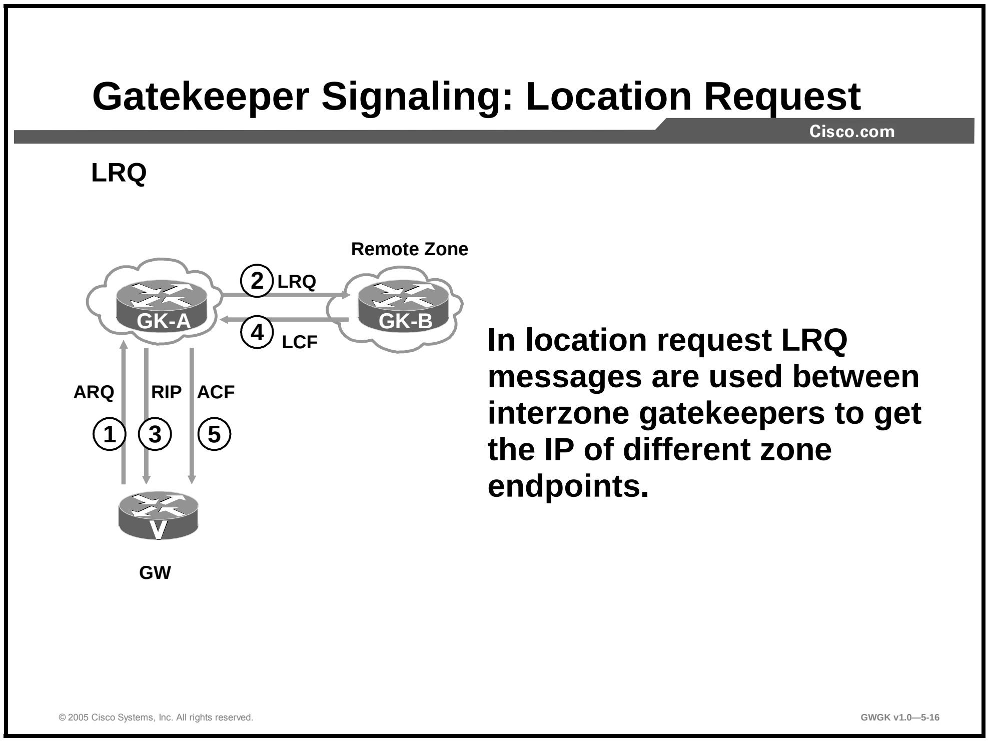
Step 7 Gatekeeper 1 returns an ACF with the IP address of Gateway A.

Step 8 Gateway B and Gateway A initiate an H.245 capability exchange and open logical channels.

Step 9 Gateway B sets up a POTS call to Phone B at 408-222-1111.

Step 10 When Phone B answers, Gateway B sends an H.245 call connect to Gateway A.

Step 11 Dual RTP streams flow between gateways.



Gatekeeper Signaling: Location Request

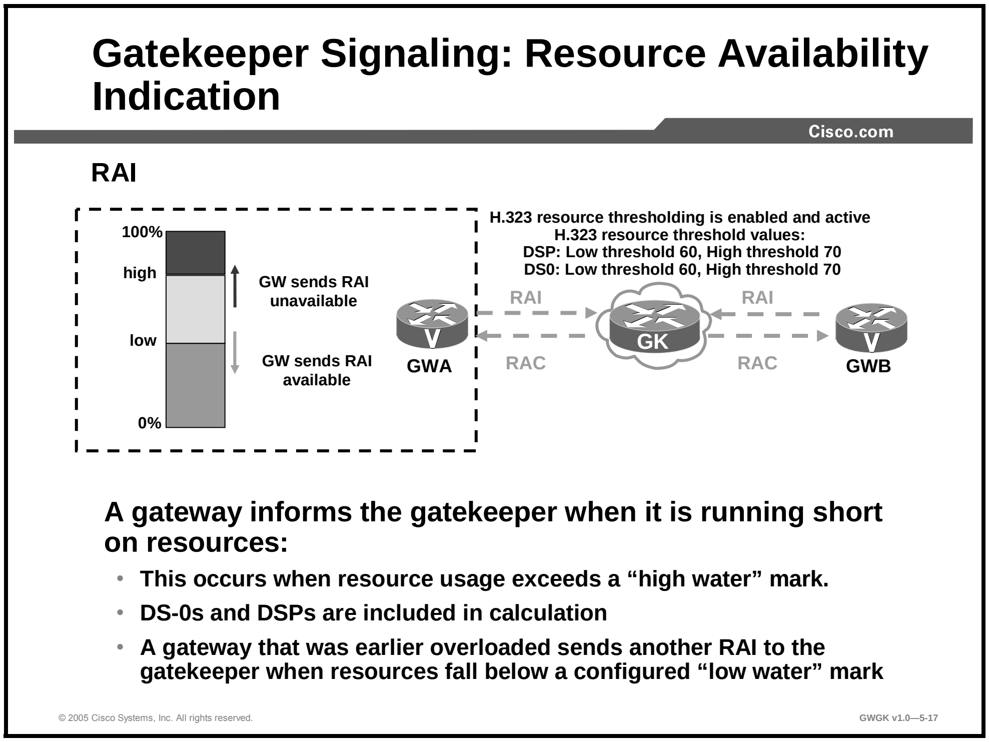
LRQ

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

GWGK v1.0—5-16

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

Note	LRQs are not RAS messages exchanged between gateways and gatekeepers. They are only exchanged between gatekeepers.



Gatekeeper Signaling: Resource Availability Indication

Cisco.com

RAI

100%
high
low
0%
GW sends RAI unavailable
GW sends RAI available
GWA
H.323 resource thresholding is enabled and active
H.323 resource threshold values:
DSP: Low threshold 60, High threshold 70
DS0: Low threshold 60, High threshold 70
RAI
RAI
GK
RAC
RAC
GWB

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

- **This 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**

GWGK v1.0—5-17

To allow gatekeepers to make intelligent call routing decisions, the gateway reports the status of its resource availability to its gatekeeper. Resources that are monitored are digital signal level 0 (DS-0) channels and digital signal processor (DSP) channels.

The gateway reports its resource status to the gatekeeper with the use of RAS RAI messages. 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 cross above another configurable threshold, the gateway sends an RAI that indicates that the resource depletion condition no longer exists.

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 RAC message to each RAI.

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 gateway is peering to the PSTN. A sample call flow follows:

1. A gatekeeper receives a LRQ or an ARQ. It may have multiple potential gateways to use to reach the requested E.164 number within the PSTN.

2. The gatekeeper asks each gateway which gateway is under heavy load.

3. The decision of which gateway to use now comes from the originating gatekeeper when it sends an ACF or LCF message back to the requester (the gateway, gatekeeper, or directory gatekeeper) with the IP address of the gateway that is under low load conditions.

There are two gateways shown in the figure,. Gateway A shows the configuration with high and low threshold values. The gateways will send out periodic RAIs to inform the gatekeeper of their relative workload. If the gatekeeper receives an RAI that tells it that, for instance, Gateway A is out of resources, then the gatekeeper can send an ACF or LCF back to the requester with the address of Gateway B.

To configure a gateway to report H.323 resource availability to its gatekeeper, use the resource threshold command in gateway configuration mode. To disable gateway resource-level reporting, use the no form of this command. The following command was integrated into Cisco IOS Release 12.2(11)T.

```
gateway1(config-gateway)# resource threshold [all] [high
percentage-value] [low percentage-value]
```

Syntax Description

Syntax	Description
all	(Optional) High- and low-parameter settings are applied to all monitored H.323 resources. This is the default condition.
high ***percentage-value***	(Optional) Resource utilization level that triggers an RAI message that indicates 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.

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

Use the **show call resource voice threshold** command from enable mode to check the threshold state on the gateway, as shown here.

```
            DFW-GW#show call resource voice threshold


            Resource Monitor -  Dial-up Resource Threshold
Information:


            DS0 Threshold:


            Client Type: h323
            High Water Mark: 70
            Low Water Mark: 60
            Threshold State: low_threshold_hit


            DSP Threshold:
```

```
Client Type: h323
High Water Mark: 70
Low Water Mark: 60
Threshold State: low_threshold_hit
```

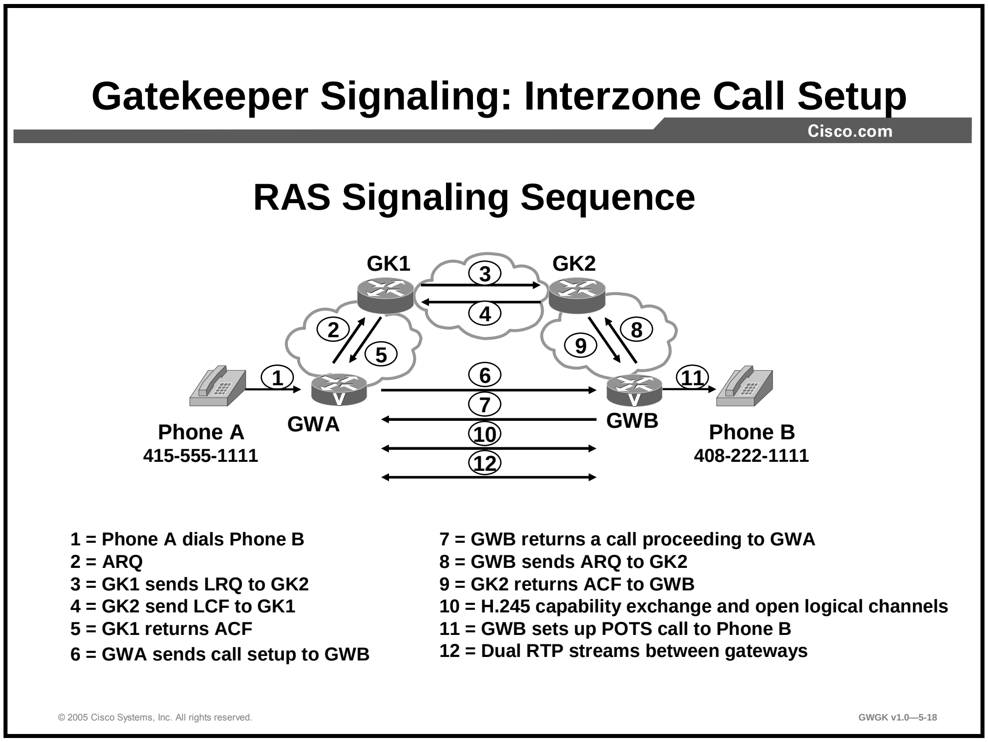
In the following example, **show gateway** is the result of the configuration of resource threshold.

```
DFW-GW#show gateway
H.323 ITU-T Version: 4.0 H323 Stack Versions: 0.1

 H.323 service is up
 Gateway  DFW-GW  is registered to Gatekeeper DFW-GK

Alias list (CLI configured)
 E164-ID 1001
 E164-ID 9725551001
 E164-ID 1002
 E164-ID 9725551002
 H323-ID DFW-GW
Alias list (last RCF)
 E164-ID 1001
 E164-ID 9725551001
 E164-ID 1002
 E164-ID 9725551002
 H323-ID DFW-GK

 H323 resource thresholding is Enabled and Active
 H323 resource threshold values:
  DSP: Low threshold 60, High threshold 70      ← Threshold
values
  DS0: Low threshold 60, High threshold 70      ← Threshold
values
```

Use the **show call resource voice stat** command from the enable mode to show the statistics of all the resources (DSPs and DS-0s).

In this output, the DSP use is 34 ÷ 120 = 28%, and the DS-0 utilization is 34 ÷ 48= 70%. The high threshold value configured on both cases (DSP and DS-0 utilization) is not exceeded.

```
            DFW-GW#show call resource voice stat


            Resource Monitor -  Dial-up Resource Statistics
Information:


            DSP Statistics:


            Utilization: 0 percent

            Total channels: 120     ← Total DSP Channels

Inuse channels: 34      ← Total in use channels or 34/120 =
28%


Disabled channels: 0

Pending channels: 0

Free channels: 86


DS0 Statistics:


Utilization: 0 percent

Total channels: 96

Addressable channels: 48      ← Total addressable channels

Inuse channels: 34      ← Total in use channels or 34/48 =
70%



Disabled channels: 24

Free channels: 14
```



Gatekeeper Signaling: Interzone Call Setup

Cisco.com

RAS Signaling Sequence

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

GWGK v1.0—5-18

This figure shows a how gatekeepers signal one another in a multi-zone gatekeeper network. This figure shows the sequence of RAS signaling events between gatekeepers and shows the LRQ RAS messages and how LRQ is used.

This figure shows the basic gateway to gatekeeper signaling between zones.

Step 1 Phone A dials the phone number 408-222-1111 for Phone B.

Step 2 Gateway A sends Gakekeeper1 an ARQ, asking permission to call Phone B.

Step 3 Gatekeeper 1 does a look-up and does NOT find Phone B registered. Gatekeeper 1 does a prefix look-up and finds a match with Gatekeeper 2. Gatekeeper 1 sends an LRQ to Gatekeeper 2 and RIP to Gateway A.

Step 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.

Step 5 Gatekeeper 1 returns an ACF with the IP address of Gateway B.

Step 6 Gateway A sends an H.225 call-setup to Gateway B with the phone number of phone B.

Step 7 Gateway B sends an H.225 call proceeding message to Gateway A

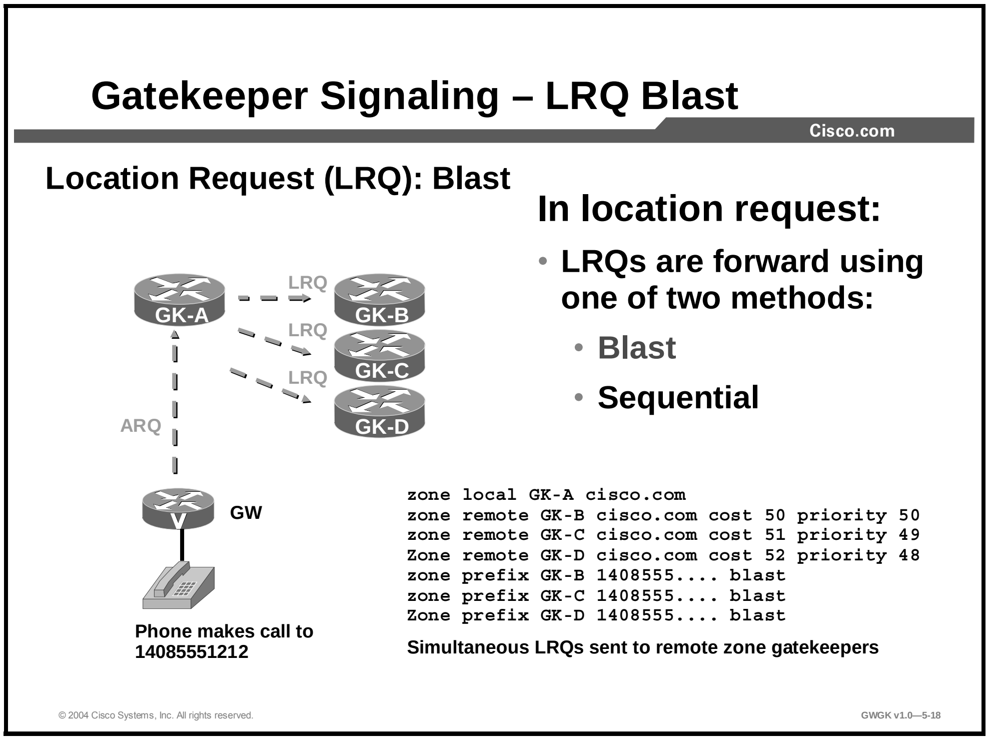
Step 8 Gateway B sends Gatekeeper 2 an ARQ, asking permission to answer the call from Gateway A.

Step 9 Gatekeeper 2 returns an ACF with the IP address of Gateway A.

Step 10 Gateway B and Gateway A initiate an H.245 capability exchange and open logical channels.

Step 11 Gateway B sets up a POTS call to Phone B at 408-222-1111.

Step 12 When Phone B answers, dual RTP streams flow between gateways.



Gatekeeper Signaling – LRQ Blast

Location Request (LRQ): Blast

In location request:

- **LRQs are forward using one of two methods:**
  - **Blast**
  - **Sequential**

```
zone local GK-A cisco.com
zone remote GK-B cisco.com cost 50 priority 50
zone remote GK-C cisco.com cost 51 priority 49
Zone remote GK-D cisco.com cost 52 priority 48
zone prefix GK-B 1408555.... blast
zone prefix GK-C 1408555.... blast
Zone prefix GK-D 1408555.... blast
```

Phone makes call to 14085551212

Simultaneous LRQs sent to remote zone gatekeepers

GWGK v1.0—5-18

As you are configuring your network, you may have multiple remote zones that can service a given dialed number. The gatekeeper should therefore be able to query all of them all at once. This is known as a “blast” LRQ.

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, as shown in the example here:

```
zone remote GK-B cisco.com cost 50 priority 50

zone remote GK-C cisco.com cost 51 priority 49

zone remote GK-D Cisco.com cost 52 priority 48
```

The cost and priority command options need to be examined carefully for correct operation. The default cost is 50 in a range from 1 to 100. In the example, you see that 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, then Gatekeeper C, and finally Gatekeeper D.

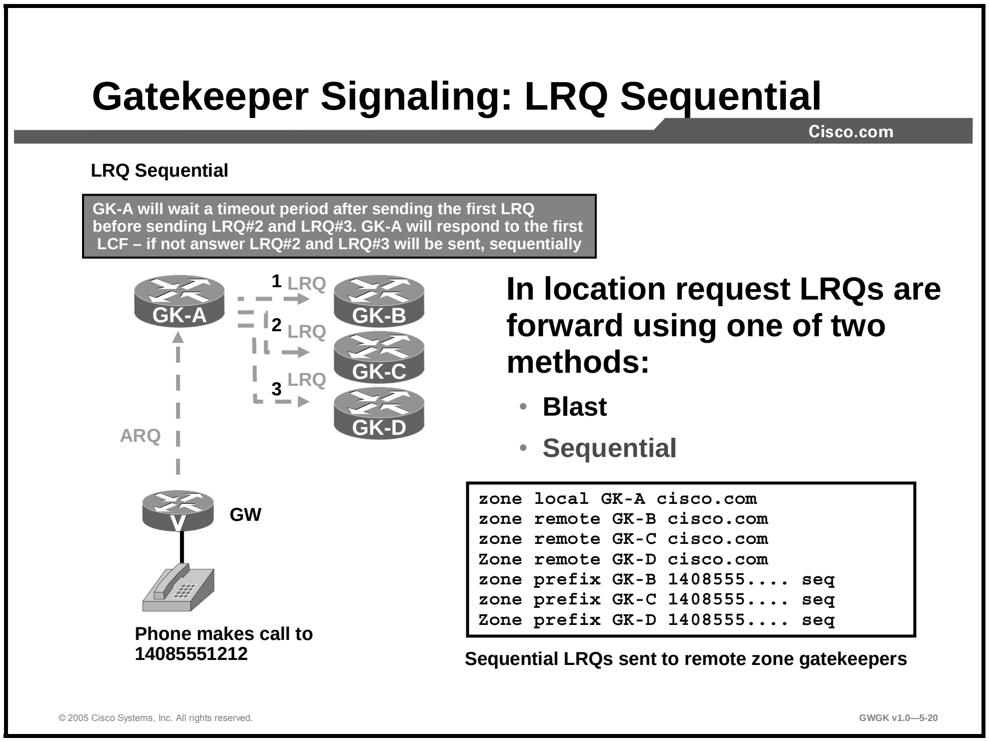
The priority can also be set. The default for this option is also 50 in a range from 1 to 100. In the example, you see that the gatekeepers with higher cost also have a lower priority. When each of the gatekeepers returns an LCF to Gatekeeper A, a decision as to which gatekeeper the call should be forwarded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

```
zone prefix GK-B 1408555.... blast
zone prefix GK-C 1408555.... blast
zone prefix GK-D 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 can be 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 based on sequence.

To summarize, Gatekeeper A receives an ARQ from a gateway for 14085551212. Gatekeeper A then blasts LRQs to all gatekeepers, in this case 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 Gatekeeper B as the gatekeeper to which to forward the call.



Gatekeeper Signaling: LRQ Sequential

LRQ Sequential

GK-A will wait a timeout period after sending the first LRQ before sending LRQ#2 and LRQ#3. GK-A will respond to the first LCF – if not answer LRQ#2 and LRQ#3 will be sent, sequentially

Phone makes call to 14085551212

In location request LRQs are forward using one of two methods:

- **Blast**
- **Sequential**

```
zone local GK-A cisco.com
zone remote GK-B cisco.com
zone remote GK-C cisco.com
Zone remote GK-D cisco.com
zone prefix GK-B 1408555.... seq
zone prefix GK-C 1408555.... seq
Zone prefix GK-D 1408555.... seq
```

Sequential LRQs sent to remote zone gatekeepers

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 before sending the next LRQ to the next gatekeeper on the list until all of the gatekeepers have been sent an LRQ. However, if the originating gatekeeper receives an LCF while it is waiting, it will terminate the LRQ forwarding process.

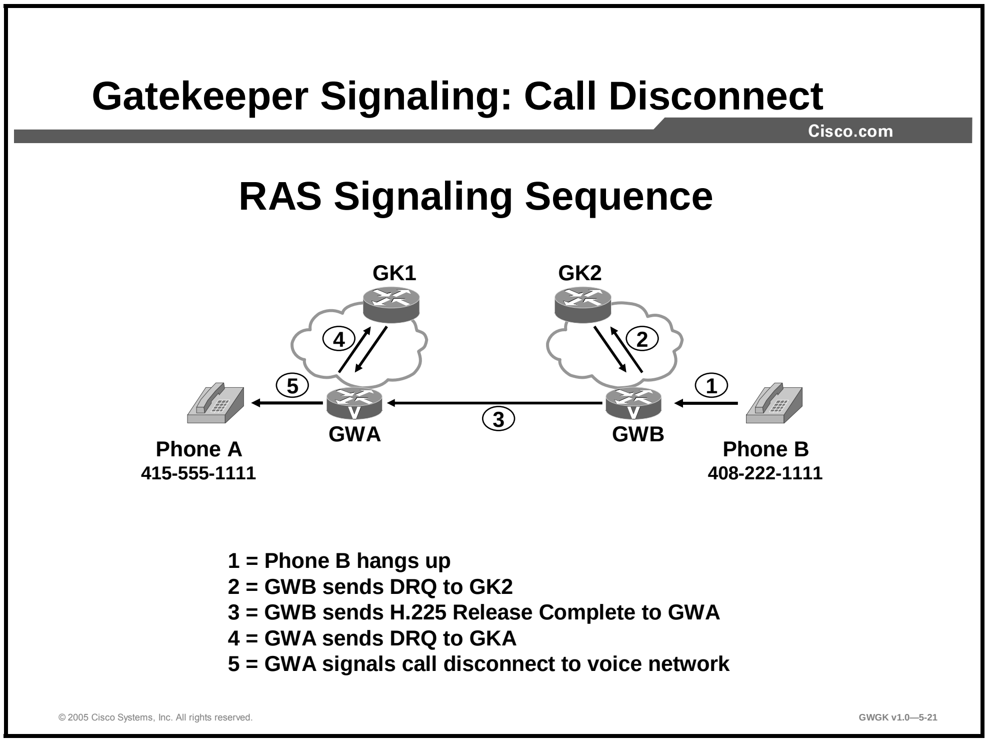
If you have multiple matching prefix zones, you may want to consider using sequential LRQ forwarding as opposed to blast LRQ forwarding. With sequential forwarding, you can configure which route is the primary, secondary and tertiary.

There are three gatekeepers in the example 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. Since sequence is the default method for LRQ forwarding, the option **seq** can be included, and sequential LRQ forwarding will take place.

Note that with sequential LRQs, there is a fixed timer between 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.

Finally, if Gatekeeper B or Gatekeeper C decides to forward the LRQ on to another gatekeeper (Gatekeeper D in this case), it acts as a directory gatekeeper. Directory gatekeepers wait to receive responses o all of their LRQs, and then provide a single response to the originating gatekeeper. For example, suppose that Gatekeeper A sends an LRQ to Gatekeeper B. Gatekeeper B forwards it to Gatekeeper C and Gatekeeper D. Gatekeeper C and Gatekeeper D both reply with positive responses (LCFs). Gatekeeper B will aggregate that information in its LCF back to Gatekeeper A.



Gatekeeper Signaling: Call Disconnect

Cisco.com

RAS Signaling Sequence

1 = Phone B hangs up
2 = GWB sends DRQ to GK2
3 = GWB sends H.225 Release Complete to GWA
4 = GWA sends DRQ to GKA
5 = GWA signals call disconnect to voice network

GWGK v1.0—5-21

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

Phones A and B are in two conversations. The following steps show the RAS signaling sequence:

Step 1 Phone B hangs up.

Step 2 Gateway B sends DRQ to Gatekeeper 2, disconnecting the call between Phones A and B. A DCF is received some time later.

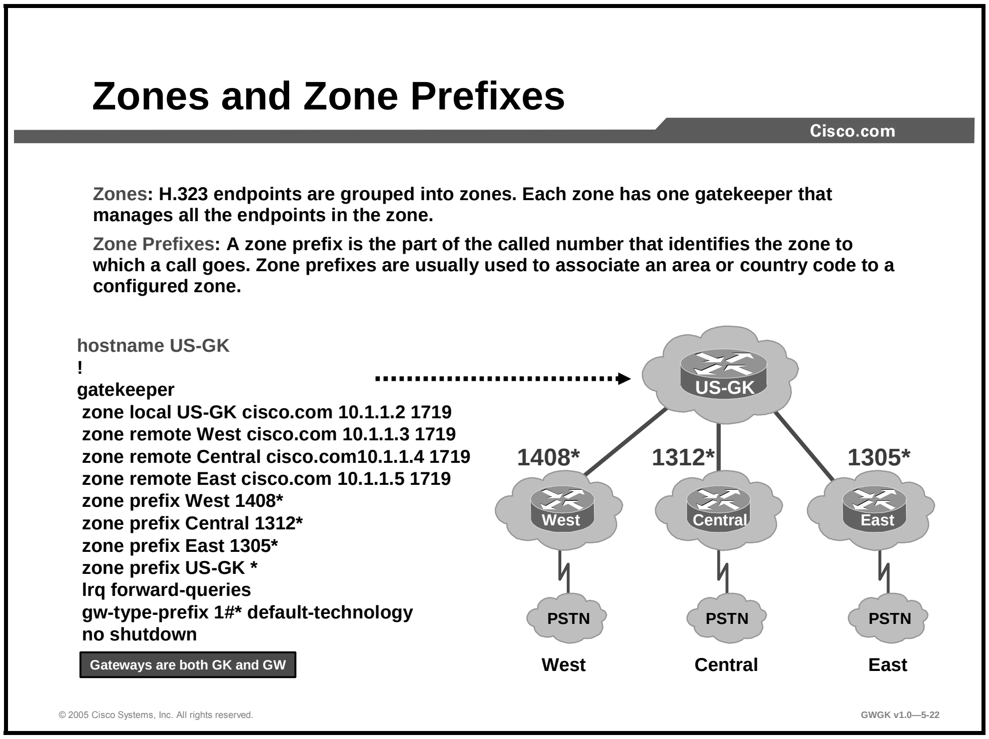
Step 3 Gateway B sends a Q.931 release complete to Gateway A.

Step 4 Gateway A sends DRQ to Gatekeeper 1, disconnecting the call between Phones A and B. A DCF is received some time later.

Step 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.)

Zones and Zone Prefixes

This topic describes zones and zone prefixes.



Zones and Zone Prefixes

Cisco.com

Zones: H.323 endpoints are grouped into zones. Each zone has one 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.

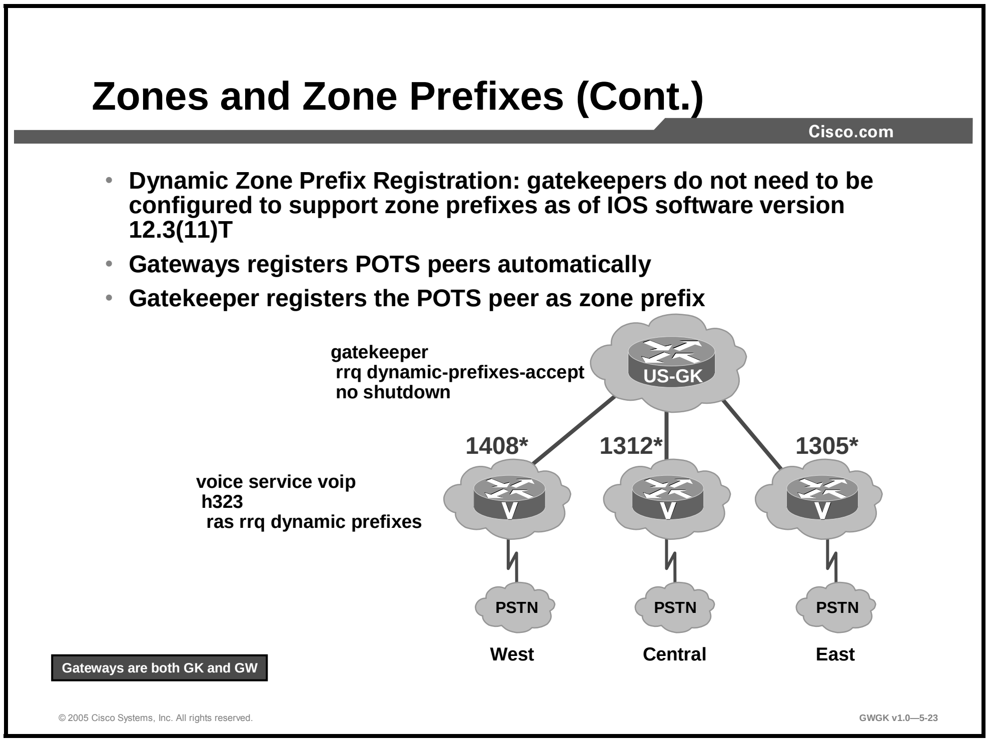
```
hostname US-GK
!
gatekeeper
 zone local US-GK cisco.com 10.1.1.2 1719
 zone remote West cisco.com 10.1.1.3 1719
 zone remote Central cisco.com10.1.1.4 1719
 zone remote East cisco.com 10.1.1.5 1719
 zone prefix West 1408*
 zone prefix Central 1312*
 zone prefix East 1305*
 zone prefix US-GK *
 lrq forward-queries
 gw-type-prefix 1#* default-technology
 no shutdown
```

Gateways are both GK and GW

GWGK v1.0—5-22

A gatekeeper zone is a collection of endpoints for routing calls. This zone can include H.323 clients, CallManager clusters, or H.323 gateways. This figure shows three regional zones that are managed by one gatekeeper. The gatekeeper US-Gatekeeper manages three major zones: West, Central, and East.

A zone prefix is a string of numbers that are used to associate a gateway to a dialed number in a zone. In this figure, US-Gatekeeper supports the 1408, 1312, and 1305 zone prefixes. The gateways in each zone use the technology prefix associated with the local area codes to register with US-Gatekeeper. This allows US-Gatekeeper to route the calls for a specific area code to the correct zone and gateway.



Zones and Zone Prefixes (Cont.)

Cisco.com

- Dynamic Zone Prefix Registration: gatekeepers do not need to be configured to support zone prefixes as of IOS software version 12.3(11)T
- Gateways registers POTS peers automatically
- Gatekeeper registers the POTS peer as zone prefix

```
gatekeeper
 rrq dynamic-prefixes-accept
 no shutdown
```

```
voice service voip
 h323
  ras rrq dynamic prefixes
```

Gateways are both GK and GW

GWGK v1.0—5-23

The H.323v4 Gateway Zone Prefix Registration Enhancements feature provides support for two capabilities included in H.323 version 4: Additive registration and dynamic zone prefix registration. Additive registration allows a gateway to add to or modify a list of aliases contained in a previous registration without first unregistering from the gatekeeper. Dynamic zone prefix registration allows a gateway to register actual PSTN destinations served by the gateway with its gatekeeper.

The benefit of using the dynamic zone registration process is that you do not have to enter the zone prefix on the gatekeepers that control the gateways. If you configure all of your gatekeepers to accept dynamic registration from their supported gateways, you will not have to enter the zone prefix number on the gatekeeper.

H.323v4 allows a gateway to register actual zone prefixes that it can terminate to the PSTN with a gatekeeper. A gateway can register multiple zone prefixes with the gatekeeper via the RRQ message, and it can subsequently remove one or more zone prefixes by using a URQ RAS message that indicates the specific prefixes to be removed. When the gatekeeper receives the URQ, it leaves the gateway registered and removes the specified zone prefixes.

To enable the H.323v4 Gateway Zone Prefix Registration Enhancements feature, the gateway and the gatekeeper need to be configured. Once these services are enabled on a trunking gateway and gatekeeper, all addresses specified by the destination patterns in the POTS dial peers that are operational in the gateway are advertised to the gatekeeper.

The “Gatekeeper Configuration Commands” and the “Gateway Configuration Commands” tables show the commands for configuring zones and zone prefixes on gatekeepers and gateways and the descriptions of the commands.

In the gatekeeper, add these commands to the configuration:

Gatekeeper Configuration Commands

Command	Description
US-GK(config)# gatekeeper	This enters gatekeeper configuration mode
US-GK(config-gk)#rrq dynamic-prefixes-accept	This allows US-Gatekeeper to receive the RRQ RAS messages from the gateway
US-GK(config-gk)#exit	This exits gatekeeper configuration mode

In the gateway, add these commands to the configuration:

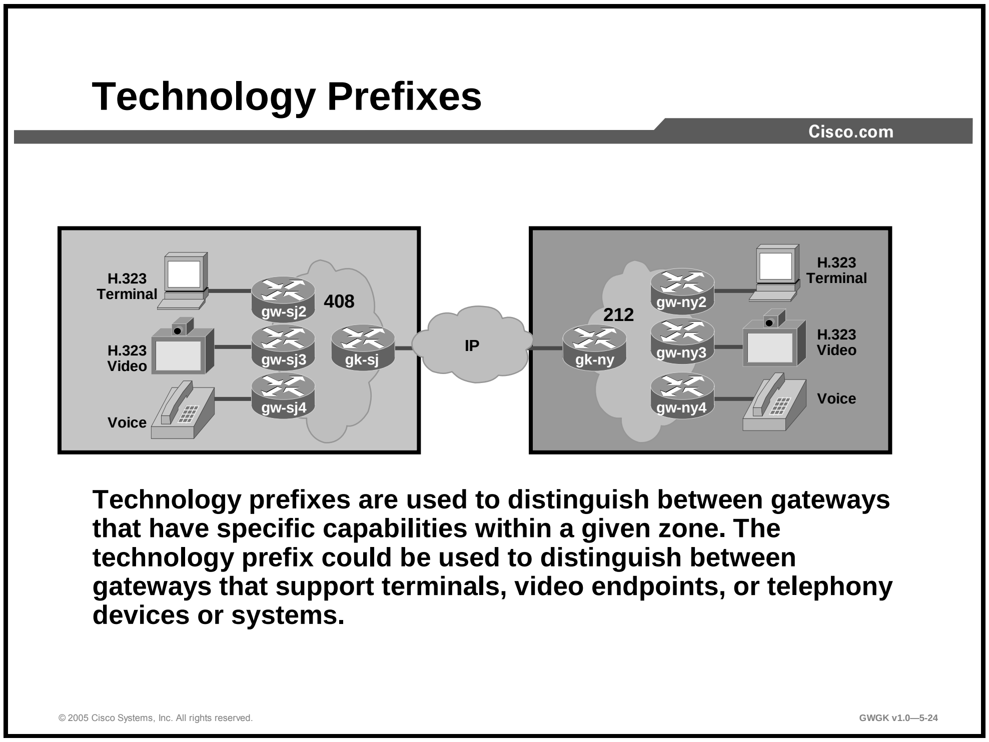
Gateway Configuration Commands

Command	Description
West(config)#voice service voip	This enters voice service configuration mode
West(config-voice-serv)#h323	This enters the H.323 voice service configuration mode
West(conf-serv-h323)# ras rrq dynamic prefixes	This enables the gateway to send and advertisement of dynamic prefixes in additive RRQ RAS messages
West(conf-serv-h323)#exit	This exits H.323 voice service configuration mode

The gatekeeper treats these addresses similarly to configured zone prefixes. The dynamically registered zone prefixes are used in routing decisions just as if they had been entered using the **zone prefix** command. Dynamically registered zone prefixes have a default gateway priority of 5.

Technology Prefixes

This topic describes technology prefixes.



Technology Prefixes

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

GWGK v1.0—5-24

A technology prefix is an optional H.323 standards-based feature that is supported by Cisco gateways and gatekeepers that enable more flexibility in call routing within an H.323 VoIP network. For example, technology prefixes may be 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.

A gateway registers to a gatekeeper with a technology prefix. For example, the gateway sends the technology prefix information contained in the RRQ message to the gatekeeper. While placing a call, the gateway prefixes the technology-prefix number to the E.164 number in the ARQ. The gatekeeper receives the number and checks for the technology prefix in its own configuration. If there is no match, the gatekeeper checks the zone prefix and tries to route the call.

The remaining string is compared against the configured zone prefixes. If the address resolves to a remote zone, the entire address, including both technology prefix and zone prefixes, is sent to the remote gatekeeper in an LRQ.

A terminating gatekeeper resolves an address by first checking the called number (DNIS) for a technology prefix. If there is a technology prefix, it strips the technology prefix off the called number and then evaluates the called number for zone prefixes.

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

Here is a call flow example using the technology prefix concept:

When a call is presented to Gatekeeper San Jose (gk-sj) with the following target address in San Jose, 2#2125551212, Gatekeeper San Jose recognizes that 2# is a technology prefix. Gatekeeper San Jose was not configured for technology prefix, but because Gateway San Jose 2 (gw-sj2) registered with it, the gatekeeper now treats 2# as a technology prefix. Gatekeeper San Jose strips the technology prefix, which leaves the telephone number 2125551212. This number is matched against the zone prefixes that have been configured. Gatekeeper San Jose has a match for 212......., and knows that Gatekeeper New York (gk-ny) handles this call. Gatekeeper San Jose forwards the entire address 2#2125551212 over to Gatekeeper New York, which also looks at the technology prefix 2# and routes it to Gateway New York 2.

For the San Jose gatekeeper, the configuration commands are as follows:

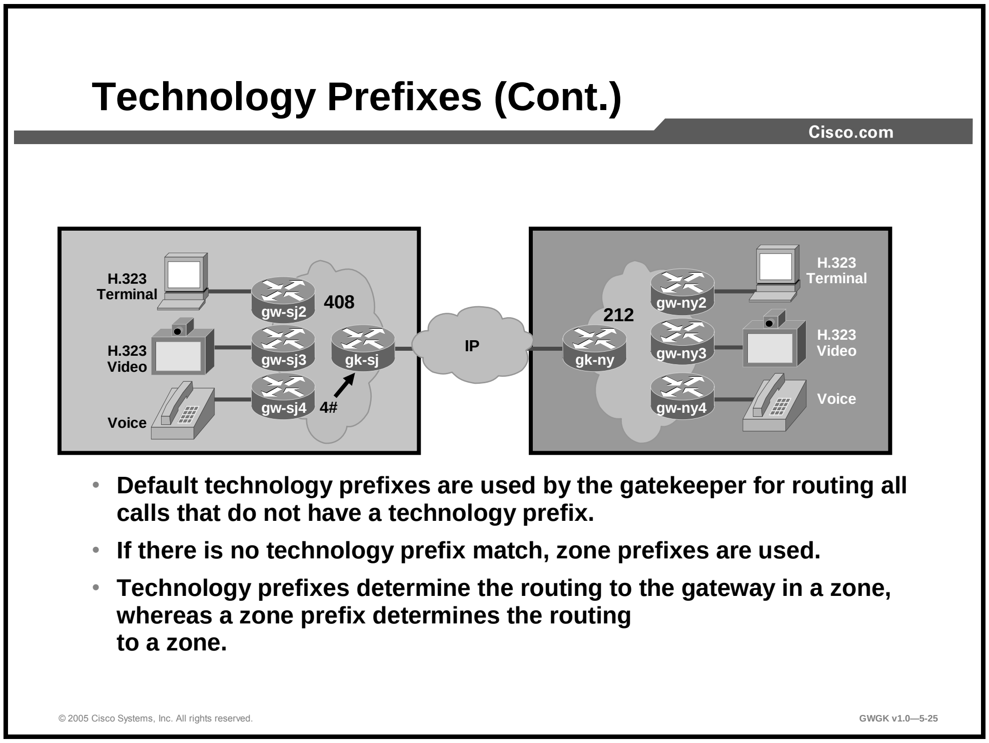
```
gatekeeper
 zone local gk-sj cisco.com
 zone remote gk-ny cisco.com 172.21.127.27
 zone prefix gk-sj 408.......
 zone prefix gk-ny 212.......
 gw-type-prefix 3# hopoff gk-sj2
 gw-type-prefix 4# default-technology
```

For the New York gatekeeper, the configuration commands are as follows:

```
gatekeeper
 zone local gk-ny cisco.com
 zone remote gk-sj cisco.com 172.21.1.48
 zone prefix gk-sj 408.......
 zone prefix gk-ny 212.......
 gw-type-prefix 3# hopoff gk-ny2
 gw-type-prefix 4# default-technology
```

Cisco gatekeepers use technology 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 only register their H.323 ID (unless they have FXS ports configured). Without E.164 addresses registered, the Cisco gatekeeper relies on two options to make the call routing decision:

- With the technology prefix matches option, the Cisco gatekeeper uses the technology prefix appended in the called number to select the destination gateway or zone.
- With the 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 technology prefix of the gateways.



Technology Prefixes (Cont.)

Cisco.com

- Default technology prefixes are used by the gatekeeper for routing all calls that do not have a technology prefix.
- If there is no technology prefix match, zone prefixes are used.
- Technology prefixes determine the routing to the gateway in a zone, whereas a zone prefix determines the routing to a zone.

GWGK v1.0—5-25

Using the same figure as before, here is an example of the use of default technology prefix at work:

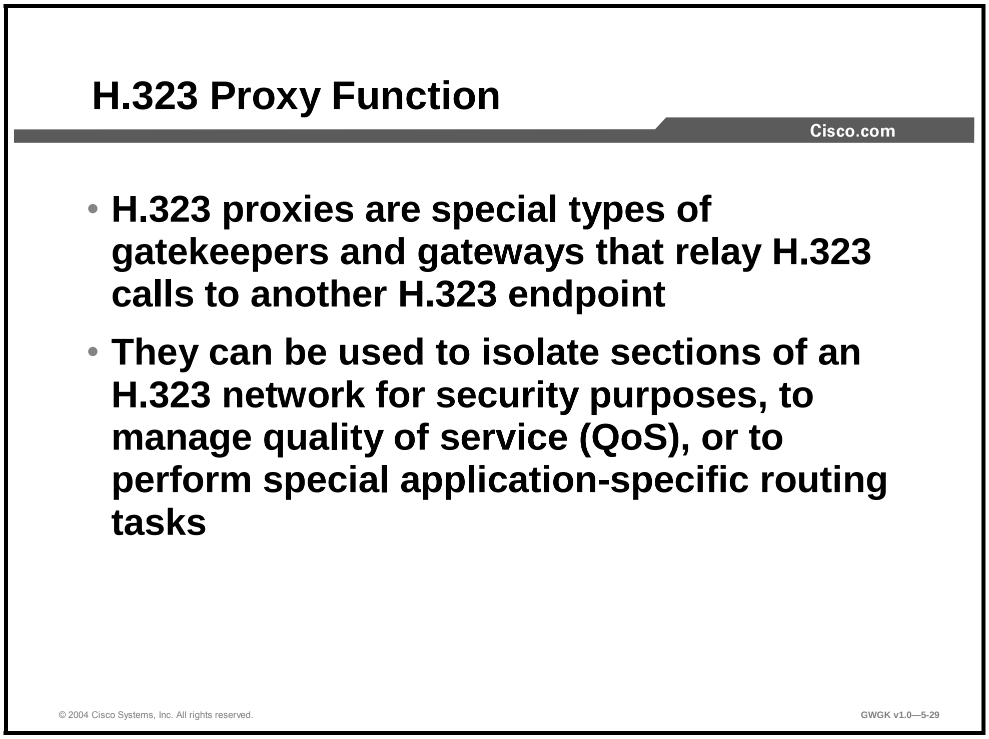
Gatekeeper San Jose receives a call 2125551212 from one its gateways. Gatekeeper San Jose checks this number against known technology prefixes but finds no match. It then checks it against zone prefixes and finds a match on 212....... and routes the call to Gatekeeper New York. Gatekeeper New York does not have any local registrations for this address, and there is no technology prefix on the address. However, the default prefix is 4#, and Gateway New York 4 is registered with 4#, so the call gets routed to Gateway New York 4.

Here is the configuration for the New York gatekeeper using default technology prefix:

```
gatekeeper
 zone local gk-ny cisco.com
 zone remote gk-sj cisco.com 172.21.1.48
 zone prefix gk-sj 408.......
 zone prefix gk-ny 212.......
 gw-type-prefix 3# hopoff gw-ny2
 gw-type-prefix 4# default-technology
```

H.323 Proxy Functions

This topic describes the function of a gatekeeper proxy and the signaling flows associated with it.



H.323 Proxy Function

Cisco.com

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

© 2004 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—5-29

Gatekeeper proxy signaling is typically used for three purposes:

- **Security:** When terminals signal each other directly, they must have direct access to the addresses of each other. This exposes key information about a network. When a proxy is used, the only addressing information that is exposed to the network is the address of the proxy; all other terminal and gateway addresses are hidden.
- **Quality of Service:** Adequate QoS usually requires terminals that are capable of signaling such premium services. There are two major ways to achieve such signaling:
  - — Resource Reservation Protocol (RSVP) to reserve flows that have adequate QoS based on the media codecs of H.323 traffic
  - — IP precedence bits to signal that the H.323 traffic is special and that it deserves higher priority

  Unfortunately, the vast majority of H.323 terminals cannot achieve signaling in either of these ways.

  The proxy can be configured to use any combination of RSVP and IP precedence bits. However, the proxy is not capable of modifying the QoS between the terminal and itself. To achieve the best overall QoS, ensure that terminals are connected to the proxy using a network that intrinsically has good QoS. In other words, configure a path between a terminal and proxy that provides good bandwidth, delay, and packet-loss characteristics without the terminal needing to request special QoS. A high-bandwidth LAN works well for this configuration.

- **Application-Specific Routing (ASR):** To achieve adequate QoS, a network may be deployed that is separate from the standard data network. The proxy can take advantage of such a partitioned network using a feature known as ASR.

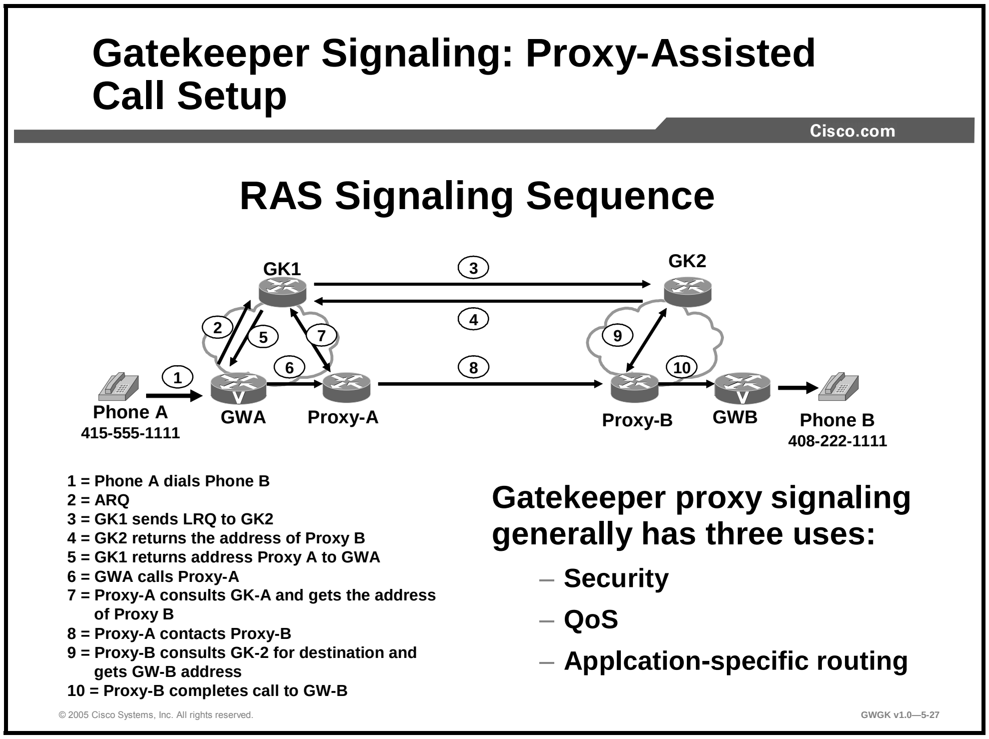
  ASR is simple. When the proxy receives outbound traffic, it directs traffic to an interface that is connected directly to the QoS network. The proxy does not send the traffic through an interface that is specified for the regular routing protocol. Similarly, inbound traffic from other proxies is received on the interface that is connected to the QoS network. This is true if all these other proxies around the QoS network use ASR in a consistent fashion. ASR then ensures that ordinary traffic is not routed into the QoS network by mistake.

Implementation of ASR ensures the following:

- Each time a connection is established with another proxy, the proxy automatically installs a host route pointing at the interface designated for ASR.
- The proxy is configured to use a loopback interface address. The proxy address is visible to both the ASR interface and all regular interfaces, but there are no routes established between the loopback interface and the ASR interface. This configuration ensures that only H.323 traffic is routed through the ASR interface.

Proxy Gateway Configuration Example

```
proxy h323
!
interface Loopback0
 ip address 10.0.0.1 255.0.0.0
 h323 interface
 h323 qos ip-precedence 4
 h323 h323-id px1@zone1.com
 h323 gatekeeper ipaddr 172.20.0.3
```



Gatekeeper Signaling: Proxy-Assisted Call Setup

Cisco.com

RAS Signaling Sequence

1 = Phone A dials Phone B
2 = ARQ
3 = GK1 sends LRQ to GK2
4 = GK2 returns the address of Proxy B
5 = GK1 returns address Proxy A to GWA
6 = GWA calls Proxy-A
7 = Proxy-A consults GK-A and gets the address of Proxy B
8 = Proxy-A contacts Proxy-B
9 = Proxy-B consults GK-2 for destination and gets GW-B address
10 = Proxy-B completes call to GW-B

Gatekeeper proxy signaling generally has three uses:

- **Security**
- **QoS**
- **Applcation-specific routing**

GWGK v1.0—5-27

This figure shows basic signaling sequencing between gateways and how a proxy gateway communicates with gateways and gatekeepers. You can see in this figure how Proxy A is directly communicating with Proxy B and how the actual gateways never see the IP addresses of the other gateways. The proxy gateways are hiding Gateway A and Gateway B from each other. The following steps show how to set up proxy signaling:

Step 1 Phone A dials phone B.

Step 2 Gateway A sends ARQ to Gatekeeper 1.

Step 3 Gatekeeper 1 sends LRQ to Gatekeeper 2.

Step 4 Gatekeeper 2 returns the address of Proxy B, hiding the identity of Gateway B.

Step 5 Gatekeeper 1 knows to get to Proxy B, it must go through Proxy A, so Gatekeeper 1 returns the address of Proxy A to Gateway A.

Step 6 Gateway A calls Proxy A.

Step 7 Proxy A consults Gatekeeper 1 to find the true destination, Gatekeeper 1 tells it to call Proxy B.

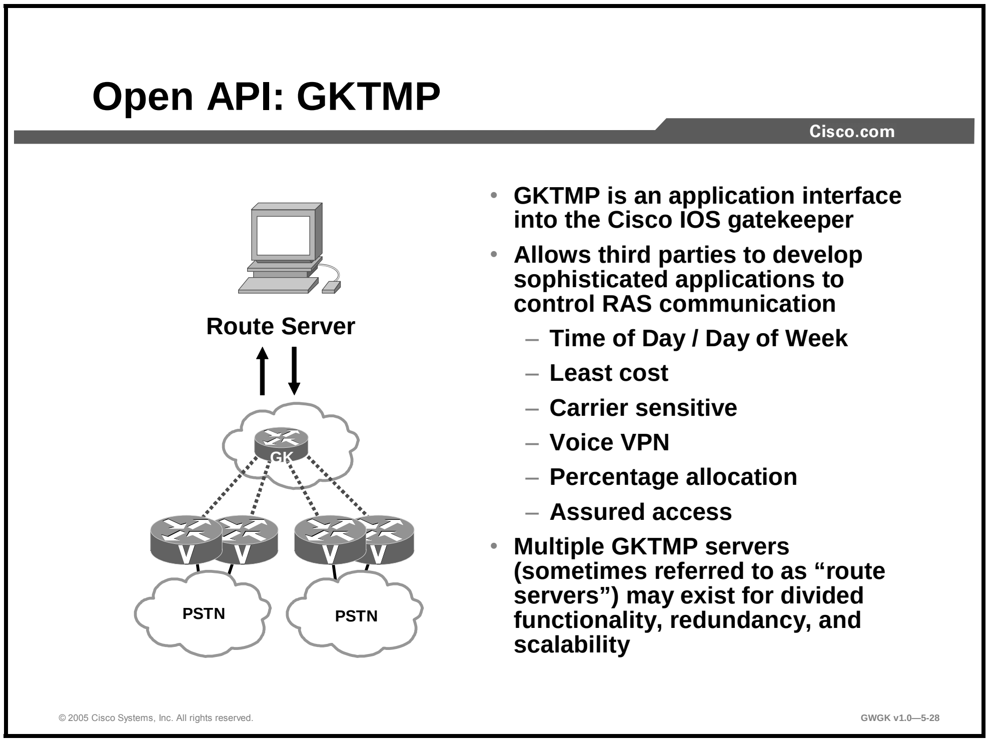
Step 8 Proxy A calls Proxy B.

Step 9 Proxy B consults Gatekeeper 2 for the true destination, which is Gateway B; Gatekeeper 2 provides the address of Gateway B to Proxy B.

Step 10 Proxy B completes the call to Gateway B.

Gatekeeper Transaction Message Protocol

This topic describes the Gatekeeper Transaction Message Protocol (GKTMP).



Route Server
GK
V
V
V
V
PSTN
PSTN

Open API: GKTMP

Cisco.com

- GKTMP is an application interface into the Cisco IOS gatekeeper
- Allows third parties to develop sophisticated applications to control RAS communication
  - Time of Day / Day of Week
  - Least cost
  - Carrier sensitive
  - Voice VPN
  - Percentage allocation
  - Assured access
- Multiple GKTMP servers (sometimes referred to as “route servers”) may exist for divided functionality, redundancy, and scalability

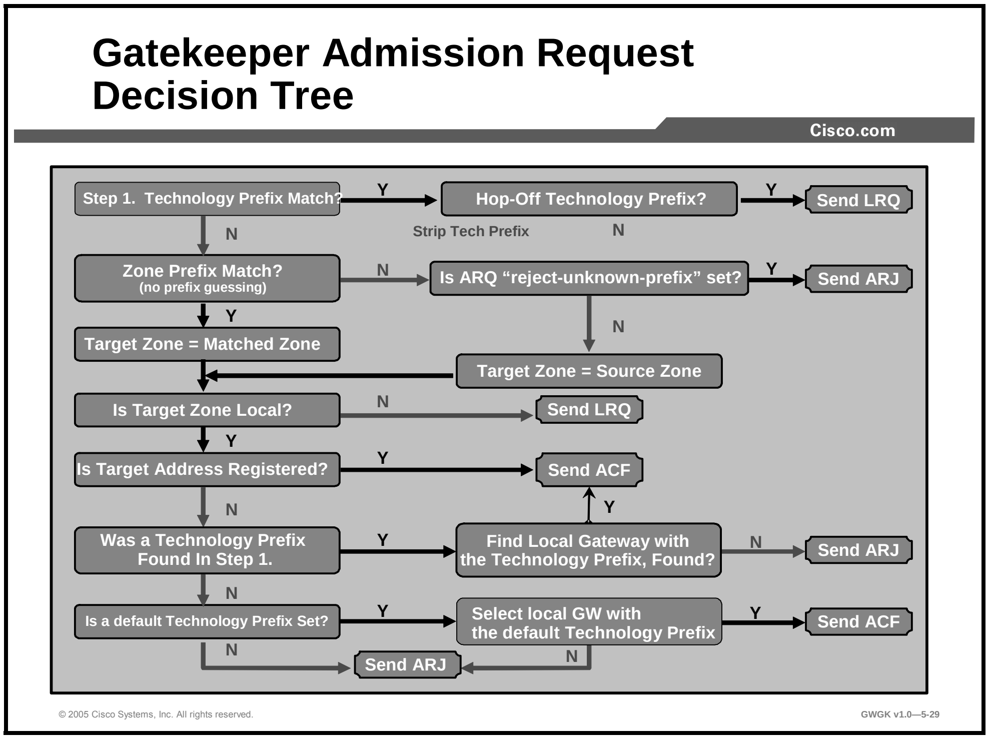
© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—5-28

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.

GKTMP is an independent platform 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 Address Resolution Process

This topic describes the gatekeeper address resolution process for admission requests and location requests.



Gatekeeper Admission Request Decision Tree

Cisco.com

Step 1. Technology Prefix Match?
Y → Hop-Off Technology Prefix?
Y → Send LRQ
Strip Tech Prefix
N
N
Zone Prefix Match?
(no prefix guessing)
N → Is ARQ "reject-unknown-prefix" set?
Y → Send ARJ
N
Y
Target Zone = Matched Zone
Target Zone = Source Zone
Is Target Zone Local?
N → Send LRQ
Y
Is Target Address Registered?
Y → Send ACF
N
Was a Technology Prefix Found In Step 1.
Y → Find Local Gateway with the Technology Prefix, Found?
Y
N → Send ARJ
N
Is a default Technology Prefix Set?
Y → Select local GW with the default Technology Prefix
Y → Send ACF
N
N
Send ARJ

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—5-29

When a gatekeeper receives an ARQ message from a gateway, it performs the following procedure:

- If there is a technology prefix specified in the admission request and it is a hop-off technology prefix, the gatekeeper sends an LRQ message.
- If there is no technology prefix or the technology prefix is not a hop off technology prefix, the gatekeeper uses the exact E.164 alias in the ARQ message, including the zone prefix, if any, to search its E.164 alias table:
  - — 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 a 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 technology prefix or the default technology prefix, the gatekeeper sends an ACF. If no local gateway with the specified technology prefix is found, the gatekeeper sends an ARJ message.

If there is no matching technology prefix and no default technology prefix is set, the gatekeeper sends an ARJ message.

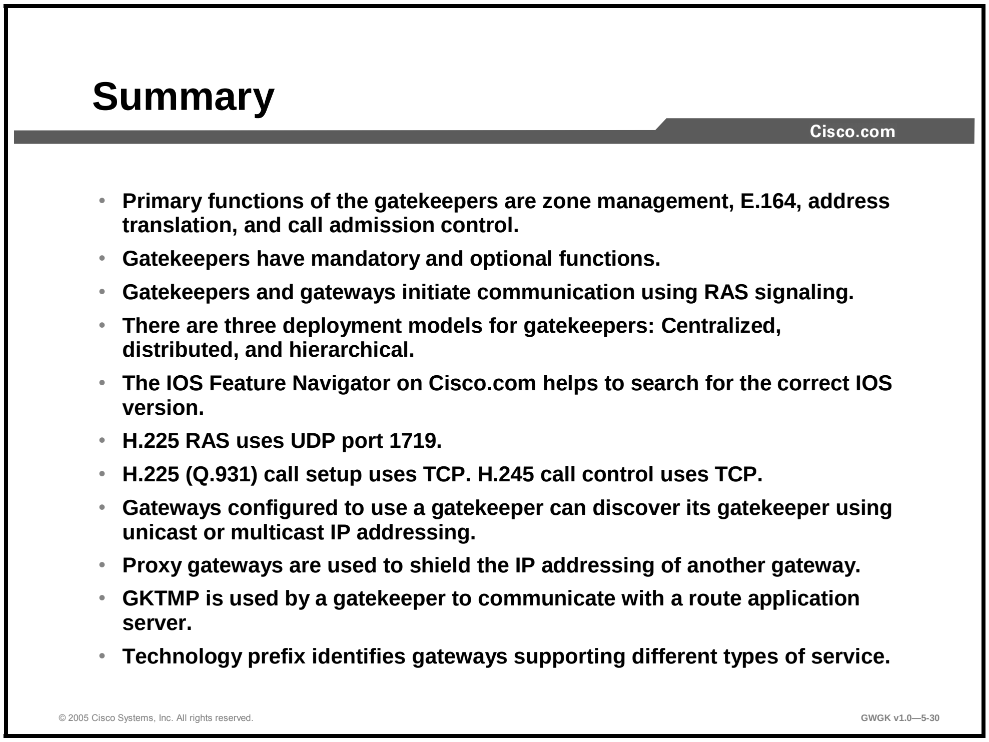
When a gatekeeper receives an LRQ message from a gateway, it performs either of the following procedures:

- If there is a hop off technology 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 technology prefix or the technology 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.
  - 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 technology prefix, the gatekeeper sends an LCF message. If no local gateway with the specified technology 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 technology prefix, and no default technology prefix is set, the gatekeeper sends an LRJ message.

Summary

This topic summarizes the key points discussed in this lesson.

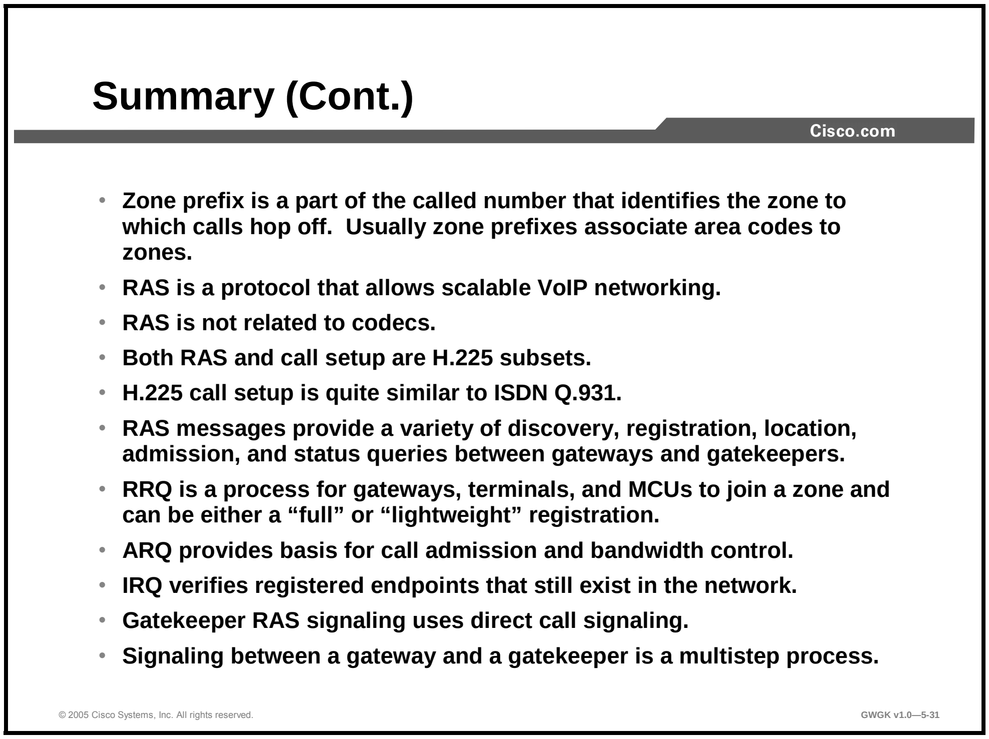


Summary

Cisco.com

- Primary functions of the gatekeepers are zone management, E.164, address translation, and call admission control.
- Gatekeepers have mandatory and optional functions.
- Gatekeepers and gateways initiate communication using RAS signaling.
- There are three deployment models for gatekeepers: Centralized, distributed, and hierarchical.
- The IOS Feature Navigator on Cisco.com helps to search for the correct IOS version.
- H.225 RAS uses UDP port 1719.
- H.225 (Q.931) call setup uses TCP. H.245 call control uses TCP.
- Gateways configured to use a gatekeeper can discover its gatekeeper using unicast or multicast IP addressing.
- Proxy gateways are used to shield the IP addressing of another gateway.
- GKTMP is used by a gatekeeper to communicate with a route application server.
- Technology prefix identifies gateways supporting different types of service.

GWGK v1.0—5-30

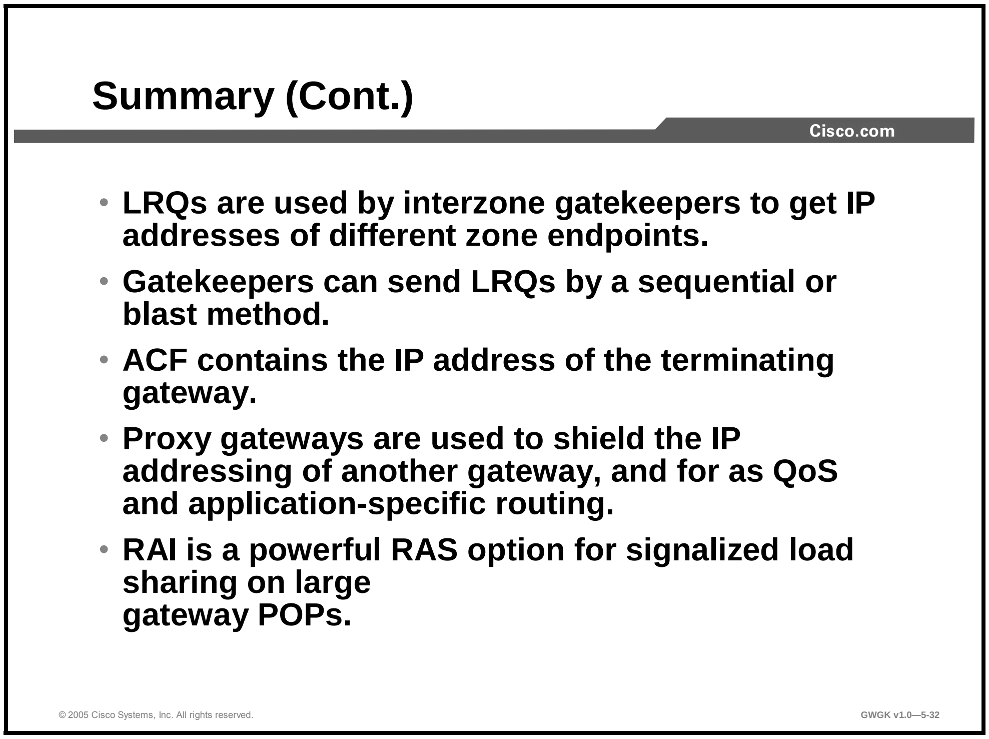


Summary (Cont.)

Cisco.com

- Zone prefix is a part of the called number that identifies the zone to which calls hop off. Usually zone prefixes associate area codes to zones.
- RAS is a protocol that allows scalable VoIP networking.
- RAS is not related to codecs.
- Both RAS and call setup are H.225 subsets.
- H.225 call setup is quite similar to ISDN Q.931.
- RAS messages provide a variety of discovery, registration, location, admission, and status queries between gateways and gatekeepers.
- RRQ is a process for gateways, terminals, and MCUs to join a zone and can be either a “full” or “lightweight” registration.
- ARQ provides basis for call admission and bandwidth control.
- IRQ verifies registered endpoints that still exist in the network.
- Gatekeeper RAS signaling uses direct call signaling.
- Signaling between a gateway and a gatekeeper is a multistep process.

GWGK v1.0—5-31



Summary (Cont.)

Cisco.com

- LRQs are used by interzone gatekeepers to get IP addresses of different zone endpoints.
- Gatekeepers can send LRQs by a sequential or blast method.
- ACF contains the IP address of the terminating gateway.
- Proxy gateways are used to shield the IP addressing of another gateway, and for as QoS and application-specific routing.
- RAI is a powerful RAS option for signalized load sharing on large gateway POPs.

GWGK v1.0—5-32

References

For additional information, refer to these resources:

Gatekeeper Alias Registration and Address Resolution Enhancements

- http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00800b5d3a.html

Understanding Gatekeepers:

- http://www.cisco.com/en/US/tech/tk652/tk701/technologies_tech_note09186a00800c5e0d.shtml#protosuite

Understanding Gatekeeper Call Routing

- http://www.cisco.com/warp/public/788/voip/gk-call-routing.pdf

Configuring Gatekeepers and Proxies

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/323confg/5gkconf.htm

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) What are four mandatory functions of a Cisco gatekeeper? (Source:)

A) call management, bandwidth management, call authorization, and call control signaling
B) address translation, zone management, bandwidth control, and admission control
C) call management, zone management, call control, and address translation
D) address translation, call control signaling, admission request, and call management

Q2) LRQs are RAS messages sent from which device? (Source:)

A) gateways to gatekeepers
B) gatekeepers to gateways
C) gatekeepers to gatekeepers
D) gatekeepers to registered endpoints

Q3) Location request confirmation messages are commonly used between interzone gatekeepers to obtain which element of the endpoint? (Source:)

A) mac address
B) directory number
C) IP address
D) UDP port numbers

Q4) H.245 call control messages are messages sent between which devices? (Source:)

A) gatekeeper to gateway
B) gateway to gateway
C) gateway to gatekeeper
D) All call control messages are managed by the gatekeeper.

Q5) RAS uses which kind of ports? (Source:)

A) TCP
B) UDP
C) Q.931
D) Q.921

Q6) Multicast discovery uses what multicast address? (Source:)

A) 240.22.40.1
B) 224.0.1.40
C) 224.0.1.41
D) 224.0.1.42

Q7) When a gateway first registers with a gatekeeper (first RRQ), that registration is considered to be which type of signaling? (Source: Gatekeeper Signaling)

A) **h323-gateway voip id**
B) lightweight registration
C) initial registration
D) full registration

Q8) ACF from a gatekeeper also contains which important reachable element of the endpoint? (Source:)

A) IP address
B) UDP port number set from lowest to highest
C) TCP port number set from lowest to highest
D) **h323-gateway voip interface**

Lesson Self-Check Answer Key

Q1)	A
Q2)	C
Q3)	C
Q4)	B
Q5)	B
Q6)	D
Q7)	D
Q8)	A

Lesson 2

Configuring Gatekeepers

Overview

In this lesson, you will learn how to configure gatekeepers and Cisco CallManager to operate together. You will also learn how the gatekeeper can be used to scale to large H.323 VoIP networks and how it is responsible for managing admission control and bandwidth for both voice and video calls.

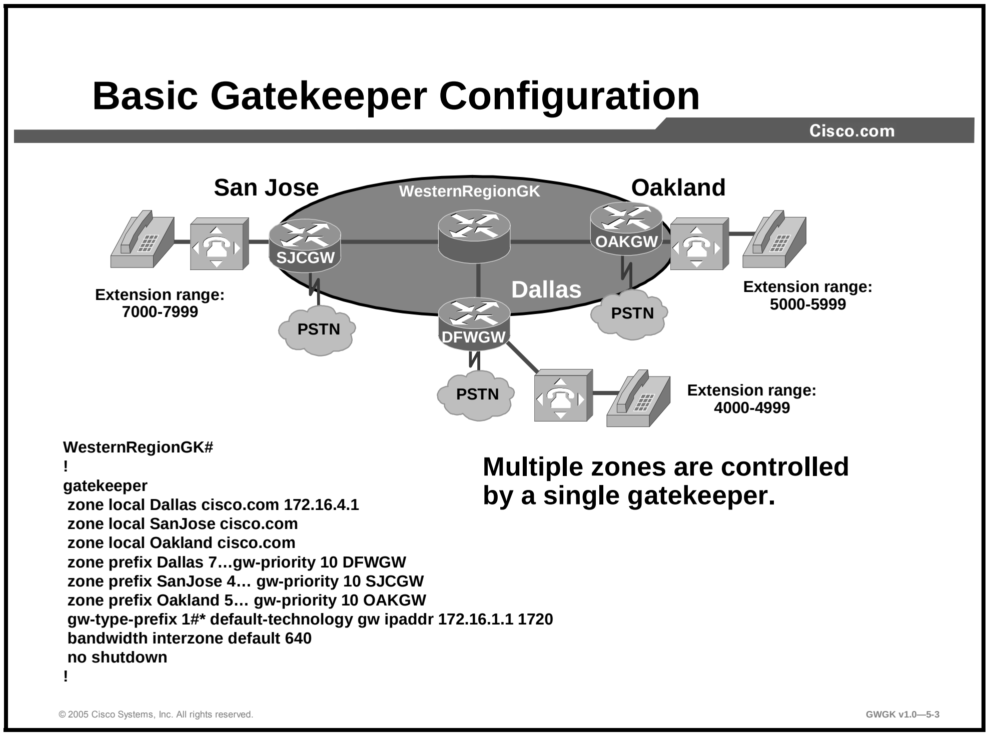
Objectives

Upon completing this lesson, you will be able to configure single and multiple zone gatekeepers to provide number resolution and CAC for H.323 gateways. This ability includes being able to meet these objectives:

- Define the initial steps in configuring gatekeepers
- Define the initial steps in configuring endpoints to register with a gatekeeper
- Configure a gatekeeper to support multiple zones
- Configure a gatekeeper to provide CAC by using bandwidth management
- Configure Cisco CallManager to use a gatekeeper for E.164 address resolution and CAC
- Learn to use troubleshooting tools to resolve gatekeeper issues

Basic Gatekeeper Configuration

This topic describes the initial configuration to activate a gatekeeper.

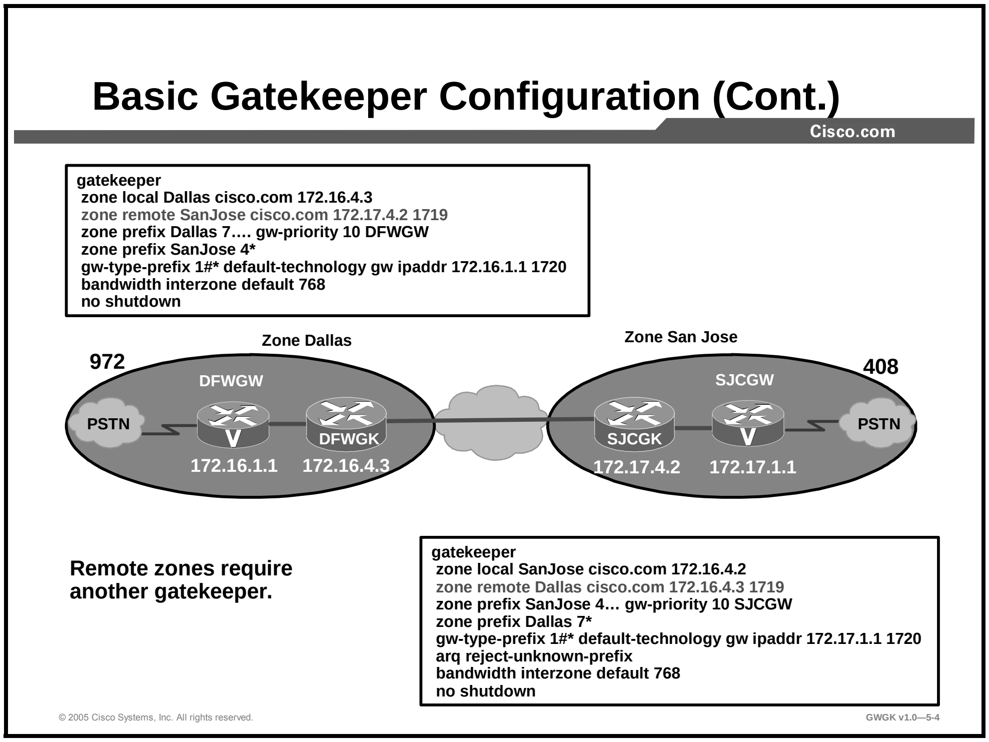


Basic Gatekeeper Configuration

```
WesternRegionGK#
!
gatekeeper
 zone local Dallas cisco.com 172.16.4.1
 zone local SanJose cisco.com
 zone local Oakland cisco.com
 zone prefix Dallas 7…gw-priority 10 DFWGW
 zone prefix SanJose 4… gw-priority 10 SJCGW
 zone prefix Oakland 5… gw-priority 10 OAKGW
 gw-type-prefix 1#* default-technology gw ipaddr 172.16.1.1 1720
 bandwidth interzone default 640
 no shutdown
!
```

Multiple zones are controlled by a single gatekeeper.

This figure shows a common topology where a gatekeeper, in this scenario Western Region Gatekeeper, manages multiple zones. There can be only one gatekeeper controlling a zone at any time. There are exceptions, however, where backup gatekeepers may be deployed. This topic is covered in the “Configuring Gatekeeper Redundancy” lesson of this module.



Basic Gatekeeper Configuration (Cont.)

```
gatekeeper
 zone local Dallas cisco.com 172.16.4.3
 zone remote SanJose cisco.com 172.17.4.2 1719
 zone prefix Dallas 7…. gw-priority 10 DFWGW
 zone prefix SanJose 4*
 gw-type-prefix 1#* default-technology gw ipaddr 172.16.1.1 1720
 bandwidth interzone default 768
 no shutdown
```

Remote zones require another gatekeeper.

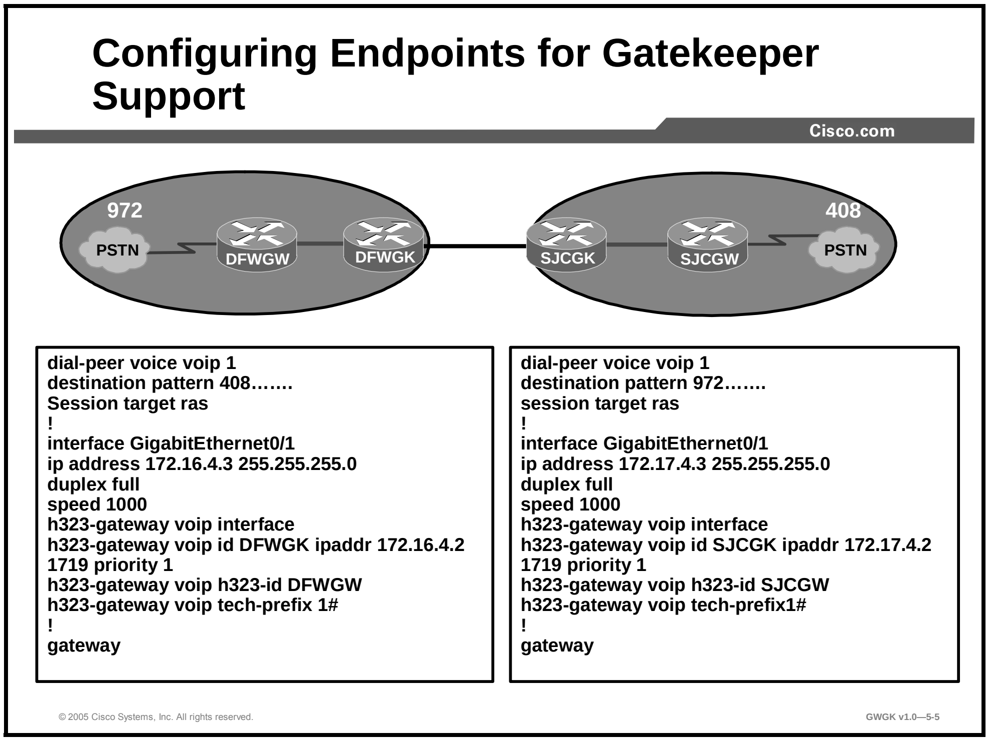
```
gatekeeper
 zone local SanJose cisco.com 172.16.4.2
 zone remote Dallas cisco.com 172.16.4.3 1719
 zone prefix SanJose 4… gw-priority 10 SJCGW
 zone prefix Dallas 7*
 gw-type-prefix 1#* default-technology gw ipaddr 172.17.1.1 1720
 arq reject-unknown-prefix
 bandwidth interzone default 768
 no shutdown
```

GWGK v1.0—5-4

This figure shows the basic steps in configuring gatekeepers managing local and remotes zones. This figure shows that gateways Dallas Gateway and San Jose Gateway communicate to two separate gatekeepers in different zones: The local Dallas zone and the local San Jose zone. If the gateway used one of the gatekeepers rather than the two separate ones, as seen in the previous figure, they would be registered to one gatekeeper and would support two zones.

Configuring Endpoints for Gatekeeper Support

This topic describes the gateway configuration that is required for the gateway to interoperate with a gatekeeper.



Configuring Endpoints for Gatekeeper Support

```
dial-peer voice voip 1
destination pattern 408…….
Session target ras
!
interface GigabitEthernet0/1
ip address 172.16.4.3 255.255.255.0
duplex full
speed 1000
h323-gateway voip interface
h323-gateway voip id DFWGK ipaddr 172.16.4.2
1719 priority 1
h323-gateway voip h323-id DFWGW
h323-gateway voip tech-prefix 1#
!
gateway
```

```
dial-peer voice voip 1
destination pattern 972…….
session target ras
!
interface GigabitEthernet0/1
ip address 172.17.4.3 255.255.255.0
duplex full
speed 1000
h323-gateway voip interface
h323-gateway voip id SJCGK ipaddr 172.17.4.2
1719 priority 1
h323-gateway voip h323-id SJCGW
h323-gateway voip tech-prefix1#
!
gateway
```

GWGK v1.0—5-5

This figure builds upon the figure with the Basic Gatekeeper Configuration figure. The dial peers in this figure are focused on the IP WAN and tail-end hop-off (TEHO), whereas, in the previous figure, they dial peers pointed to the PSTN.

The steps for configuring a H323 gateway to function with a gatekeeper are shown in the “H.323 Gateway Configuration Procedure” table:

H.323 Gateway Configuration Procedure

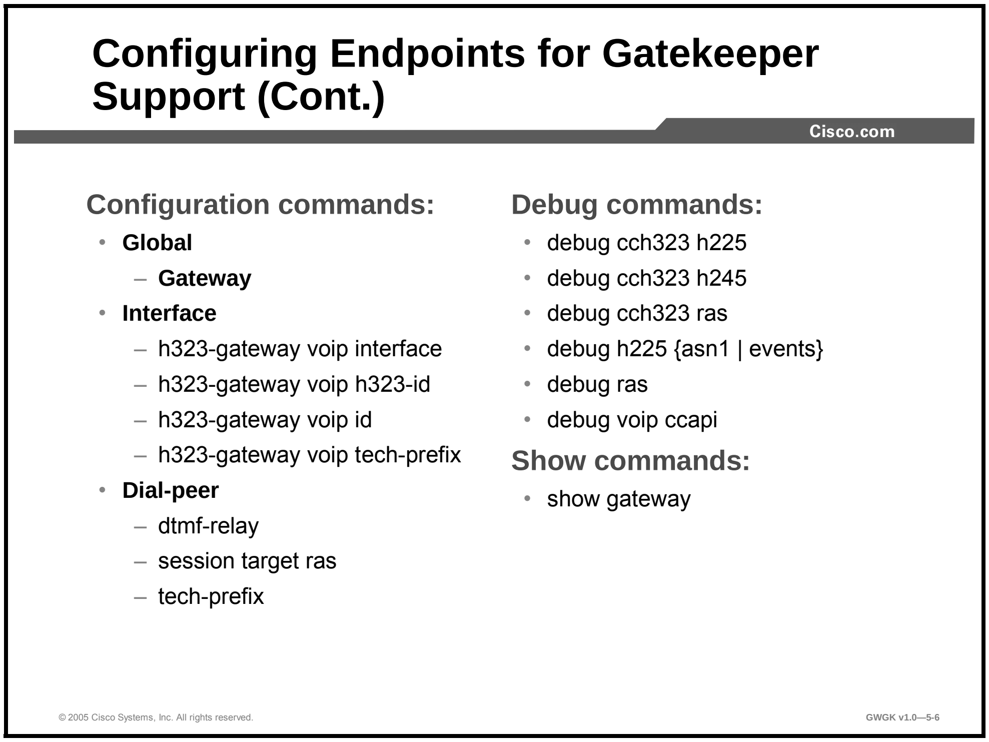
Step	Command	Purpose

1.	`gateway`
	Example:
	`Router(config)# gateway`
		Enters gateway configuration mode and enables the gateway to register with the gatekeeper

2.	`exit`
	Example:
	`Router(config-gateway)# exit`
		Exits the current mode

3.	`h323-gateway voip interface`
	Example:
	`Router(config-if)# h323-gateway voip interface`
		Identifies this as a VoIP gateway interface

Step	Command	Purpose
4.	**h323-gateway voip id** ***gatekeeper-id*** {**ipaddr** ***ip-address*** [***port***]| **multicast**} [**priority** ***priority***] Example: **Router(config-if)# h323-gateway voip id gk3.gg-dn1 ipaddr 172.18.0.0 1719**	(Optional) Defines the name and location of the gatekeeper for this gateway Keywords and arguments are as follows: ■ *gatekeeper-id*: H.323 identification of the gatekeeper. Must exactly match the gatekeeper ID in the gatekeeper configuration. Recommended format: name.domainname. ■ **ipaddr** *ip-address*: IP address to be used to identify the gatekeeper. ■ *port*: Port number used. ■ **multicast**: Gateway uses multicast to locate the gatekeeper. ■ **priority** *priority*: Priority of this gatekeeper. Range: 1 to 127. Default: 127.
5.	**h323-gateway voip h323-id** ***interface-id*** Example: **Router(config-if)# h323-gateway voip h323-id name@domainname**	(Optional) Defines the H.323 name of the gateway, identifying 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.
6.	**h323-gateway voip tech-prefix** ***prefix*** Example: **Router(config-if)# h323-gateway voip tech-prefix 2#**	(Optional) Defines the numbers used as the technology prefix that the gateway registers with the gatekeeper This command can contain up to 11 characters. Although not strictly necessary, a pound symbol (#) is frequently used as the last digit in a prefix. Valid characters: 0 to 9, #, and *.
7.	**h323-gateway voip bind srcaddr** ***ip-address*** Example: **Router(config-if)# h323-gateway voip bind srcaddr 192.168.0.0**	Sets the source IP address to be used for this gateway The argument is as follows: ■ *ip-address*: IP address to be used for outgoing H.323 traffic, which includes H.225, H.245, and RAS messages. Typically, this is the IP address assigned to the Ethernet interface.



Configuring Endpoints for Gatekeeper Support (Cont.)

Cisco.com

Configuration commands:

- **Global**
  - **Gateway**
- **Interface**
  - h323-gateway voip interface
  - h323-gateway voip h323-id
  - h323-gateway voip id
  - h323-gateway voip tech-prefix
- **Dial-peer**
  - dtmf-relay
  - session target ras
  - tech-prefix

Debug commands:

- debug cch323 h225
- debug cch323 h245
- debug cch323 ras
- debug h225 {asn1 | events}
- debug ras
- debug voip ccapi

Show commands:

- show gateway

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—5-6

This figure gives a summary the previous gateway H323 configuration.

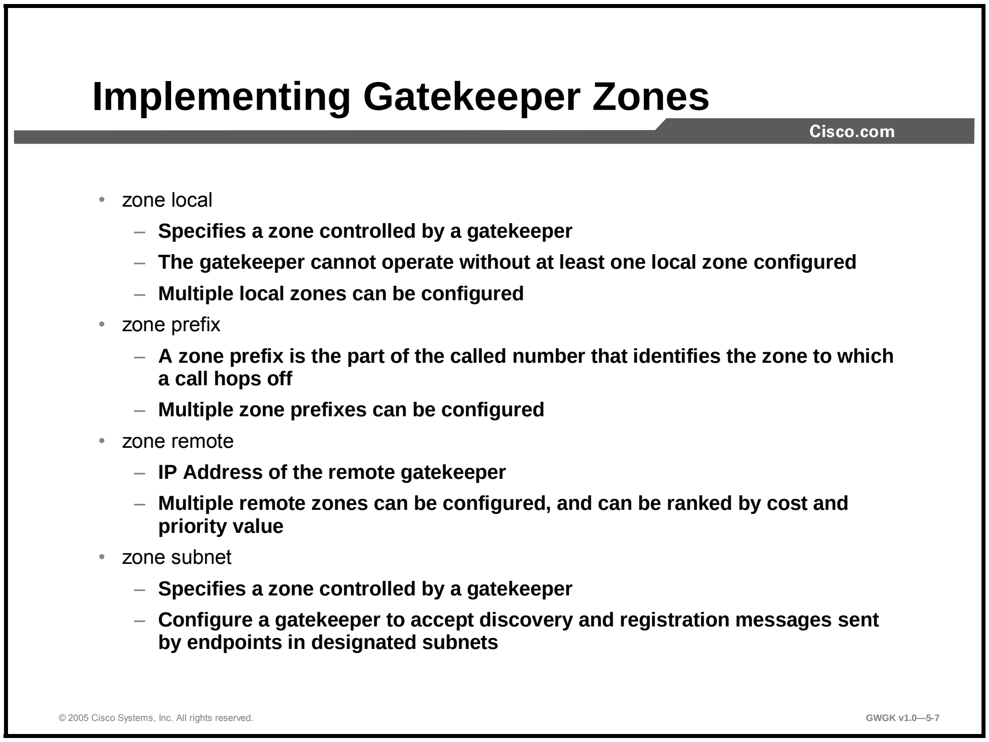
```
SJC-GK#show gateway
H.323 ITU-T Version: 4.0 H323 Stack Versions: 0.1

 H.323 service is up
 Gateway  SJC-GK  is registered to Gatekeeper SJC-GK

Alias list (CLI configured)
 H323-ID SJC-GK
 E164-ID 6001
 E164-ID 4155556001
 E164-ID 6002
 E164-ID 4155556002
Alias list (last RCF)
 H323-ID SJC-GK
 E164-ID 6001
 E164-ID 4155556001
 E164-ID 6002
 E164-ID 4155556002

 H323 resource thresholding is enabled and Active
 H323 resource threshold values:
  DSP: Low threshold 10, High threshold 70
```

```
DS0: Low threshold 10, High threshold 70

SJC-GK#show h323 gateway ras

RAS STATISTICS AT 1w2d

 RAS MESSAGE     REQUESTS SENT    CONFIRMS RCVD    REJECTS RCVD
 GK Discovery    grq         4    gcf         2    grj        0
 Registration    rrq     18063    rcf     18063    rrj        0
 Admission       arq        53    acf        46    arj        7
 Bandwidth       brq        16    bcf        16    brj        0
 Disengage       drq        46    dcf        46    drj        0
 Unregister      urq         0    ucf         0    urj        0
 Resource Avail  rai         1    rac         1
 Req In Progress rip         0


 RAS MESSAGE     REQUESTS RCVD    CONFIRMS SENT    REJECTS SENT
 GK Discovery    grq         0    gcf         0    grj        0
 Registration    rrq         0    rcf         0    rrj        0
 Admission       arq         0    acf         0    arj        0
 Bandwidth       brq         0    bcf         0    brj        0
 Disengage       drq         0    dcf         0    drj        0
 Unregister      urq         1    ucf         1    urj        0
 Resource Avail  rai         0    rac         0
 Req In Progress rip        37
```

Note Debug commands will be practiced in “Lab 5-1: Configuring Gatekeepers.”

Implementing Gatekeeper Zones

This topic describes how to configure zones on gatekeepers and gateways.



Implementing Gatekeeper Zones

Cisco.com

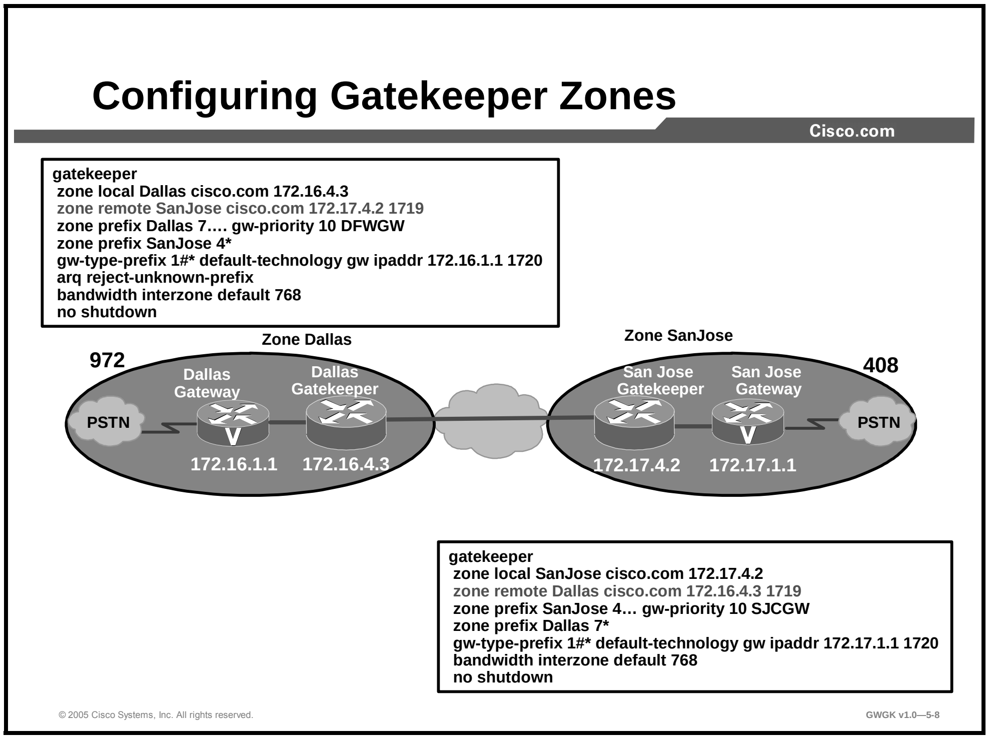
- zone local
  - **Specifies a zone controlled by a gatekeeper**
  - **The gatekeeper cannot operate without at least one local zone configured**
  - **Multiple local zones can be configured**
- zone prefix
  - **A zone prefix is the part of the called number that identifies the zone to which a call hops off**
  - **Multiple zone prefixes can be configured**
- zone remote
  - **IP Address of the remote gatekeeper**
  - **Multiple remote zones can be configured, and can be ranked by cost and priority value**
- zone subnet
  - **Specifies a zone controlled by a gatekeeper**
  - **Configure a gatekeeper to accept discovery and registration messages sent by endpoints in designated subnets**

GWGK v1.0—5-7

The following text defines **zones local**, **zone prefix**, **zone remote**, and **zone subnet** in greater detail.

- **Zone Local**
  - 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 may support more than one zone. Even though there is a single a gatekeeper per local zone, communications 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 RAS IP address. If you define this argument in the first zone definition, you can omit it for all subsequent zones, which 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. Once the argument is defined, you can change it by reissuing any **zone local** command with a different **ras**-*IP-address* argument.
  - If the **ras**-*IP-address* argument is a Hot Standby Router Protocol (HSRP) virtual address, it automatically puts the gatekeeper into HSRP mode. In this mode, the gatekeeper assumes standby or active status according to whether the HSRP interface is in standby or active status.
  - 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, which forces the endpoints, gateways, and the 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.
- **Zone Prefix**
  - A gatekeeper can handle more than one zone prefix, but a zone prefix cannot be shared by more than one gatekeeper. If you have defined a zone prefix as being handled by a gatekeeper and now define it as being handled by a second gatekeeper, the second assignment cancels the first.
- **Zone Remote**
  - Not all gatekeepers have to be in the Domain Name System (DNS). For those that are not, use the **zone remote** command so that the local gatekeeper knows how to access them. In addition, you may wish to improve call response time slightly for frequently accessed zones. If the **zone remote** command is configured for a particular zone, you do not need to make a DNS lookup transaction.
  - The maximum number of zones defined on a gatekeeper varies depending on the mode, the call model, or both. For example, a directory gatekeeper may be in the mode of being responsible for forwarding location request (LRQ) messages and may not be handling any local registrations and calls. The call model might be E.164 addressed calls instead of H.323-ID addressed calls.
  - For a directory gatekeeper that does not handle local registrations and calls, the maximum remote zones defined should not exceed 10,000. An additional 4 MB of memory is required to store this maximum number of remote zones.
  - For a gatekeeper that handles local registrations and only E.164 addressed calls, the number of remote zones defined should not exceed 2000.
  - For a gatekeeper that handles H.323-ID calls, the number of remote zones defined should not exceed 200.
  - When there are several remote zones configured, they can be ranked by cost and priority value. A zone with a lower cost value and a higher priority value is given preference over others.
- **Zone Subnet**
  - You can use the **zone subnet** command more than once to create a list of subnets controlled by a gatekeeper. The subnet masks do not have to match the actual subnets that use at your site. For example, to specify a particular endpoint, you can supply its address with a 32-bit netmask.



Configuring Gatekeeper Zones

Cisco.com

```
gatekeeper
 zone local Dallas cisco.com 172.16.4.3
 zone remote SanJose cisco.com 172.17.4.2 1719
 zone prefix Dallas 7…. gw-priority 10 DFWGW
 zone prefix SanJose 4*
 gw-type-prefix 1#* default-technology gw ipaddr 172.16.1.1 1720
 arq reject-unknown-prefix
 bandwidth interzone default 768
 no shutdown
```

```
gatekeeper
 zone local SanJose cisco.com 172.17.4.2
 zone remote Dallas cisco.com 172.16.4.3 1719
 zone prefix SanJose 4… gw-priority 10 SJCGW
 zone prefix Dallas 7*
 gw-type-prefix 1#* default-technology gw ipaddr 172.17.1.1 1720
 bandwidth interzone default 768
 no shutdown
```

GWGK v1.0—5-8

To enter gatekeeper configuration mode and to start the gatekeeper, use the following commands beginning in global configuration mode:

Gatekeeper Configuration Procedure

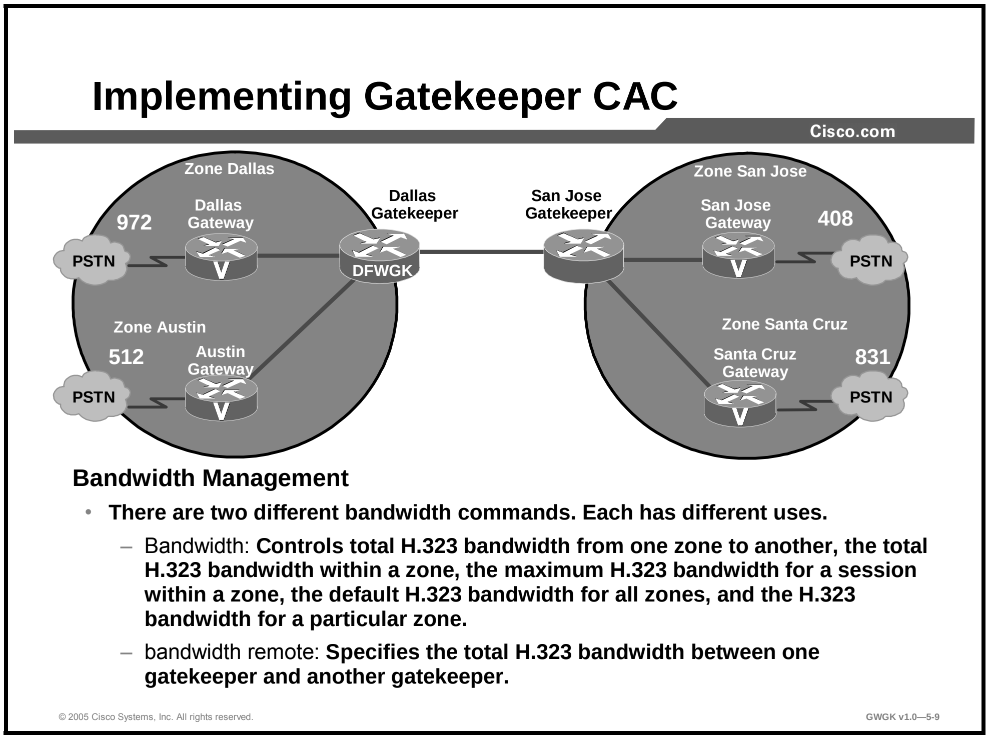
Step	Command	Purpose
1.	`Router(config)#` **`gatekeeper`**	Enters gatekeeper configuration mode
2.	`Router(config-gk)#` **`zone local`** *`gatekeeper-name domain-name`* `[`*`ras-IP-address`*`]`	Specifies a zone controlled by a gatekeeper The arguments are as follows: ■ *gatekeeper-name*: Specifies the gatekeeper name or zone name. This is usually the fully domain-qualified host name of the gatekeeper. For example, if the domain name is cisco.com, the gatekeeper name might be gk1.cisco.com. However, if the gatekeeper is controlling multiple zones, the gatekeeper name for each zone should be some unique string that has a mnemonic value. ■ *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. **Note:** Setting this address for one local zone makes it the address used for all local zones.

Step	Command	Purpose
3.	`Router(config-gk)#` **`zone prefix`** *`gatekeeper-name e164-prefix`* [**`blast`** | **`seq`**] [**`gw-priority`** *`priority gw-alias`* [*`gw-alias`*, ...]]	Adds a prefix to the gatekeeper zone list The keywords and arguments are as follows: ■ *gatekeeper-name*: Specifies the name of a local or remote gatekeeper, which must have been defined by using the **zone local** or **zone remote** command. ■ *e164-prefix*: Specifies an E.164 prefix in standard form followed by dots (.). Each dot represents a number in the E.164 address. For example, 212....... is matched by 212 and any 7 numbers. **Note:** Although the preferred configuration method is to use a dot to represent each digit in an E.164 address, you can also enter an asterisk (*) to match any number of digits. ■ blast: (Optional) If you list multiple hopoffs, 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, indicates that the LRQs should be sent sequentially to the gatekeepers based on the order in which they were listed. The default is seq. ■ **gw-priority** *priority gw-alias*: (Optional) Use the **gw-priority** option to define how the gatekeeper selects gateways in its local zone for calls to numbers that begin with prefix e164-prefix. Do not use this option to set priority levels for a prefix assigned to a remote gatekeeper. Use values from 0 to 10. A 0 value prevents the gatekeeper from using the gateway *gw-alias* for that prefix. Value 10 places the highest priority on gateway *gw-alias*. If you do not specify a priority value for a gateway, the value 5 is assigned. To assign the same priority value for one prefix to multiple gateways, list all the gateway names after the pri-0-to-10 value. The *gw-alias* name is the H.323 ID of a gateway that is registered or will register with the gatekeeper. This name is set on the gateway with the **h323-gateway voip h.323-id** command.

Step	Command	Purpose
4.	Router(config-gk)# **zone subnet** *local-gatekeeper-name* [**default** | *subnet-address* {**/***bits-in-mask* | *mask-address*} **enable**]	Defines a set of subnets that constitute the gatekeeper zone. Enables the gatekeeper for each of these subnets and disables it for all other subnets. (Repeat for all subnets.) The keywords and arguments are as follows: ■ *local-gatekeeper-name*: Specifies the name of the local gatekeeper. ■ **default**: (Optional) Applies to all other subnets that are not specifically defined by the **zone subnet** command. ■ *subnet-address*: (Optional) Specifies the address of the subnet that is being defined. ■ *bits-in-mask*: (Optional) Specifies the number of bits of the mask to be applied to the subnet address. **Note:** The slash must be entered before this argument. ■ *mask-address*: (Optional) Specifies the mask (in dotted string format) to be applied to the subnet address. ■ **enable**: (Optional) Specifies that the gatekeeper accepts discovery and registration from the specified subnets. **Note**: To define the zone as being all but one set of subnets by disabling that set and enabling all other subnets, use the **no** form of the command as follows: Configure **no zone subnet** *local-gatekeeper-name subnet-address* {**I***bits-in-mask* | *mask-address*} **enable**. **Note**: To accept the default behavior, which is that all subnets are enabled, use the **no** form of the command as follows: **no zone subnet** *local-gatekeeper-name* **default enable**.
5.	Router(config-gk)# **no shutdown**	Brings the gatekeeper online

Implementing Gatekeeper CAC

This topic describes how to implementing CAC on a gatekeeper.



Implementing Gatekeeper CAC

Bandwidth Management

- **There are two different bandwidth commands. Each has different uses.**
  - Bandwidth: **Controls total H.323 bandwidth from one zone to another, the total H.323 bandwidth within a zone, the maximum H.323 bandwidth for a session within a zone, the default H.323 bandwidth for all zones, and the H.323 bandwidth for a particular zone.**
  - bandwidth remote: **Specifies the total H.323 bandwidth between one gatekeeper and another gatekeeper.**

GWGK v1.0—5-9

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

To specify the maximum aggregate bandwidth for H.323 traffic and to verify the available bandwidth of the destination gatekeeper, use the **bandwidth** command in gatekeeper configuration mode. To disable maximum aggregate bandwidth, use the **no** form of this command.

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

no bandwidth {interzone | total | session} {default | zone
zone-name}
```

Each aspect of this example is described in the “Bandwidth Commands” table.

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
default	Default value for all zones
zone	A particular zone
zone-name	Name of the particular zone
bandwidth-size	Maximum bandwidth, in kbps For **interzone** and **total**, the range is from 1 to 10,000,000. For **session**, the range is from 1 to 5000.

Use the bandwidth remote command to specify the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper, use the **bandwidth remote** command in gatekeeper configuration mode. To disable total bandwidth specified, use the **no** form of this command.

Cisco IOS first supported the bandwidth commands for intra and inter zone bandwidth management in 12.1(3).

```
bandwidth remote bandwidth-size
no bandwidth remote
```

The bandwidth remote command is described in the “Bandwidth Remote Command” table.

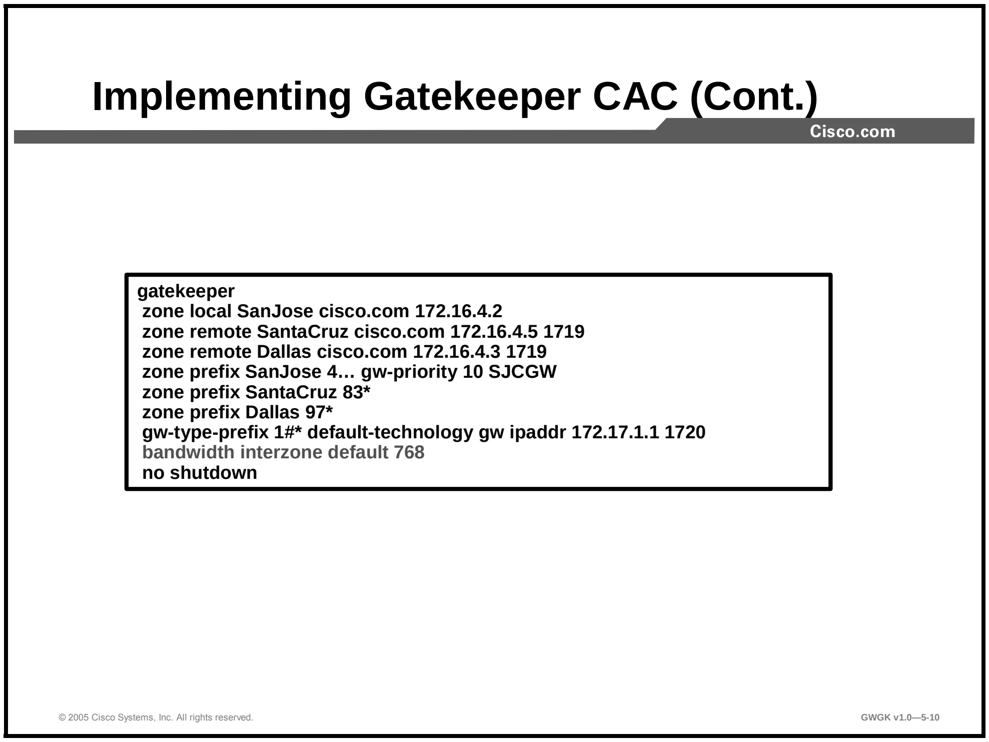
Bandwidth Remote Command

Command	Description
bandwidth-size	Maximum bandwidth, in kbps. Range is from 1 to 10,000,000.

Use the example in the figure to explore these two commands. If a call was being placed from the Austin zone to the Dallas zone you would use the **bandwidth interzone** command because this configures the H.323 bandwidth from one zone to another. We could use the **bandwidth zone** command if we wanted to set the H.323 bandwidth for a zone like Austin. We would use the bandwidth total command if we wanted to set the total H.323 bandwidth that would be allowed in a zone.

If you need to allocate the bandwidth between the Dallas gatekeeper and the San Jose gatekeeper, you would use the bandwidth **remote command**. There is a lot of flexibility in the ability to tune the bandwidth that is used both inside a zone (between zones) and between gatekeepers.

More information on gatekeeper bandwidth commands for Cisco IOS Software 12.3(T) can be found at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tvr/vrg_b1.htm#wp1503256.



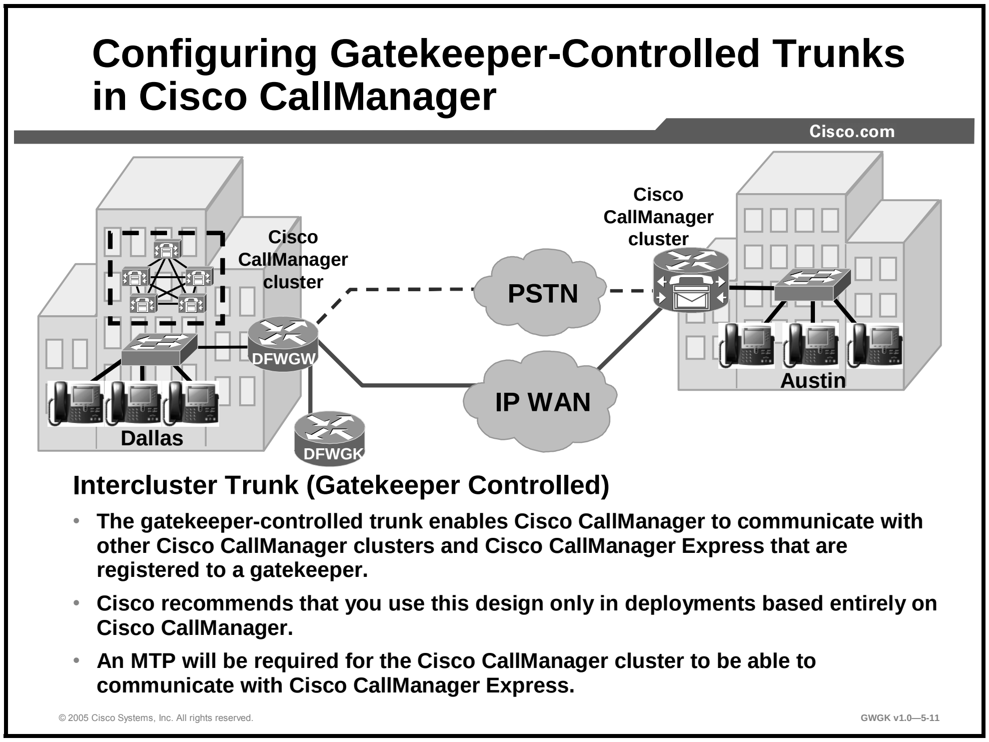
Implementing Gatekeeper CAC (Cont.)

```
gatekeeper
 zone local SanJose cisco.com 172.16.4.2
 zone remote SantaCruz cisco.com 172.16.4.5 1719
 zone remote Dallas cisco.com 172.16.4.3 1719
 zone prefix SanJose 4… gw-priority 10 SJCGW
 zone prefix SantaCruz 83*
 zone prefix Dallas 97*
 gw-type-prefix 1#* default-technology gw ipaddr 172.17.1.1 1720
 bandwidth interzone default 768
 no shutdown
```

The figure shows a sample of the configuration of the San Jose gatekeeper. There is one local zone, San Jose, and two remote zones, Santa Cruz and Dallas. Notice that the **bandwidth interzone** command has been highlighted. This command will allocate 768 kbps of bandwidth for H.323 traffic between two zones. Remember, the interzone option in the bandwidth command specifies the bandwidth from one zone to another. Because there are only two remote zones and the Dallas zone is across a gatekeeper-to-gatekeeper link, the bandwidth interzone command controls the bandwidth on the link between San Jose and Santa Cruz.

Configuring Gatekeeper-Controlled Trunks

This topic describes gatekeeper-controlled trunks in Cisco CallManager.



Configuring Gatekeeper-Controlled Trunks in Cisco CallManager

Intercluster Trunk (Gatekeeper Controlled)

- **The gatekeeper-controlled trunk enables Cisco CallManager to communicate with other Cisco CallManager clusters and Cisco CallManager Express that are registered to a gatekeeper.**
- **Cisco recommends that you use this design only in deployments based entirely on Cisco CallManager.**
- **An MTP will be required for the Cisco CallManager cluster to be able to communicate with Cisco CallManager Express.**

GWGK v1.0—5-11

The intercluster gatekeeper-controlled trunk enables Cisco CallManager to communicate with other Cisco CallManager clusters that are registered to an H.323 gatekeeper. Cisco recommends that you use the intercluster gatekeeper-controlled trunk only in deployments based entirely on Cisco CallManager.

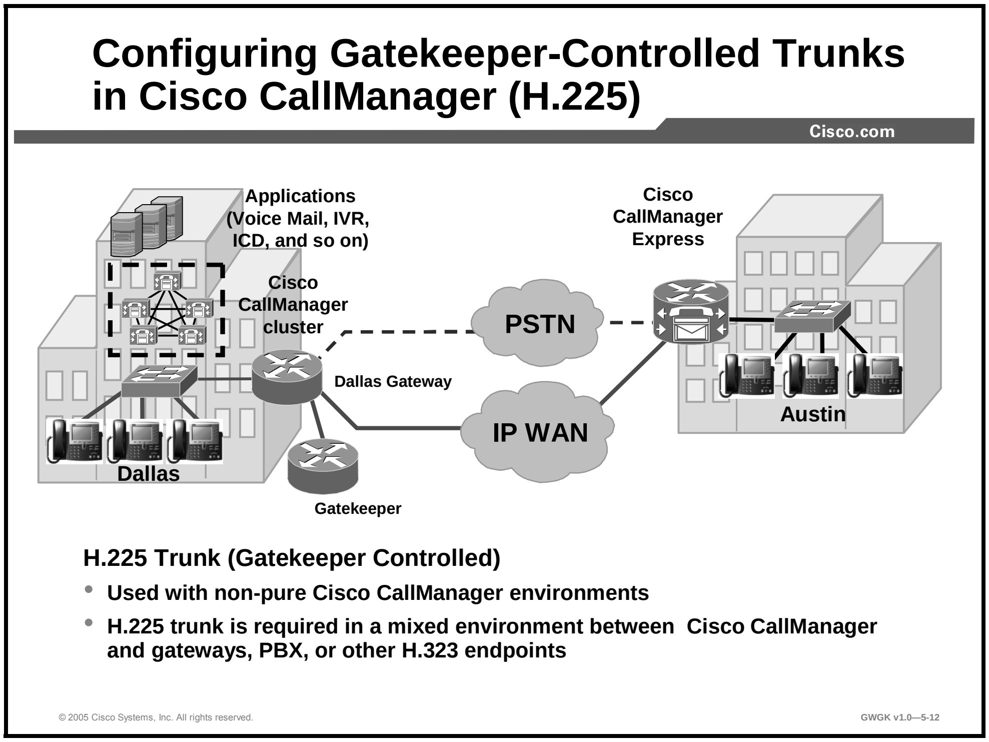
Follow these guidelines when using an intercluster gatekeeper-controlled trunk:

- Configure the gatekeeper the same way in each Cisco CallManager cluster.
- Configure the intercluster gatekeeper-controlled trunk in each Cisco CallManager cluster, matching the zone to the correct gatekeeper zone for the site.
- Configure a media termination point (MTP) is configured with it because the CallManager Express does initiate any Terminal Capabilities Set (TCS) signaling. The use of the MTP will prevent any TCS exchange between the Cisco CallManager and Cisco CallManager Express.
- Each Cisco CallManager subscriber listed in the Cisco CallManager redundancy group of the device pool registers an intercluster gatekeeper-controlled trunk with the gatekeeper (maximum of three).
- Calls are load-balanced across the registered trunks in the Cisco CallManager cluster.
- Cisco CallManager supports multiple gatekeepers and trunks.
- Configure a separate zone in the gatekeeper for each Cisco CallManager cluster.
- Use the **bandwidth interzone** command on the gatekeeper to control bandwidth between Cisco CallManager clusters and H.323 devices registered directly with the gatekeeper.
- A single Cisco IOS gatekeeper can support up to 100 Cisco CallManager clusters.

- You can provide gatekeeper redundancy by using gatekeeper clustering (alternate gatekeeper) or HSRP. Use HSRP only if gatekeeper clustering is not available in your software feature set.

The following are intercluster (gatekeeper-controlled) configuration considerations:

- The **zone local** commands create the gatekeeper zones. Each Cisco CallManager registers an intercluster gatekeeper-controlled trunk with its configured zone.
- The **zone prefix** is used to route calls between zones. You may define multiple zone prefixes for the same zone, if needed.
- The **bandwidth interzone** command allocates the amount of bandwidth that is available between zones.
- The **gw-type-prefix 1# default technology** command routes unresolved calls within a zone to the device with a registered technology prefix of 1#, which, in this example configuration, is the Cisco CallManager trunk.
- The **arq reject-unknown-prefix** command prevents call routing loops on redundant Cisco CallManager trunks.



Configuring Gatekeeper-Controlled Trunks in Cisco CallManager (H.225)

Cisco.com

H.225 Trunk (Gatekeeper Controlled)

- **Used with non-pure Cisco CallManager environments**
- **H.225 trunk is required in a mixed environment between Cisco CallManager and gateways, PBX, or other H.323 endpoints**

GWGK v1.0—5-12

The H.225 gatekeeper-controlled trunk enables Cisco CallManager to communicate with Cisco CallManager clusters and other H.323 devices registered to the H.323 gatekeeper. The H.225 gatekeeper-controlled trunk is not recommended in a pure Cisco CallManager environment, but it is required in a mixed environment with Cisco CallManager or other H.323 gateway. The trunk will require that an MTP is configured with it because the Cisco CallManager Express does not initiate any TCS signaling. The H.225 trunk attempts to discover the other H.323 device on a call-by-call basis. If it discovers a device that understands intercluster trunk protocol, it will automatically use that protocol. If it cannot discover the other device, Cisco CallManager will use the standard H.225 protocol.

Follow these guidelines when using an H.225 gatekeeper-controlled trunk for call admission control:

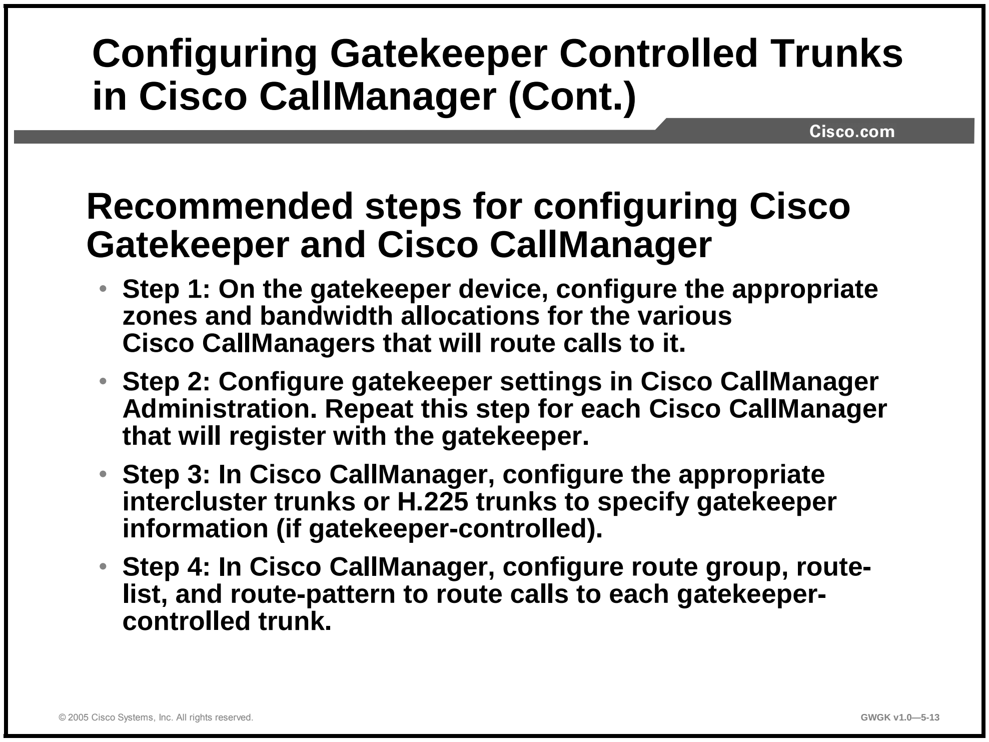
- Configure the gatekeeper the same way in each Cisco CallManager cluster.
- Configure the H.225 gatekeeper-controlled trunk in the Cisco CallManager cluster, matching the zone to the correct gatekeeper zone for the site.
- Each Cisco CallManager subscriber listed in the CallManager redundancy group of the device pool registers an H.225 gatekeeper-controlled trunk with the gatekeeper (maximum of three) .
- Calls are load-balanced across the registered trunks in the Cisco CallManager cluster.
- Cisco CallManager supports multiple gatekeepers and trunks.
- Configure a separate zone in the gatekeeper for each site supporting Cisco CallManagers, Cisco CallManager Express, or voice gateways.
- Use the **bandwidth interzone** command on the gatekeeper to control bandwidth between Cisco CallManager clusters, Cisco CallManager Express servers, and H.323 devices registered directly with the gatekeeper.

- Use the **bandwidth remote** command if there are multiple gatekeepers to control bandwidth between Cisco CallManager clusters, Cisco CallManager Express servers, and H.323 devices registered directly with the gatekeeper.
- A single Cisco IOS gatekeeper can support up to 100 zones or sites.
- You can provide gatekeeper redundancy by using gatekeeper clustering (alternate gatekeeper) or HSRP. Use HSRP only if gatekeeper clustering is not available in your software feature set.

The following are H.225 trunk (gatekeeper-controlled) configuration considerations:

- The **zone local** commands create the gatekeeper zones. Each Cisco CallManager registers an intercluster gatekeeper-controlled trunk with its configured zone.
- The **zone prefix** is used to route calls between zones.
- The **bandwidth interzone** command allocates the amount of bandwidth available between zones.
- The **gw-type-prefix 1# default technology** command routes unresolved calls within a zone to the device with a registered technology prefix of 1#, which, in this example configuration, is the Cisco CallManager trunk.
- The **arq reject-unknown-prefix** command prevents call routing loops on redundant Cisco CallManager trunks.

The Cisco CallManager gatekeeper and trunk configuration is relativity the same for intercluster trunk configuration. The only expectation is that with gatekeeper-controlled intercluster trunking ,you are trunking with another Cisco CallManager cluster. Whereas with H.225 gatekeeper control, you are configuring trunking with a device other than Cisco CallManager.



Configuring Gatekeeper Controlled Trunks in Cisco CallManager (Cont.)

Cisco.com

Recommended steps for configuring Cisco Gatekeeper and Cisco CallManager

- Step 1: On the gatekeeper device, configure the appropriate zones and bandwidth allocations for the various Cisco CallManagers that will route calls to it.
- Step 2: Configure gatekeeper settings in Cisco CallManager Administration. Repeat this step for each Cisco CallManager that will register with the gatekeeper.
- Step 3: In Cisco CallManager, configure the appropriate intercluster trunks or H.225 trunks to specify gatekeeper information (if gatekeeper-controlled).
- Step 4: In Cisco CallManager, configure route group, route-list, and route-pattern to route calls to each gatekeeper-controlled trunk.

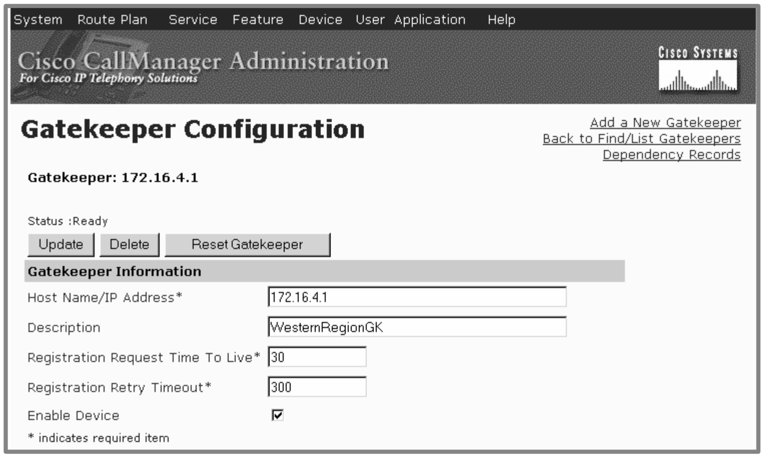
GWGK v1.0—5-13

Before you begin configuring Cisco CallManager to interoperate with a gatekeeper, familiarize yourself with the steps required to correctly configure Cisco CallManager and the gatekeeper.

Information about configuring an anonymous device gatekeeper with Cisco CallManager can be found at http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_configuration_example09186a0080169445.shtml.

Configuring Gatekeeper-Controlled Trunks in Cisco CallManager (Cont.)

Cisco.com



Gatekeeper Configuration

Gatekeeper: 172.16.4.1

Status :Ready

Gatekeeper Information

Host Name/IP Address*	172.16.4.1
Description	WesternRegionGK
Registration Request Time To Live*	30
Registration Retry Timeout*	300
Enable Device	☑

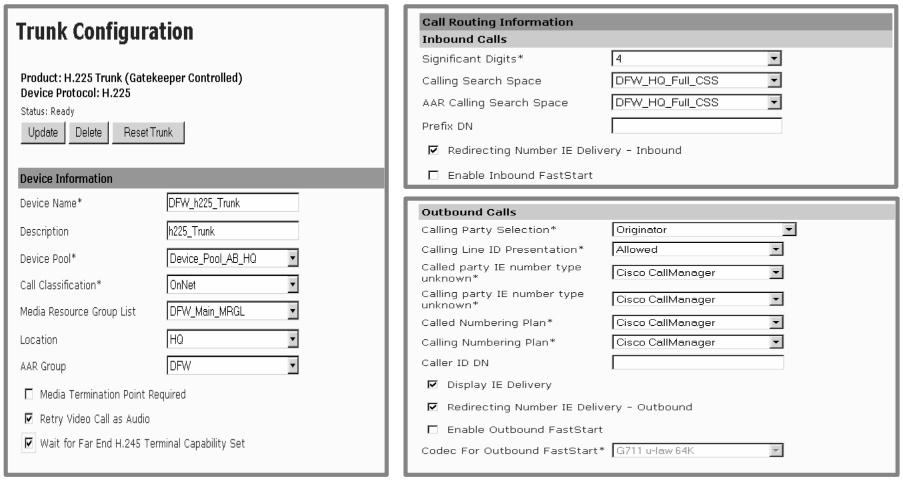
* indicates required item

GWGK v1.0—5-14

Configuring Gatekeeper-Controlled Trunks in Cisco CallManager (Cont.)

Cisco.com

H.225 Gatekeeper-Controlled Trunk



Trunk Configuration

Product: H.225 Trunk (Gatekeeper Controlled)
Device Protocol: H.225
Status: Ready

Device Information

Device Name*	DFW_h225_Trunk
Description	h225_Trunk
Device Pool*	Device_Pool_AB_HQ
Call Classification*	OnNet
Media Resource Group List	DFW_Main_MRGL
Location	HQ
AAR Group	DFW

☐ Media Termination Point Required
☑ Retry Video Call as Audio
☑ Wait for Far End H.245 Terminal Capability Set

Call Routing Information

Inbound Calls

Significant Digits*	4
Calling Search Space	DFW_HQ_Full_CSS
AAR Calling Search Space	DFW_HQ_Full_CSS
Prefix DN	

☑ Redirecting Number IE Delivery - Inbound
☐ Enable Inbound FastStart

Outbound Calls

Calling Party Selection*	Originator
Calling Line ID Presentation*	Allowed
Called party IE number type unknown*	Cisco CallManager
Calling party IE number type unknown*	Cisco CallManager
Called Numbering Plan*	Cisco CallManager
Calling Numbering Plan*	Cisco CallManager
Caller ID DN	

☑ Display IE Delivery
☑ Redirecting Number IE Delivery - Outbound
☐ Enable Outbound FastStart

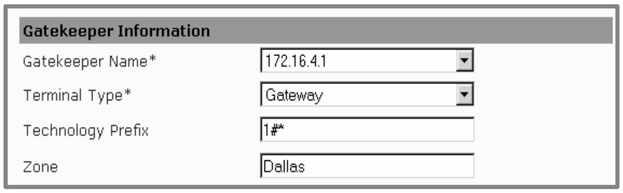
Codec For Outbound FastStart*	G711 u-law 64K

GWGK v1.0—5-15

This figure shows the Cisco CallManager H.225 trunk configuration page for the Dallas (DFW) Cisco CallManager cluster. The trunk device name is what the gatekeeper used as it registered as the H.323-ID. The remaining configuration in this figure is specific to the incoming and outgoing setup for calls to and from the cluster.

Configuring Gatekeeper-Controlled Trunks in Cisco CallManager (Cont.)

Cisco.com



Gatekeeper Information

Gatekeeper Name* 172.16.4.1

Terminal Type* Gateway

Technology Prefix 1#*

Zone Dallas

GWGK v1.0—5-16

After you have configured the H.225 gatekeeper-controlled trunk and selected the appropriate gatekeeper IP address, terminal type, technology prefix, and zone that the Cisco CallManager will register in, reset the gatekeeper. Wait a couple of minutes, then, enter **show gatekeeper endpoints** on the gatekeeper. You should notice that the gatekeeper has registered the H.225 trunk name as the H.323-ID and placed a _1 at the end of the name. The _1 is placed at the end of the H.323-ID as an identifier because there maybe multiple subscribers registered under the same cluster. The following show output shows how the gatekeeper places a tag at the end of the trunks registered from the Cisco CallManager cluster.

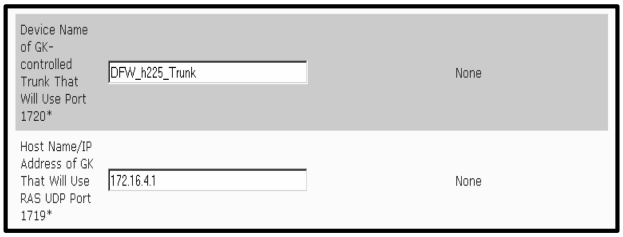
```
WesternRegionGK#show gatekeeper endpoint

                    GATEKEEPER ENDPOINT REGISTRATION

                    ================================

CallSignalAddr  Port  RASSignalAddr   Port  Zone Name
Type    Flags

--------------- ----- --------------- ----- ---------
----    -----

172.16.1.1      1720  172.16.1.1      1719  Dallas
VOIP-GW

    H323-ID: DFW_h225_Trunk_1

    Voice Capacity Max.=  Avail.=  Current.= 0

172.16.1.2      1720  172.16.1.2      1719  Dallas
VOIP-GW

    H323-ID: DFW_h225_Trunk_2

    Voice Capacity Max.=  Avail.=  Current.= 0
```

DFW_h225_Trunk_2 is a subscriber. Anymore subscribers in the cluster that is registering with the gatekeeper would receive _3, _4, and so on. If the publisher was to fail, the other trunks would remain registered to the gatekeeper and process calls.

Configuring Gatekeeper-Controlled Trunks in Cisco CallManager (Cont.)

Cisco.com

System Parameters



Device Name of GK-controlled Trunk That Will Use Port 1720*	DFW_h225_Trunk	None
Host Name/IP Address of GK That Will Use RAS UDP Port 1719*	172.16.4.1	None

New in Cisco CallManager v4.1(2)

GWGK v1.0—5-17

This figure shows the required system parameters cluster configuration that is needed for the Cisco CallManager Cluster 4.1(2) to integrate with a gatekeeper.

The following are the parameter definitions. This configuration is required.

- **Device name of gatekeeper-controlled trunk that will use port 1720:** This parameter specifies the device name of the gatekeeper-controlled H.225 or intercluster trunk that will use port 1720 for H.225 signaling. The device name should match exactly the device name of the trunk as specified in Cisco CallManager Administration. When an intercluster gatekeeper-controlled trunk is designated to use port 1720 via this parameter, a nongatekeeper-controlled trunk should not be configured between the same two Cisco CallManager servers; doing so will result in unpredictable call behavior.

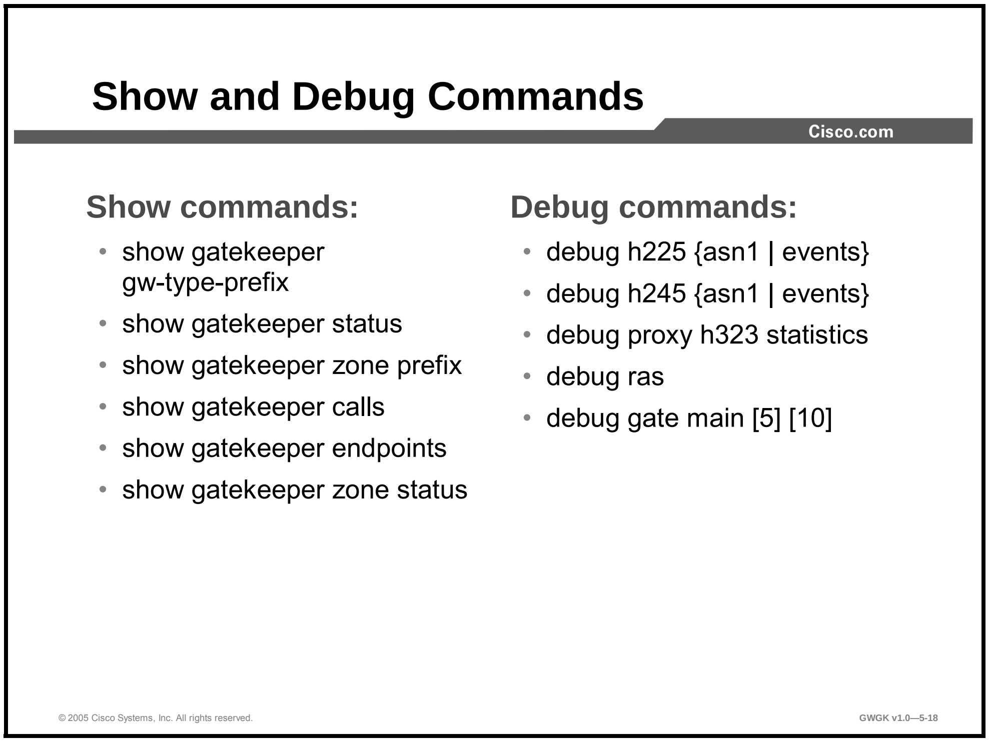
Note You must reset the corresponding gatekeeper-controlled H.225 intercluster trunk for the parameter change to take effect. This is a required field. Set the default to None and the maximum length to 50. Reset the corresponding gatekeeper-controlled H225 intercluster trunk for the parameter change to take effect.

- **Host name or IP address of gatekeeper that will use RAS UDP port 1719:** This parameter specifies the host name or IP address of the gatekeeper for which Cisco CallManager will use UDP port 1719 to receive RAS messages from that gatekeeper. The Host Name/IP Address should match the Host Name/IP Address that is specified in the Gatekeeper Configuration window in Cisco CallManager Administration.

Note You must reset the gatekeeper from the Gatekeeper Configuration window for the parameter change to take effect. If you are replacing one gatekeeper with another gatekeeper in this service parameter, you must reset both the gatekeepers. If you are deleting a value that was previously specified in this parameter, set it to its default value None. This is a required field. The maximum length is 255. Reset the gatekeeper from the Gatekeeper Configuration window for the parameter change to take effect.

Troubleshooting Gatekeepers

This topic describes how to troubleshoot gatekeepers using gateway registration rejection.



Show and Debug Commands

Cisco.com

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]

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—5-18

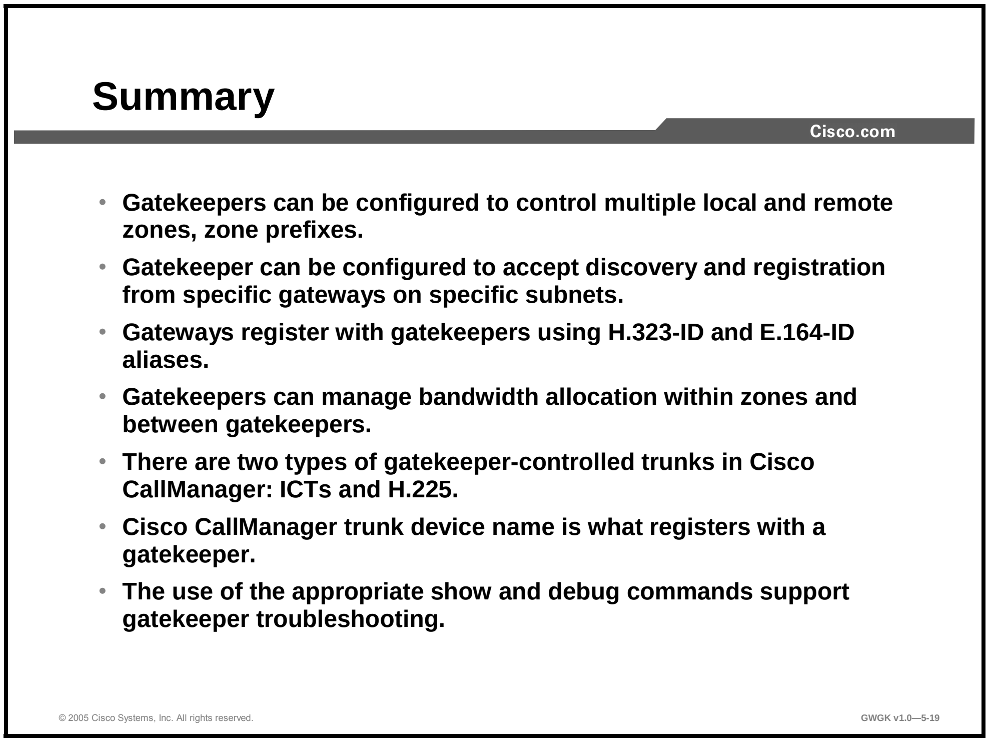
This figure shows in summary the commands that can be used to monitor and debug gatekeeper configurations and interoperability with gateways. The following are examples of the some of the show commands in the output:

```
SJC-GK#show gatekeeper gw-type-prefix
GATEWAY TYPE PREFIX TABLE
=========================
Prefix: 2#*
Zone SJC-GK master gateway list:
172.16.4.2:1720 SJC-GK

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

```
SJC-GK#show gatekeeper zone prefix
      ZONE PREFIX TABLE
      =================
GK-NAME                E164-PREFIX
-------                -----------
SJC-GK                 408*
DGK-FRSW               *

SJC-GK#show gatekeeper endpoints
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name Type Flags
--------------- ----- --------------- ----- --------- ---- -----
172.16.4.2      1720  172.16.4.2      55364 SJC-GK    VOIP-GW
    E164-ID: 6001
    E164-ID: 4155556001
    E164-ID: 6002
    E164-ID: 4155556002
    H323-ID: SJC-GK
    Voice Capacity Max.=  Avail.=  Current.= 0
Total number of active registrations = 1

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


SJC-GK       cisco.com     172.16.4.2      1719  LS
  BANDWIDTH INFORMATION (kbps) :
    Maximum total bandwidth : unlimited
    Current total bandwidth: 0
    Maximum interzone bandwidth: unlimited
    Current interzone bandwidth: 0
    Maximum session bandwidth : unlimited
  SUBNET ATTRIBUTES:
    All Other Subnets : (Enabled)
  PROXY USAGE CONFIGURATION :
    Inbound Calls from all other zones :
    to terminals in local zone SJC-GK: use proxy
    to gateways in local zone SJC-GK: do not use proxy
    to MCUs in local zone SJC-GK: do not use proxy
    Outbound Calls to all other zones :
    from terminals in local zone SJC-GK: use proxy
    from gateways in local zone SJC-GK: do not use proxy
    from MCUs in local zone SJC-GK  : do not use proxy
DGK-FRSW     cisco.com     172.16.4.1      1719  RS
```

Summary

This topic summarizes the key points discussed in this lesson.



Summary

Cisco.com

- Gatekeepers can be configured to control multiple local and remote zones, zone prefixes.
- Gatekeeper can be configured to accept discovery and registration from specific gateways on specific subnets.
- Gateways register with gatekeepers using H.323-ID and E.164-ID aliases.
- Gatekeepers can manage bandwidth allocation within zones and between gatekeepers.
- There are two types of gatekeeper-controlled trunks in Cisco CallManager: ICTs and H.225.
- Cisco CallManager trunk device name is what registers with a gatekeeper.
- The use of the appropriate show and debug commands support gatekeeper troubleshooting.

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—5-19

References

Understanding Cisco IOS Software Gatekeeper Call Routing:

- http://www.cisco.com/en/US/tech/tk652/tk701/technologies_tech_note09186a00800a8928.shtml

Configuring H323 Gateways

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/323confg/4gwconf.htm#wp1124639

Designing a Scaleable Dial Plan:

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/dp3_isd.htm

Configuring Gatekeepers and Proxies

- http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_configuration_guide_chapter09186a00802b460c.html

Configuring an Anonymous Device Gatekeeper with Cisco CallManager Versions 3.3 and 4.1

- http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_configuration_example09186a0080169445.shtml

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 parameter **h323-gateway voip id** serves what purpose on a gateway interface? (Source:)

A) to identify the gatekeeper for this gateway interface
B) to identify the alternate gatekeeper
C) to identify this interface for VoIP
D) to identify the signaling interface for this gateway

Q2) The parameter **h323-gateway voip id** is also used to do what? (Choose two.) (Source:)

A) identify an alternate gateway
B) identify the alternate gatekeeper
C) identify an alternate VoIP signaling interface
D) identify the priority of the alternate gatekeeper

Q3) When trunking between multiple Cisco CallManager clusters, what type of trunk should you use? (Source:)

A) H.225 gatekeeper controlled
B) intercluster gatekeeper controlled
C) intercluster nongatekeeper controlled
D) H.323 gateway

Q4) When trunking between multiple Cisco CallManager Express sites and multiple Cisco CallManager clusters, what type of trunk should you use? (Source:)

A) H.225 gatekeeper controlled
B) intercluster gatekeeper controlled
C) intercluster nongatekeeper controlled
D) H.323 gateway

Q5) Zone prefix is use to do what? (Source:)

A) match the zone technology prefix
B) prevent call loops from occurring
C) identify unresolved calls between zones
D) identifies the zone for call routing

Lesson Self-Check Answer Key

Q1)	A
Q2)	A, D
Q3)	B
Q4)	B
Q5)	D

Lesson 3

Configuring Directory Gatekeepers

Overview

Gatekeepers keep track of H.323 zones and forward inquiries regarding resources to process voice and video VoIP calls. A directory gatekeeper is basically a gatekeeper that forwards location request (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. This lesson discusses the overall role of the directory gatekeeper, and the role it plays within the H.323 gatekeeper solution. It also discusses how to deploy directory gatekeepers.

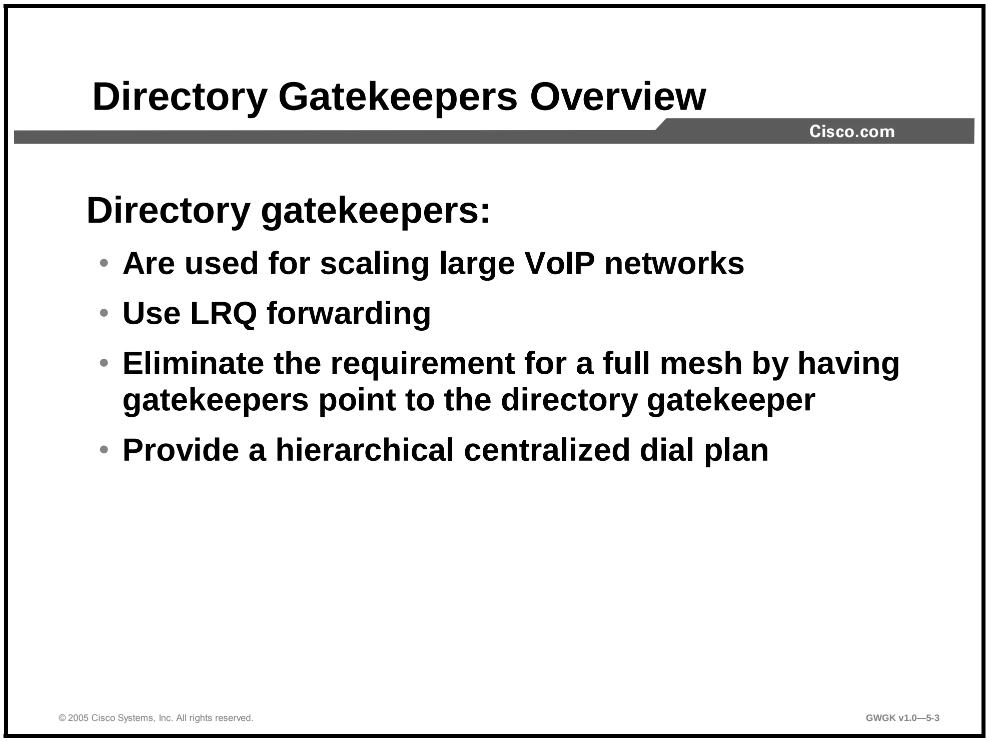
Objectives

Upon completing this lesson, you will be able to configure directory gatekeepers in a multiple-gatekeeper environment. This ability includes being able to meet these objectives:

- Describe directory gatekeeper functions and why and when they would be used
- Describe the RAS signaling used by directory gatekeepers with other gatekeepers
- Describe common directory gatekeeper deployment scenarios
- Configure a directory gatekeeper
- Use troubleshooting tools to resolve gatekeeper issues

Directory Gatekeeper Overview

This topic gives an overview of directory gatekeepers.



Directory Gatekeepers Overview

Cisco.com

Directory gatekeepers:

- **Are used for scaling large VoIP networks**
- **Use LRQ forwarding**
- **Eliminate the requirement for a full mesh by having gatekeepers point to the directory gatekeeper**
- **Provide a hierarchical centralized dial plan**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—5-3

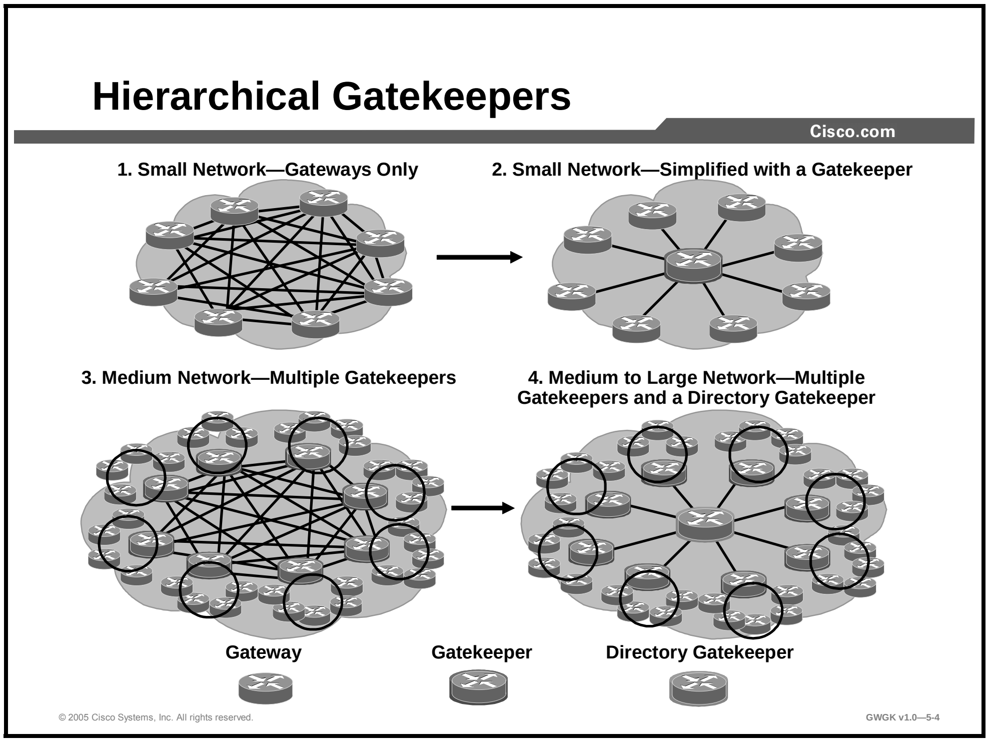
Gatekeepers keep track of other H.323 zones and forward calls appropriately. When many H.323 zones are present, gatekeeper configuration can become administratively intensive. In large VoIP installations, a centralized directory gatekeeper that contains a registry of all the different zones and coordinates LRQ-forwarding processes can be used. With directory gatekeepers, there is no longer a need for a full-mesh configuration between interzone gatekeepers.

Note A directory gatekeeper is not an industry standard, but is available in the Cisco implementation.

A directory gatekeeper is essentially a super gatekeeper that forwards LRQ messages. LRQ messages are Registration, Admission, and Status (RAS) messages triggered by an admission request (ARQ) message from endpoints that go from gatekeeper to gatekeeper. There is a limit of five hops for an LRQ message, which allows up to a four-tier gatekeeper hierarchy. Determining if a dedicated or shared directory gatekeeper is deployed is a network design decision.

By using a directory gatekeeper, it is no longer necessary to have 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 Signaling System 7-Advanced Intelligent Network (SS7-AIN), Gatekeeper Transaction Message Protocol (GKTMP) route servers, central authentication, authorization, and accounting (AAA), and so on.

Usually, directory gatekeepers are used only in large service provider wholesale deployments.



Hierarchical Gatekeepers

Cisco.com

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

GWGK v1.0—5-4

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

This example shows four network deployments:

1. For an H.323 network without gatekeepers, a fully meshed dial plan is required for each gateway. This entails significant administrative effort. A solution is to use a gatekeeper as shown in diagram 2.

2. Gatekeepers allow for 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. However, in a large network with multiple gatekeepers, again a full mesh is required between the gatekeepers to share dial plan information. When many 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 would use a centralized directory gatekeeper, sometimes called a super gatekeeper possibly 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 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.

Additional Considerations for Using Directory Gatekeepers

As mentioned, with 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 manage multiple 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.

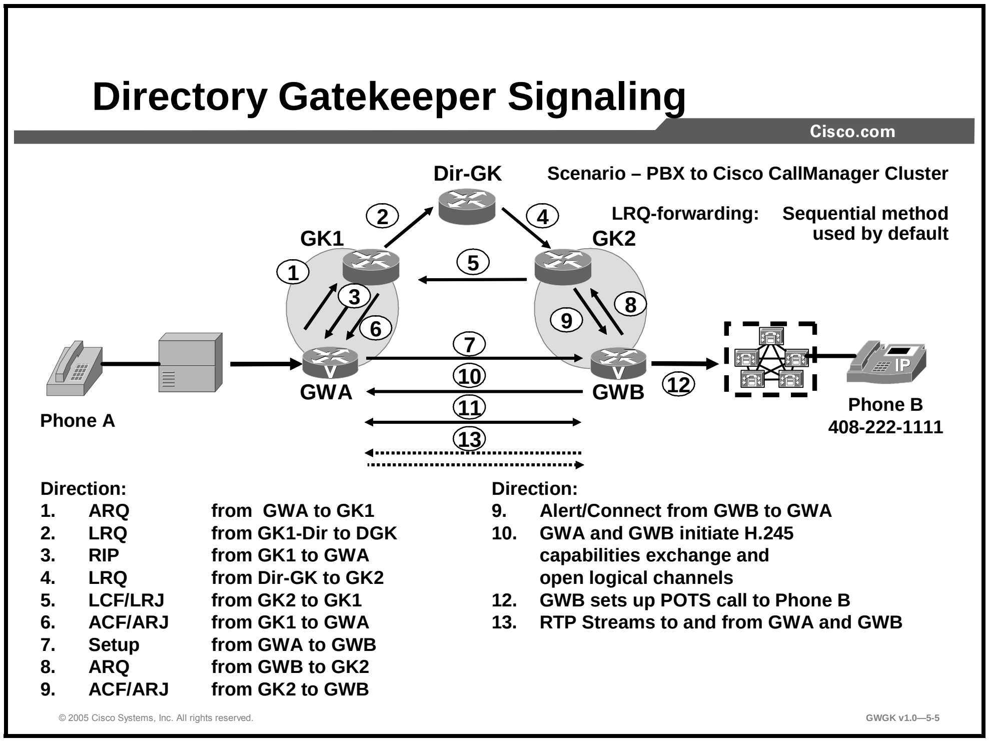
When adding a directory gatekeeper to a network, consider the following:

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

Each zone has its own gatekeeper. The directory gatekeeper minimizes gatekeeper configuration. Each gatekeeper knows its own information as well as the knowledge of the directory gatekeeper for all other calls. This way, the individual gatekeepers do not need the route information for gatekeepers in other zones.

Directory Gatekeeper Signaling

This topic describes directory gatekeeper RAS signaling.



Directory Gatekeeper Signaling

Cisco.com
Dir-GK
Scenario – PBX to Cisco CallManager Cluster
LRQ-forwarding: Sequential method used by default
GK1
GK2
1
2
3
4
5
6
7
8
9
10
11
12
13
GWA
GWB
IP
Phone A
Phone B
408-222-1111

Direction:
1. ARQ from GWA to GK1
2. LRQ from GK1-Dir to DGK
3. RIP from GK1 to GWA
4. LRQ from Dir-GK to GK2
5. LCF/LRJ from GK2 to GK1
6. ACF/ARJ from GK1 to GWA
7. Setup from GWA to GWB
8. ARQ from GWB to GK2
9. ACF/ARJ from GK2 to GWB

Direction:
9. Alert/Connect from GWB to GWA
10. GWA and GWB initiate H.245 capabilities exchange and open logical channels
12. GWB sets up POTS call to Phone B
13. RTP Streams to and from GWA and GWB

GWGK v1.0—5-5

There are two methods of forwarding LRQs: Blast and sequential. Sequential is the default. In the blast method, the gatekeeper will send LRQs to all of the destination gatekeepers whose zone prefixes or tech prefixes match the requesting destination pattern. With the blast method, the location confirmation (LCF) or location rejection (LRJ) messages flow directly back to the source gatekeeper bypassing any intermediate gatekeepers. Using the blast method the gatekeeper does not care if there is a response to the LRQ. The sequential LRQ method on the other hand, allows the gatekeeper to originate the LRQs with a finite delay. This delay can be used to trigger a new LRQ to another gatekeeper. Unlike the blast method, the sequential method allows for quicker resolution and can also limit the number of LRQ messages being sent. With the sequential method the LCF or LRJ flow back through the directory gatekeeper. In other words, the RAS messages traverse the same path as the LRQ.

- **Blast forwarding:** LRQs are sent immediately back-to-back in rapid sequence.
- **Sequential forwarding:** LRQs are sent one at a time with a delay between them.
- **LRQs:** LRQ messaging is sent between gatekeepers to locate a remote endpoint. Upon receiving an ARQ, a gatekeeper will determine whether the endpoint IP address is locally registered or if it needs to query another gatekeeper. In the later case, an LRQ is generated and sent to a neighboring gatekeeper for further resolution. The neighboring gatekeeper will send a LCF or an LRJ, or forward the LRQ as needed.
- **LRQ message:** An LRQ request message is triggered by a gatekeeper to locate the endpoint that can terminate a given E.164 address (phone number). The terminating gatekeeper responds with an LCF or an LRJ.
- **LCF message:** The LCF message confirms the request and contains the transport address of the destination LRQ message.

- **LRJ message**: The LRJ message rejects the request. This indicates that no gateway or endpoint was found in the terminating zone, for the given E.164 address.

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 408-222-1111 for Phone B

Step 1 Gateway A sends Gatekeeper 1 an ARQ, asking permission to call Phone B.

Step 2 Gatekeeper 1 does a look-up and does not find Phone B registered. Gatekeeper 1 does a prefix look-up and finds a wildcard match with Directory Gatekeeper. Gatekeeper 1 sends LRQ to Directory Gatekeeper and request in progress (RIP) to Gateway A.

Step 3 Gatekeeper 1 sends an RIP to Gateway A.

Step 4 Directory Gatekeeper does a prefix look-up and finds Gatekeeper 2. It forwards the LRQ to Gatekeeper 2.

Step 5 Gatekeeper 2 does a look-up and finds Phone B registered. It returns an LCF with the IP address of Gateway B to Gatekeeper 1.

Step 6 Gatekeeper 1 returns an ACF with the IP address of Gateway B.

Step 7 Gateway A sends a H.225 call-setup message to Gateway B with phone number of Phone B.

Step 8 Gateway B sends a H.225 call proceeding message to Gateway A.

Step 9 Gateway B sends Gatekeeper 2 an ARQ, asking permission to answer the call from Gateway A.

Step 10 Gatekeeper 2 returns an ACF with the IP address of Gateway A to Gateway B.

Step 11 Gateway B sends an alert/connect message Gateway A.

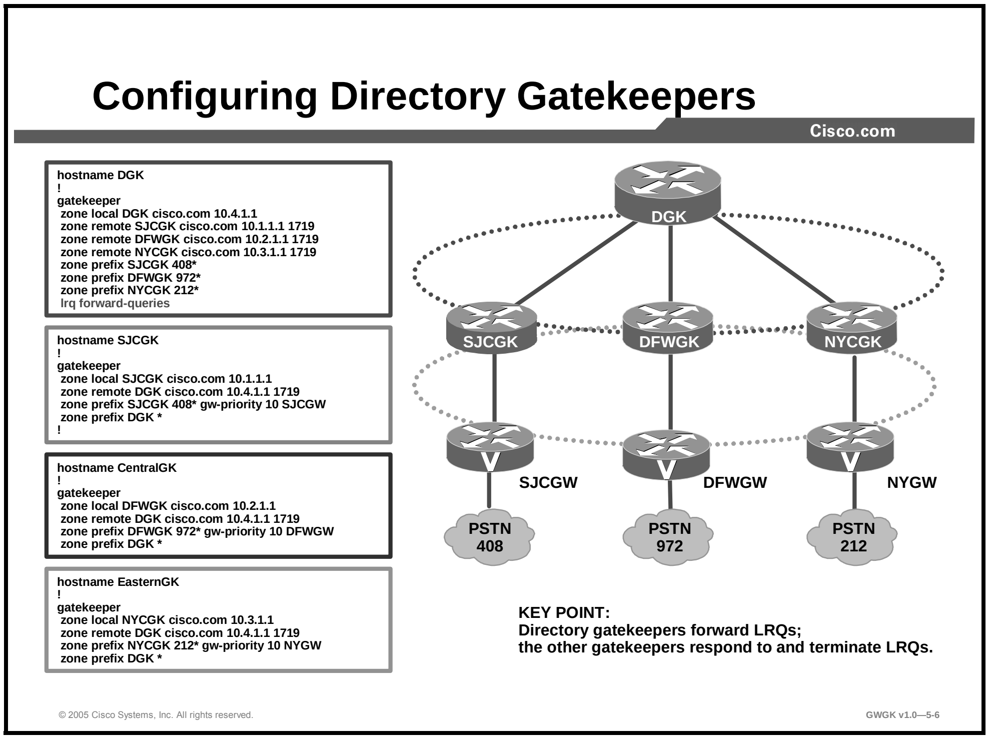
Step 12 Gateway B and Gateway A initiate H.245 capability exchange and open logical channels.

Step 13 Gateway B sets up a plain old telephone service (POTS) call to Phone B at 408-222-1111.

Step 14 Dual Real-Time Transport Protocol (RTP) streams are established between Gateway A and Gateway B.

Configuring Directory Gatekeepers

This topic describes how to configure directory gatekeepers.



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 DFWGK cisco.com 10.2.1.1 1719
 zone remote NYCGK cisco.com 10.3.1.1 1719
 zone prefix SJCGK 408*
 zone prefix DFWGK 972*
 zone prefix NYCGK 212*
 lrq forward-queries
```

```
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 CentralGK
!
gatekeeper
 zone local DFWGK cisco.com 10.2.1.1
 zone remote DGK cisco.com 10.4.1.1 1719
 zone prefix DFWGK 972* gw-priority 10 DFWGW
 zone prefix DGK *
```

```
hostname EasternGK
!
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 *
```

KEY POINT:
Directory gatekeepers forward LRQs;
the other gatekeepers respond to and terminate LRQs.

GWGK v1.0—5-6

The following are the steps to deploy a directory gatekeeper:

Step 1 Understand your dial plan requirements. Which prefixes will be managed by the directory gatekeeper and what prefixes will be managed locally by the gatekeepers?

Step 2 Configure your gateways to register with their prospective gatekeepers. Configure the local gatekeeper to manage only its local prefixes and the gateways registered to it.

Step 3 Configure the local gatekeeper to forward to the directory gatekeeper prefixes not local to it.

Step 4 Configure the directory gatekeeper to manage those prefixes between the gatekeepers it manages. Remember to add the **lrq forward-queries** command on the directory gatekeeper. This is the command that allows the gatekeeper to function as a directory gatekeeper.

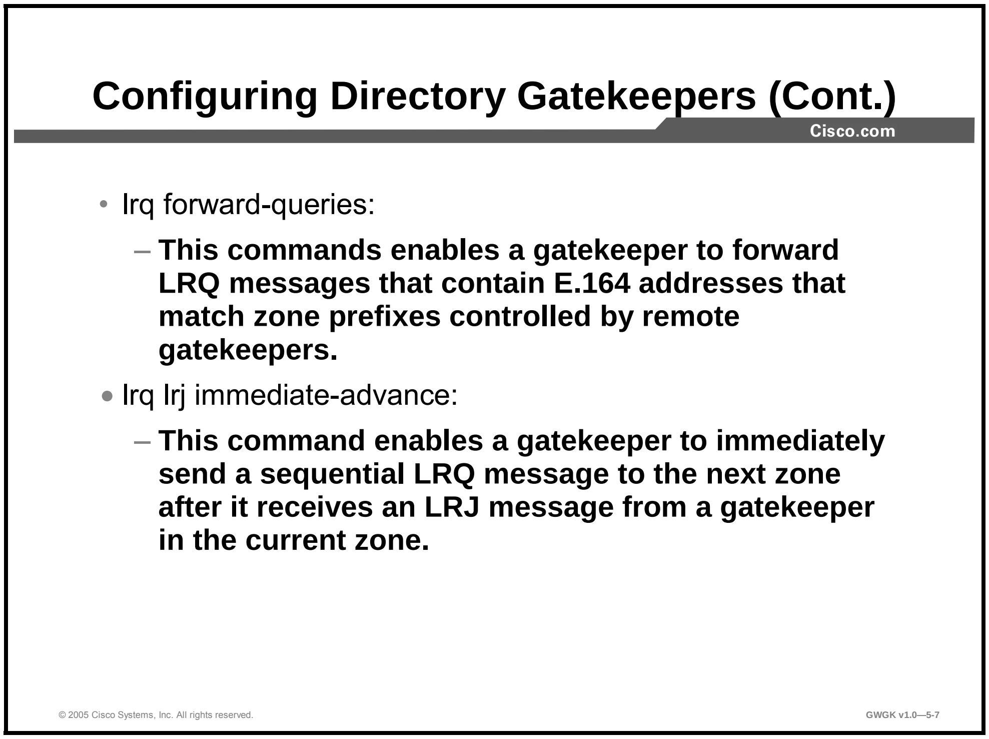
Usage Guidelines for lrq forward-queries

LRQ forwarding is dependent on a Cisco nonstandard field that first appeared in Cisco IOS Release 12.0(3)T. This means that any LRQ message received from a non-Cisco gatekeeper or any gatekeeper running a Cisco IOS software image prior to Cisco IOS Release 12.0(3)T is not forwarded.

The routing of E.164-addressed calls is dependent on the configuration of zone prefix tables (for example, area code definitions) on each gatekeeper. Each gatekeeper is configured with a list of prefixes controlled by itself and by other remote gatekeepers. Calls are routed to the zone that manages the matching prefix. Thus, in the absence of a directory service for such prefix tables, the network administrator may have to define extensive lists of prefixes on all the gatekeepers in your administrative domain.

To simplify this task, you can select one of your gatekeepers as the "directory" gatekeeper and configure that gatekeeper with the complete list of prefixes and the **lrq forward-queries** command. Simply configure all the other gatekeepers with their own prefixes and the wildcard prefix "*" for your directory gatekeeper.

This command affects only the forwarding of LRQ messages for E.164 addresses. LRQ messages for H.323-ID addresses are never forwarded.



Configuring Directory Gatekeepers (Cont.)

Cisco.com

- lrq forward-queries:
  - **This commands enables a gatekeeper to forward LRQ messages that contain E.164 addresses that match zone prefixes controlled by remote gatekeepers.**
- lrq lrj immediate-advance:
  - **This command enables a gatekeeper to immediately send a sequential LRQ message to the next zone after it receives an LRJ message from a gatekeeper in the current zone.**

GWGK v1.0—5-7

To enable the Cisco IOS gatekeeper to immediately send a sequential LRQ message to the next zone after it receives an LRJ message from a gatekeeper in the current zone, use the **lrq lrj immediate-advance** command in gatekeeper configuration mode.

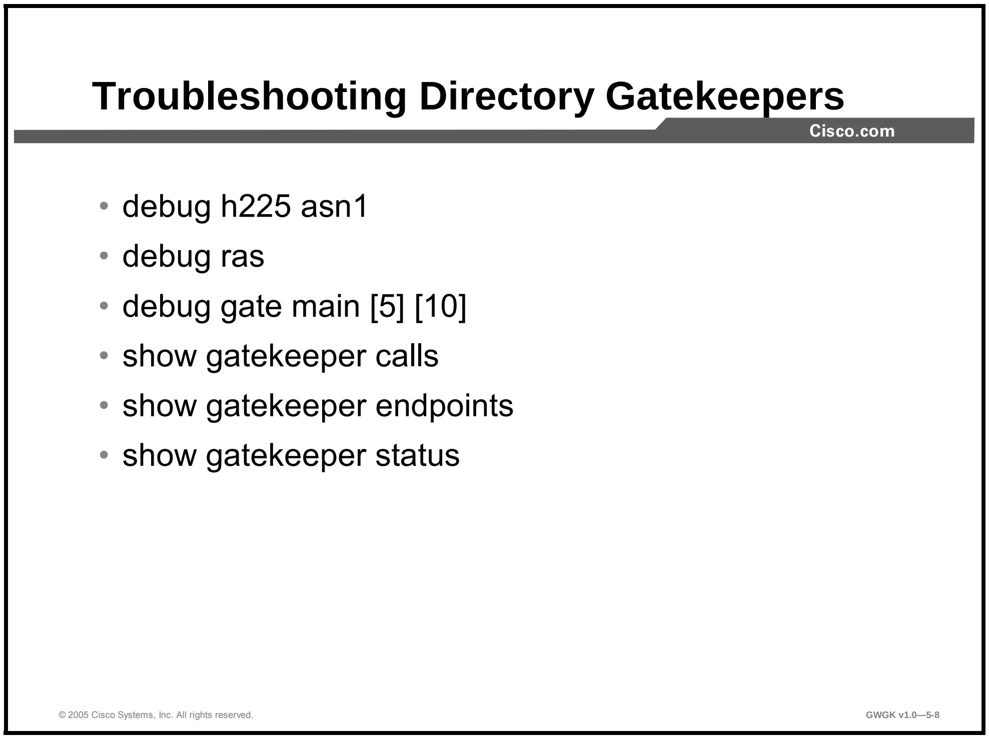
In a network in which LRQ messages are forwarded through multiple gatekeepers along a single path, a single LRQ message sent from a gatekeeper could solicit multiple LRJ and LCF responses. If an LRJ response is received first, a potentially unnecessary LRQ message could be sent to the next zone, increasing traffic.

To avoid this problem, perform the following:

- Configure the zone prefix to send sequential LRQ messages rather than to use the **blast** option, using the **zone prefix** command.
- Configure the sequential timer on each gatekeeper along the path, using the **timer lrq seq delay** command.

Troubleshooting Directory Gatekeepers

This topic describes how to troubleshoot directory gatekeepers.



Troubleshooting Directory Gatekeepers

Cisco.com

- debug h225 asn1
- debug ras
- debug gate main [5] [10]
- show gatekeeper calls
- show gatekeeper endpoints
- show gatekeeper status

GWGK v1.0—5-8

Here are a few show commands typically used to monitor gatekeeper functions:

- **show gatekeeper calls:** This command displays the status of each ongoing call of which a gatekeeper is aware.
- **show gatekeeper endpoints:** This command displays the status of all registered endpoints for a specific gatekeeper. Here is an example of the output:

```
GK# show gatekeeper endpoints


CallsignalAddr   Port  RASSignalAddr   Port   Zone Name
Type     F

---------------  ----  -------------   -----  ----------   ---
--    --

172.21.127.8     1720  172.21.127.8    24999  sj-gk        MCU

           H323-ID:joe@cisco.com

           Voice Capacity Max.=23  Avail.=23

           Total number of active registrations = 1

172.21.13.88     1720  172.21.13.88    1719   sj-gk
VOIP-GW   O    H323-ID:la-gw
```

- **show gatekeeper zone status:** This command display the status of zones related to a gatekeeper. Here is an example of the output:

```
GK# 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         0
  SUBNET ATTRIBUTES :
    All Other Subnets :(Enabled)
  PROXY USAGE CONFIGURATION :
    inbound Calls from germany.xyz.com :
      to terminals in local zone sj.xyz.com :use proxy
      to gateways in local zone sj.xyz.com  :do not use proxy
    Outbound Calls to germany.xyz.com
      from terminals in local zone germany.xyz.com :use proxy
      from gateways in local zone germany.xyz.com  :do not use proxy
    Inbound Calls from all other zones :
      to terminals in local zone sj.xyz.com :use proxy
      to gateways in local zone sj.xyz.com  :do not use proxy
    Outbound Calls to all other zones :
      from terminals in local zone sj.xyz.com :do not use proxy
      from gateways in local zone sj.xyz.com  :do not use proxy
tokyo.xyz.co xyz.com         10.0.0.0        1719  RS             0
milan.xyz.co xyz.com         10.0.0.0        1719  RS             0
```

- **show gatekeeper gw-type-prefix:** This command displays the technology prefixes for the zone. Here is an example of the output:

```
GK#show gatekeeper gw-type-prefix
GATEWAY TYPE PREFIX TABLE
=========================
Prefix: 1#*    (Default gateway-technology)
  Zone localzone1 master gateway list:
    10.1.1.240:1720 tgw1
    10.1.1.241:1720 tgw2 (out-of-resources)
```

The following are examples of the debug commands used to troubleshoot and monitor gatekeeper operations:

- **debug h225 asn1:** Abstract Syntax Notation One (ASN1). An OSI language designed to describe data types, independent of particular computer structures and representation techniques. ASN.1 is described in ISO International Standard 8824. Here is an example of the output:

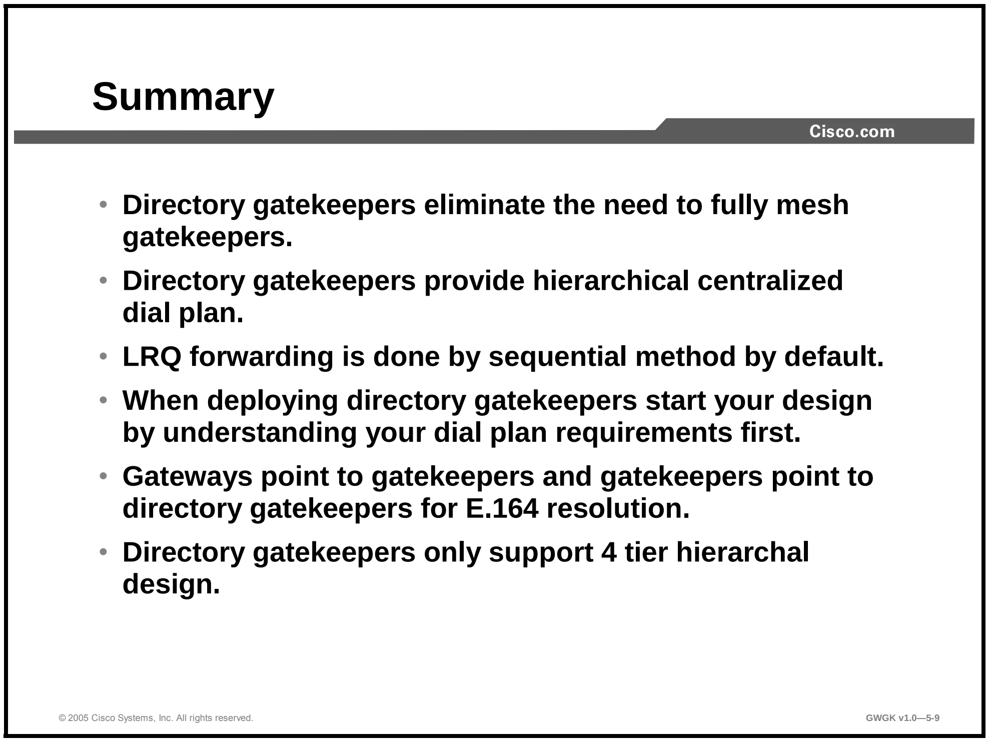
```
DGK-FRSW#debug h225 asn1

H.225 ASN1 Messages debugging is on

DGK-FRSW#

*Nov 29 08:13:22.242: RAS INCOMING ENCODE BUFFER::=
4A800825010180733440B5000012

26828990001100000000000000000000000000000000000F01400500440046
0057002D0047004B00

AC10040306B71780000F01400500440046005700 2D0047004B0180

*Nov 29 08:13:22.242:

*Nov 29 08:13:22.242: RAS INCOMING PDU ::=


value RasMessage ::= locationRequest :

    {

      requestSeqNum 2086

      destinationInfo

      {

        dialedDigits : “4001”

      }

      nonStandardData

      {

        nonStandardIdentifier h221NonStandard :

        {

          t35CountryCode 181

          t35Extension 0

          manufacturerCode 18

        }

        data '8289900011000000000000000000000000000000...'H

      }

      replyAddress ipAddress :

      {

        ip 'AC100403'H

        port 1719

      }

      sourceInfo

      {

        h323-ID : {“DFW-GK”}

      }
      canMapAlias TRUE
    }
*Nov 29 08:13:22.242: H225 NONSTD INCOMING ENCODE BUFFER::=
82899000110000000000
0000000000000000000000000F014005004400460057002D0047004B
*Nov 29 08:13:22.242:
*Nov 29 08:13:22.242: H225 NONSTD INCOMING PDU ::=

value LRQnonStandardInfo ::=
    {
      ttl 6
      nonstd-callIdentifier
      {
        guid '00000000000000000000000000000000'H
      }
      gatewaySrcInfo
      {
        h323-ID : {"DFW-GK"}
      }
    }
*Nov 29 08:13:22.242: RAS OUTGOING PDU ::=
value RasMessage ::= requestInProgress :
    {
      requestSeqNum 2086
      delay 6000
    }
*Nov 29 08:13:22.242: RAS OUTGOING ENCODE BUFFER::=
8005000825176F
*Nov 29 08:13:22.242:
*Nov 29 08:13:22.246: H225 NONSTD OUTGOING PDU ::=

value LRQnonStandardInfo ::=
    {
      ttl 5
      nonstd-callIdentifier
      {
        guid '00000000000000000000000000000000'H
      }
      gatewaySrcInfo
      {
        h323-ID : {"DFW-GK"}
      }
    }
*Nov 29 08:13:22.246: H225 NONSTD OUTGOING ENCODE BUFFER::=
82099000110000000000

0000000000000000000000000F014005004400460057002D0047004B

*Nov 29 08:13:22.246:

*Nov 29 08:13:22.246: RAS OUTGOING PDU ::=


value RasMessage ::= locationRequest :
    {
      requestSeqNum 2086
      destinationInfo
      {
        dialedDigits : “4001”
      }
      nonStandardData
      {
        nonStandardIdentifier h221NonStandard :
        {
          t35CountryCode 181
          t35Extension 0
          manufacturerCode 18
        }
        data '8209900011000000000000000000000000000000...'H
      }
      replyAddress ipAddress :
      {
        ip 'AC100403'H
        port 1719
      }
      sourceInfo
      {
        h323-ID : {“DFW-GK”}
      }
      canMapAlias TRUE
    }
```

- **debug ras:** This command displays the types and addressing of RAS messages sent and received from a gatekeeper and gateway. Here is an example of the output:

```
DGK-FRSW#debug ras

H.323 RAS Messages debugging is on

DGK-FRSW#

*Nov 29 08:10:37.542:  RecvUDP_IPSockData  successfully rcvd
message of length 8

1 from 172.16.4.3:1719

*Nov 29 08:10:37.542: LRQ (seq# 2083) rcvdparse_lrq_nonstd:
LRQ Nonstd decode su

cceeded, remlen = 1152113648

*Nov 29 08:10:37.542:  IPSOCK_RAS_sendto:   msg length 7 from
172.16.4.1:1719 to

 172.16.4.3: 1719

*Nov 29 08:10:37.542:       RASLib::RASSendRIP: RIP (seq#
2083) sent to 172.16.4

.3

*Nov 29 08:10:37.542:  IPSOCK_RAS_sendto:   msg length 81 from
172.16.4.1:1719 t

o 172.16.4.2: 1719

*Nov 29 08:10:37.542:       RASLib::RASSendLRQ: LRQ (seq#
2083) sent to 172.16.4

.2
```

Summary

This topic summarizes the key points discussed in this lesson.



Summary

Cisco.com

- Directory gatekeepers eliminate the need to fully mesh gatekeepers.
- Directory gatekeepers provide hierarchical centralized dial plan.
- LRQ forwarding is done by sequential method by default.
- When deploying directory gatekeepers start your design by understanding your dial plan requirements first.
- Gateways point to gatekeepers and gatekeepers point to directory gatekeepers for E.164 resolution.
- Directory gatekeepers only support 4 tier hierarchal design.

GWGK v1.0—5-9

References

For additional information, refer to these resources:

Gateway Configuration:

- http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00801f00ed.html#wp1183281

H.323 Technical Details and Documentation:

- http://www.cisco.com/en/US/tech/tk652/tk701/tk309/tech_protocol_home.html

Cisco IP Telephony Solution Reference Network Design (SRND) for Cisco CallManager 4.0:

- http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a00802c370c.html

Cisco IOS Software Library 12.3 T

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vcl.htm

Cisco IOS Software Library 12.3 T H.323 Gateway Configuration:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/323confg/index.htm

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) LRQ forward queries define the gatekeeper as a _________. (Source:)

A) multizone gatekeeper
B) gatekeeper that forwards LRQs
C) directory gatekeeper
D) this is part of all gatekeeper configurations

Q2) An H.323 network without gatekeepers requires that the network is _______. (Source:)

A) managed by gateways
B) fully staffed with qualified system administrators
C) a hub-and-spoke topology dial plan
D) a fully meshed dial plan

Q3) What are the possible RAS messages sent by a gatekeeper whom just sent a LRQ? (Source:)

A) LRJ
B) LRJ and LCF
C) LRJ or LCF
D) RIP

Lesson Self-Check Answer Key

Q1)	C
Q2)	D
Q3)	C

Lesson 4

Configuring Gatekeeper Redundancy

Overview

To maintain resiliency and scalability, gatekeepers need to be able to have backup to support mission-critical VoIP and video traffic. This lesson discusses three ways to provide gatekeeper redundancy and how to configure the various methods.

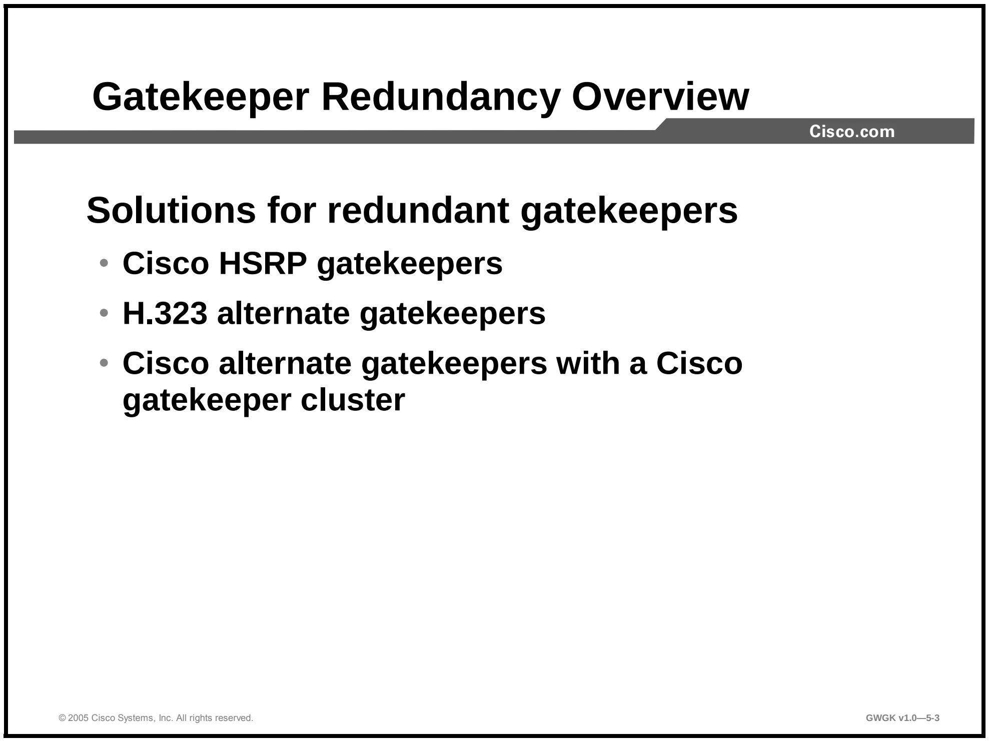
Objectives

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

- Describe the requirement for using gatekeeper redundancy and various options
- Implement gatekeeper redundancy using HSRP
- Implement alternate gatekeepers
- Implement GUP
- Implement gatekeeper clustering

Gatekeeper Redundancy Overview

This topic provides an overview of gatekeeper redundancy.



Gatekeeper Redundancy Overview

Cisco.com

Solutions for redundant gatekeepers

- **Cisco HSRP gatekeepers**
- **H.323 alternate gatekeepers**
- **Cisco alternate gatekeepers with a Cisco gatekeeper cluster**

GWGK v1.0—5-3

There are three main solutions for redundant gatekeepers:

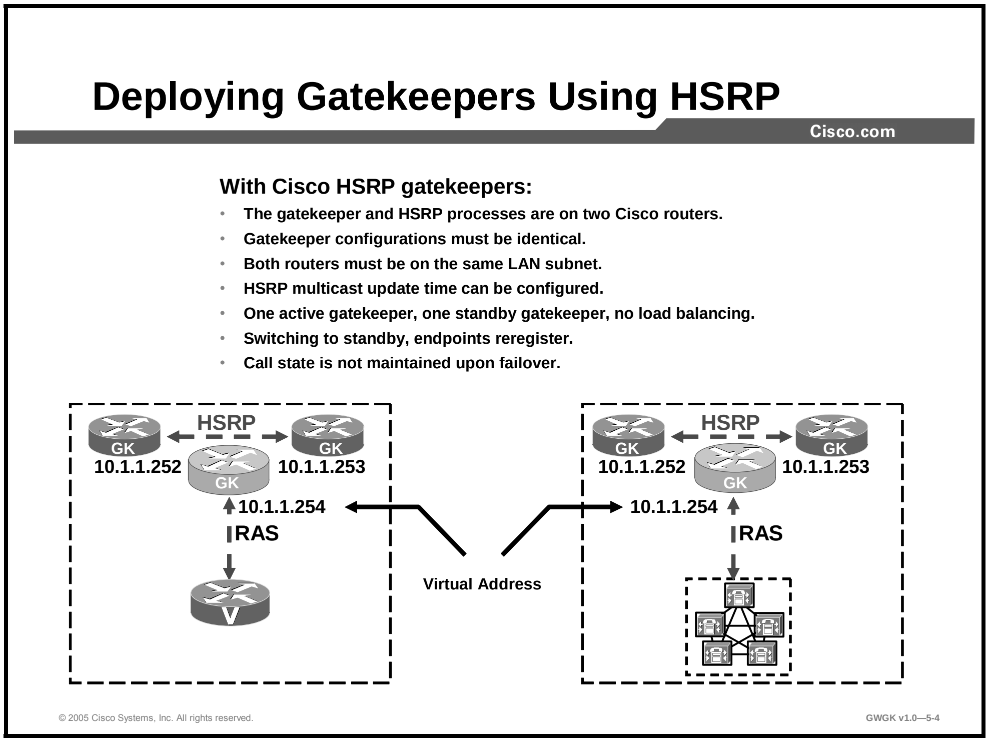
1. **H.323 alternate gatekeepers:** The alternate gatekeeper feature allows a gateway to use up to two alternate gatekeepers as a backup in the case of a primary gatekeeper failure. The main benefit of this feature is redundancy if the primary gatekeeper becomes unresponsive.

2. **Redundant gatekeepers with Hot Standby Router Protocol (HSRP):** Gatekeeper HSRP support consists of elements of the gateway and gatekeeper functions in the router. The gateway periodically retries its registration when it detects a possible gatekeeper failure to register itself with the backup gatekeeper. Although it is a backup, the gatekeeper operates in a passive mode in which it does not accept registrations, and it becomes active when it detects via HSRP a loss of communication with the primary gatekeeper.

3. **Cisco alternate gatekeepers with Cisco gatekeeper clusters:** This is a Cisco-proprietary solution using Cisco Gatekeeper Update Protocol (GUP), which runs between the alternate gatekeepers of a Cisco gatekeeper cluster.

Deploying Gatekeepers using HSRP

This topic describes how to use HSRP in a gatekeeper environment.



Deploying Gatekeepers Using HSRP

Cisco.com

With Cisco HSRP gatekeepers:

- The gatekeeper and HSRP processes are on two Cisco routers.
- Gatekeeper configurations must be identical.
- Both routers must be on the same LAN subnet.
- HSRP multicast update time can be configured.
- One active gatekeeper, one standby gatekeeper, no load balancing.
- Switching to standby, endpoints reregister.
- Call state is not maintained upon failover.

GWGK v1.0—5-4

Gatekeeper redundancy using HSRP uses two Cisco routers for the gatekeeper and HSRP processes. HSRP creates a virtual IP router for two physical routers. The virtual HSRP router has its own IP address. However, these two routes must be on the same subnet, as shown in these examples:

- HSRP-Member-Router-1 = 10.1.1.252
- HSRP-Member-Router-2 = 10.1.1.253
- HSRP-Router-12 = 10.1.1.254

The “Primary Gatekeeper Configuration Commands” table shows a sample of how HSRP is configured on a primary gatekeeper:

Primary Gatekeeper Configuration Commands

Command	Description

`interface fastethernet 0/1`
`ip address 10.1.1.252 255.255.255.0`
`standby 1 ip 10.1.1.254`
`standby 1 preempt`
`standby 1 timers 5 15`
	The timers are very important. If these values are not set to the same number in both routers, HSRP will not function properly.

`standby 1 priority 110`	This router will be the priority gatekeeper for HSRP. The default value is 100 in a range from 1 to 255

The “Alternate Gatekeeper Configuration Commands” table shows a sample of how HSRP is configured on an alternate gatekeeper:

Alternate Gatekeeper Configuration Commands

Command	Description

`interface fastethernet 0/1`
`ip address 10.1.1.253 255.255.255.0`
`standby 1 ip 10.1.1.254`
`standby 1 preempt`
	This command allows the local router to assume control as the active gatekeeper if it has a higher priority than the current active gatekeeper does.

`standby 1 timers 5 15`	This command sets the hello and holdtime values that HSRP will use to declare the active HSRP gatekeeper down.

Note Using HSRP as an IP router redundant solution is a very popular. The HSRP gatekeeper, which uses two physical gatekeepers and creates a virtual HSRP gatekeeper, is only used on Cisco routers. It is a good idea to use the same physical platforms with the same Cisco IOS releases on the HSRP routers. The down side to this is that the gatekeepers need to be on the same subnet

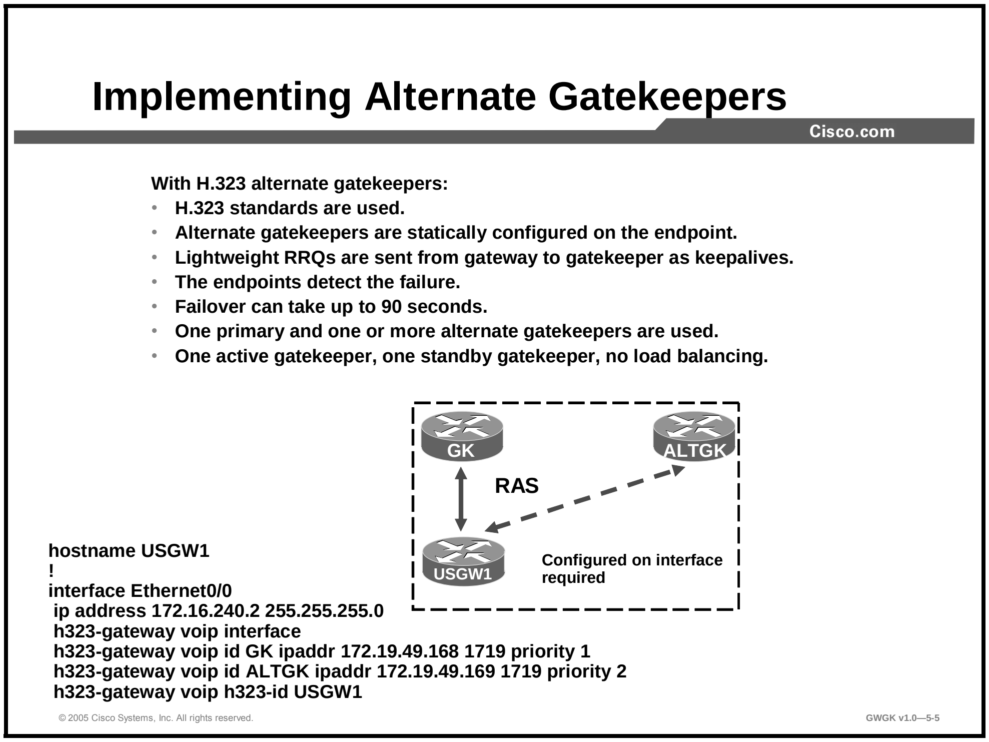
If the primary gatekeeper fails in an HSRP redundancy model, the failure is transparent to the endpoint because the endpoints are pointing to the virtual HSRP router. Failover time can be tuned to under 10 seconds by reducing the hello timers of HSRP. However, these timers must be tuned on both gatekeepers. Delay may still be an issue. Depending on where the gateway is in the registration process, gateway failover to a new gatekeeper with HSRP could be 40 or more seconds due to reregistration.

Using the HSRP redundancy method, the hello timers sent between the HSRP routers can be configured. The default time is 3 seconds. Both routers send these hellos via multicast. Failover time can also be configured; the default is 10 seconds. Depending on where the gateway is in the registration process, the gateway failover to a new gatekeeper using HSRP could take 40 or more seconds due to reregistration.

If the nonactive router does not receive three hellos in a row from its primary router, it will switch over and become the active HSRP router. Note that these routers must be on the same LAN segment. In an HSRP redundant gatekeeper deployment, only one gatekeeper is active. This means that load balancing is not possible with this feature. Another important point to remember is that the gatekeeper state is not maintained between the active and standby gatekeepers. This means that when the standby gatekeeper becomes the active gatekeeper it is unaware of the calls that are active. This can immediately affect call quality as new calls try to be placed over what could be full network connections. Over time, as calls complete and the network links return to a non-over-subscribed state and the gatekeeper continues to apply Call Admission Control (CAC), call quality will return to normal.

Implementing Alternate Gatekeepers

This topic describes how to implement alternate gatekeepers.



Implementing Alternate Gatekeepers

Cisco.com

With H.323 alternate gatekeepers:

- H.323 standards are used.
- Alternate gatekeepers are statically configured on the endpoint.
- Lightweight RRQs are sent from gateway to gatekeeper as keepalives.
- The endpoints detect the failure.
- Failover can take up to 90 seconds.
- One primary and one or more alternate gatekeepers are used.
- One active gatekeeper, one standby gatekeeper, no load balancing.

```
hostname USGW1
!
interface Ethernet0/0
 ip address 172.16.240.2 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id GK ipaddr 172.19.49.168 1719 priority 1
 h323-gateway voip id ALTGK ipaddr 172.19.49.169 1719 priority 2
 h323-gateway voip h323-id USGW1
```

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—5-5

An alternate gatekeeper provides redundancy for a gateway in a system in which gatekeepers are used. Redundant H.323 zone support in the gateway allows a user to configure two gatekeepers in the gateway (one as the primary and the other as the alternate). An endpoint that detects the failure of its gatekeeper can safely recover from that failure by using an alternate gatekeeper for future requests, including requests for existing calls. A gateway can only be registered to a single gatekeeper at a time. Only one gatekeeper is allowed to manage a single zone.

When using alternate gatekeepers, the gateways register to the gatekeeper using a static registration statement configured on the gateway or terminal. This is done using a unicast registration process. Lightweight registration requests (RRQs) are sent from the gateways and terminals to the gatekeepers as keepalives, which provide a mechanism for informing the gatekeeper about the actual state of the registered endpoints. The gatekeeper checks whether the endpoint is online or offline.

When alternate gatekeepers are added, the configuration is done on the endpoints, not on the gatekeeper. This is done with a secondary registration statement configured with a lower priority. To configure alternate gatekeepers on Cisco gateways, configure a list of gatekeepers with different priorities.

Note In the example in the figure, the lower priority wins. In other words, "ALTGK" is the alternate and is only used if "GK" is not reachable. If the gatekeeper comes back after a switchover, the gateway will still be registered with the alternate gatekeeper.

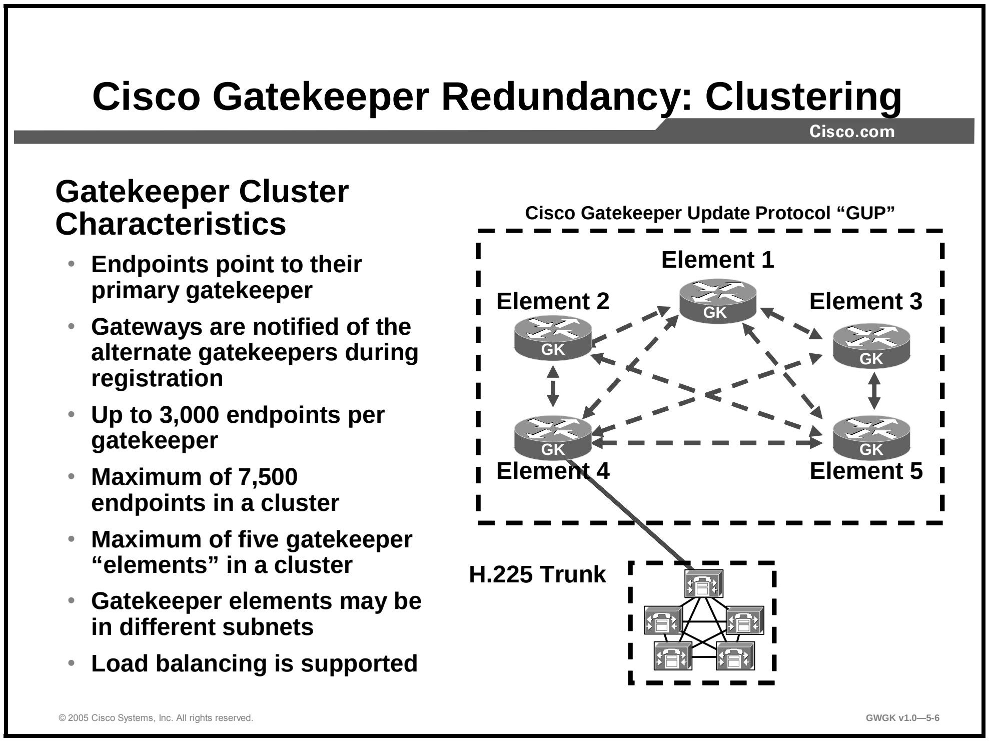
If the gatekeeper fails to send an registration confirmation (RCF) message back to the gateway, the gateway sends an RRQ message to the alternate gatekeeper. The alternate gatekeeper can be geographically independent in an IP network, but delay issues may arise if it is configured over long distances. Therefore, it is recommended that you keep alternate gatekeepers in the same geographic area.

There need to be multiple gatekeeper-controlled trunks configured to provide redundancy when you use an alternate gatekeeper for Cisco CallManager,.

When configuring Cisco CallManager gatekeeper-controlled trunks, maybe you want to create the first trunk named “primary” and the second named “secondary”. This way, you can tell which gatekeeper and IP address are primary.

Implementing GUP

This topic describes how to implement GUP.



Cisco Gatekeeper Redundancy: Clustering

Cisco.com

Gatekeeper Cluster Characteristics

- Endpoints point to their primary gatekeeper
- Gateways are notified of the alternate gatekeepers during registration
- Up to 3,000 endpoints per gatekeeper
- Maximum of 7,500 endpoints in a cluster
- Maximum of five gatekeeper "elements" in a cluster
- Gatekeeper elements may be in different subnets
- Load balancing is supported

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—5-6

Clustering

Each gatekeeper in a cluster must have the following characteristics:

- Each gatekeeper must have a configuration compatible with all other gatekeepers in the cluster. For example, the zone definitions of each gatekeeper should declare the same set of alternate zones on all other gatekeepers in the cluster.
- Each gatekeeper can act as a substitute for the whole cluster because each gatekeeper has the registration and availability information for every endpoint in the cluster. For example, location requests (LRQs) from remote gatekeepers are only sent to one gatekeeper in the cluster. This local gatekeeper uses the remote clustered gatekeepers in a round-robin fashion to balance the LRQ load between different elements of the cluster.
- Gatekeeper cluster members use GUP for communication.
- Each zone should be capable of registering the same endpoints, such as gateways. For example, each zone gatekeeper supports the same set of zone prefixes, so endpoints can register with any gatekeeper the cluster.
- A maximum of five gatekeepers can be used, including the local zone. For local clusters, this means that there can be no more than four alternate gatekeepers.
- Although each gateway registers with a single gatekeeper, any gateway can be redirected to a different gatekeeper if its original gatekeeper is at capacity or fails.
- Each gateway is informed of alternate gatekeepers at registration (with an RCF) in priority order and registers with the highest-priority alternate gatekeeper in the event of failure. A gateway can also move to another gatekeeper if its primary gatekeeper fails.

Note Gatekeeper clusters are supported on gatekeepers running Cisco IOS Release 12.2(1)T or later.

Load Balancing

Load balancing occurs when a gatekeeper with overloaded resources redirects its gateways to an alternate cluster gatekeeper with sufficient resources. Load balancing does not balance loads equally among gatekeepers. Instead, it is a means that a cluster gatekeeper offloads extra load.

In a Cisco gatekeeper cluster, it is possible to share load on all gatekeepers in the cluster. For example, a cluster with 300 gateways and three gatekeepers (Cluster Gatekeeper 1, Cluster Gatekeeper 2, and Cluster Gatekeeper 3) may have the following configuration:

- Gateways 1 through 100 use Cluster Gatekeeper 1 as the primary and Cluster Gatekeeper 2 and Cluster Gatekeeper 3 as the alternates.
- Gateways 101 through 200 use Cluster Gatekeeper 2 as the primary and Cluster Gatekeeper 1 and Cluster Gatekeeper 3 as the alternates.
- Gateways 201 through 300 use Cluster Gatekeeper 3 as the primary and Cluster Gatekeeper 1 and Cluster Gatekeeper 2 as the alternates.

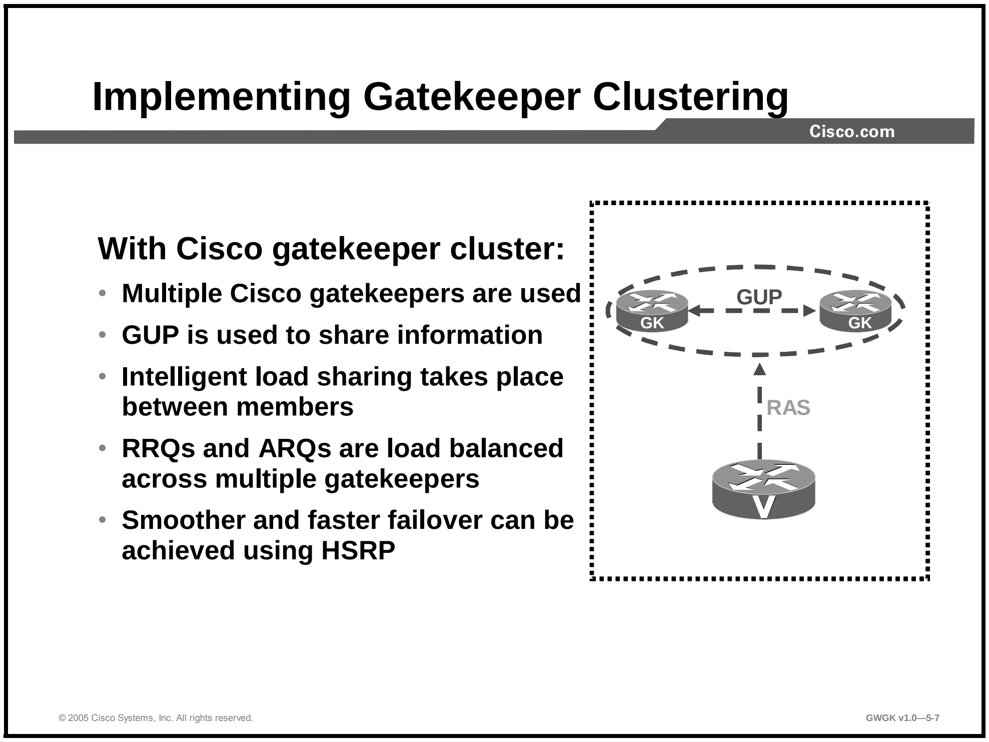
Load balancing is initiated when a gatekeeper sends RAS rejection message in response to an admission request (ARQ) or RRQ message from one of its gateways. The rejection message contains the IP address of an alternate gatekeeper. When the gateway receives this message, it attempts to register with that alternate. Once it registers, the gateway gives the new gatekeeper a list of its active calls via information request responses (IRRs).

Note Load-balanced gateways do not automatically come back to their primary gatekeeper.

The use of Cisco gatekeeper clustering eliminates the issue HRSP in CAC presents.

Implementing Gatekeeper Clustering

This topic describes how to implement gatekeeper clustering.



Implementing Gatekeeper Clustering

Cisco.com

With Cisco gatekeeper cluster:

- **Multiple Cisco gatekeepers are used**
- **GUP is used to share information**
- **Intelligent load sharing takes place between members**
- **RRQs and ARQs are load balanced across multiple gatekeepers**
- **Smoother and faster failover can be achieved using HSRP**

GK
GUP
GK
RAS
V

GWGK v1.0—5-7

When endpoints first register, they are given a list of alternate gatekeepers in a priority order in the RCF message. The priorities are determined by the capacity available at each of the alternate gatekeeper, as reported to the primary gatekeeper, by the GUP announcement message. This list is updated with every RCF (for lightweight RRQs) and the priorities are adjusted. In case of primary gatekeeper failure, the endpoints register with the highest priority gatekeeper as listed in the cluster element configuration.

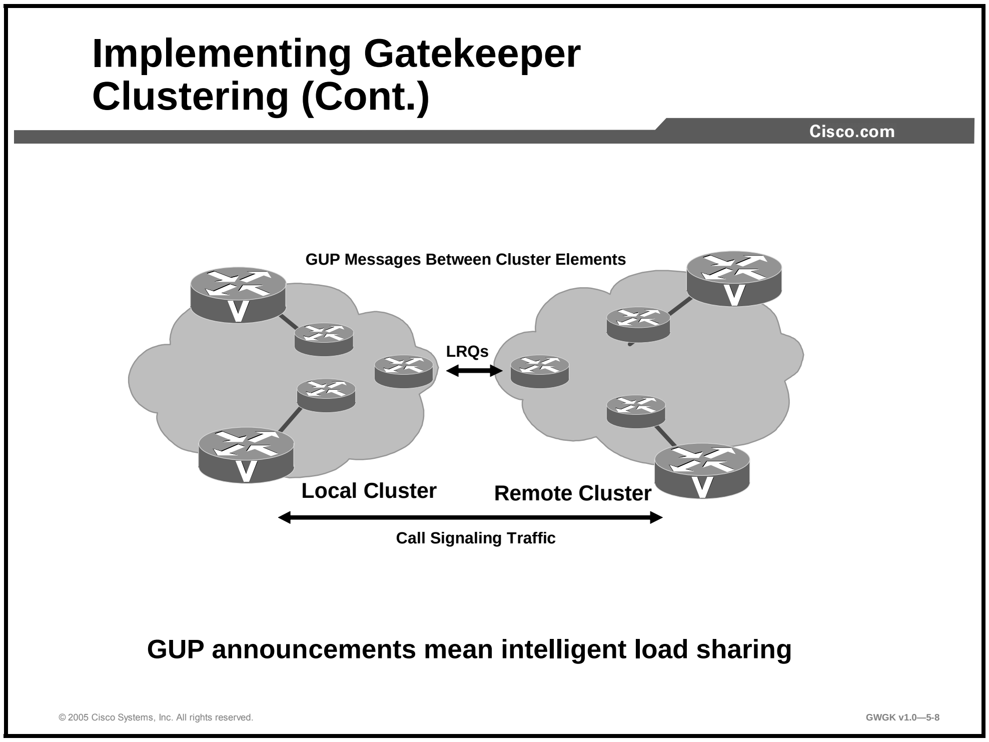
No configuration is needed on the gateway for a gateway to use gatekeeper clustering. The difference between clustering and configuring a gateway to use an alternate gatekeeper is that under the alternate gatekeeper configuration, the limit is two gatekeepers: A primary and a secondary. As with gatekeeper clustering, no configuring is needed on the gateway, the gateway received the list of backup gatekeepers from its local gatekeeper, and the limit per cluster is five. Therefore, gatekeeper clustering is a more scalable solution than using an alternate gatekeeper configuration on the gateway.

A gatekeeper cluster is a group of up to five gatekeepers within a gatekeeper zone. In the event of high call volume or gatekeeper failure, gateways can be redirected to other gatekeepers in the cluster. This ability to cluster gatekeepers together and reroute calls increases gatekeeper reliability and scalability.

Within the zone, the cluster shares information about the following elements:

- Bandwidth
- Current calls
- CPU use
- Alternate available gatekeepers
- Gateways registration within zones
- Remote gatekeepers

Gatekeeper cluster members share information via GUP, a proprietary Cisco protocol. Because gatekeepers share information, a gateway only needs to register with one gatekeeper in the cluster. Similarly, LRQ message exchanges from remote gatekeepers are only sent to one gatekeeper in the cluster. These factors make gatekeeper clusters more scalable than other redundant solutions, such as HSRP.



Implementing Gatekeeper Clustering (Cont.)

GUP announcements mean intelligent load sharing

This figure illustrates the clustering of gatekeepers. The gateways still register with a single gatekeeper, but they can be asked to move to a different one, for example, in the case of load balancing.

When a gatekeeper fails, the endpoints that it had registered to it will find different gatekeepers with which to register. The cluster should be engineered in such a way that the failure of a single gatekeeper should not put the others over their capacities.

When the gatekeeper comes back up, it will get all the GUP messages for registrations, and the like. However, no endpoints will register to it unless any of the other gatekeepers experiences a load balancing condition, in which case the new gatekeeper with no load will be the first candidate to have the endpoint sent to it. Load balancing and the redundancy feature do not require any nonstandard data or deviation from established standards from the gateways. As long as they follow alternate gatekeeper procedures as defined in the ITU standards, they should be able to work with clusters.

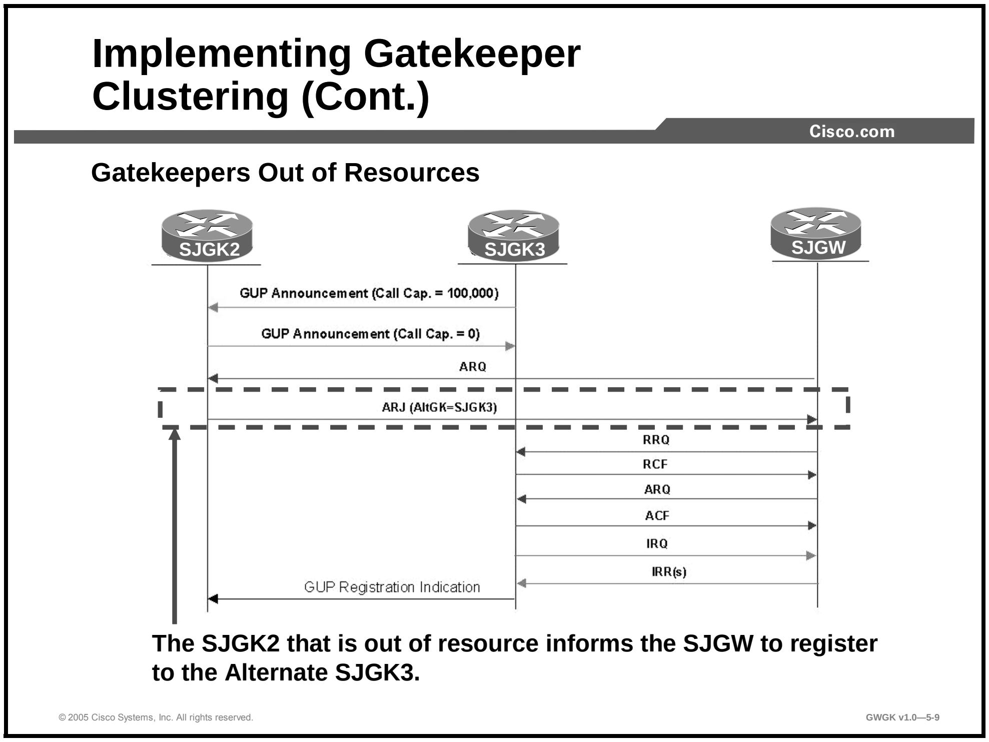
The following output shows the configuration for defining a local and a remote cluster:

```
Router(config-gk)#zone local RTPGK1 cisco.com 172.18.193.150
1719

Router(config-gk)#zone cluster local RTPCluster RTPGK1

Router(config-gk_cluster)#element RTPGK2 172.18.193.151 1719

Router(config-gk_cluster)#element RTPGK3 172.18.193.152 1719

Router(config-gk)#zone cluster remote SJCluster cisco.com cost
10 priority 20

Router(config-gk_cluster)#element SJGK1 161.18.79.23 1719

Router(config-gk_cluster)#element SJGK2 161.18.79.24 1719

Router(config-gk_cluster)#element SJGK3 161.18.79.25 1719

Router(config-gk_cluster)#exit
Router(config-gk)#zone prefix SJCluster 408*
```

This configuration defines a local cluster and specifies two alternates to that cluster. It also defines a remote cluster composed of three gatekeepers and associates a cost and priority to the cluster as a whole.

Note that a cluster member such as San Jose Gatekeeper 1 (shown as SJGK1 in the example) may also be defined as a "zone remote" with a different set of prefixes and cost values. In that case, the San Jose Gatekeeper 1 entry in the cluster will be treated as a separate entity than the "zone remote SJGK1".

The prefix associated with the cluster as a whole applies to all the members of the cluster. The local gatekeeper will perform a round robin between the members of the cluster to resolve a 408 call.



Implementing Gatekeeper Clustering (Cont.)

Cisco.com

Gatekeepers Out of Resources

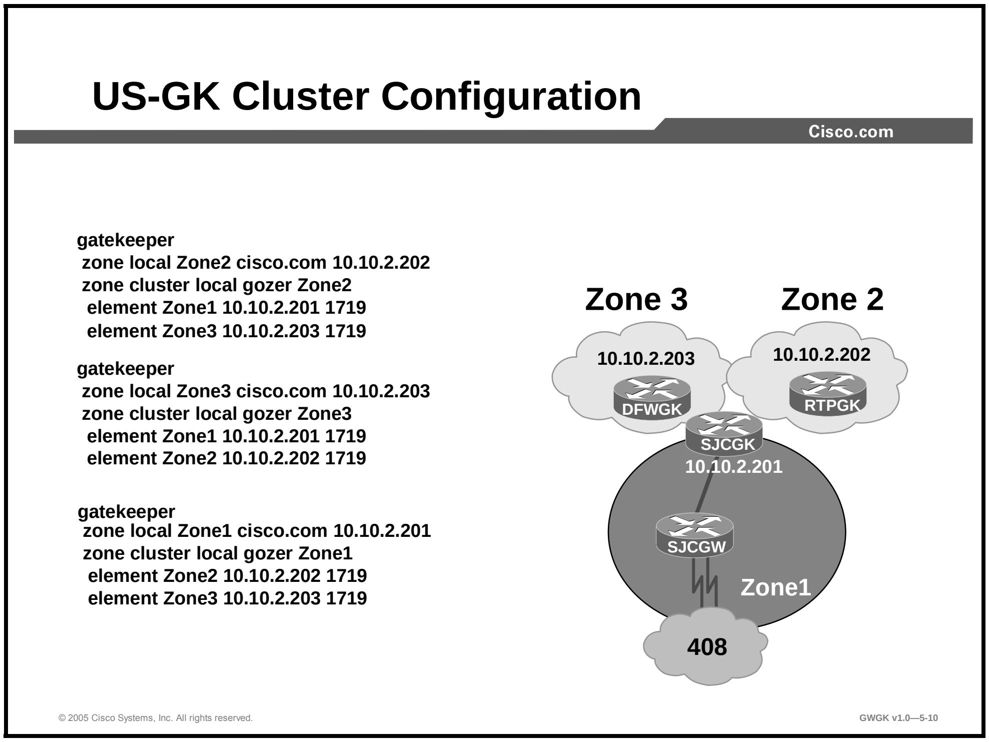
SJGK2
SJGK3
SJGW
GUP Announcement (Call Cap. = 100,000)
GUP Announcement (Call Cap. = 0)
ARQ
ARJ (AltGK=SJGK3)
RRQ
RCF
ARQ
ACF
IRQ
IRR(s)
GUP Registration Indication

The SJGK2 that is out of resource informs the SJGW to register to the Alternate SJGK3.

GWGK v1.0—5-9

Continuing with the previous example, this figure shows gatekeeper clustering at San Jose Gatekeeper 2 and San Jose Gatekeeper 3:

- San Jose Gatekeeper 3 informs San Jose Gatekeeper 2 about its actual call capacity (100,000 kbps) using a GUP announcement.
- San Jose Gatekeeper 2 informs San Jose Gatekeeper 3 about its actual call capacity, which in this case is 0. In other words, San Jose Gatekeeper 2 is experiencing a heavy load, but San Jose gatekeeper 3 is not.
- San Jose Gateway sends an ARQ to its primary gatekeeper. Although this gateway is registered with San Jose Gatekeeper 2, it is aware of the alternate gatekeepers.
- San Jose Gatekeeper 2 informs San Jose Gateway to use another gatekeeper by using the following message: ARJ I(AltGK=SJGK3). Note that this is a nonstandard ARJ message, which means that not all standard gateways support this feature. It is supported by Cisco gateways and Cisco CallManager v3.3 and later.
- The San Jose Gateway reregisters to San Jose Gatekeeper 3 and then asks for E.164 resolution via an ARQ message.
- San Jose Gatekeeper 3 informs other members of the cluster about the new registration using the GUP registration indication message.



US-GK Cluster Configuration

Cisco.com

```
gatekeeper
 zone local Zone2 cisco.com 10.10.2.202
 zone cluster local gozer Zone2
  element Zone1 10.10.2.201 1719
  element Zone3 10.10.2.203 1719

gatekeeper
 zone local Zone3 cisco.com 10.10.2.203
 zone cluster local gozer Zone3
  element Zone1 10.10.2.201 1719
  element Zone2 10.10.2.202 1719

gatekeeper
 zone local Zone1 cisco.com 10.10.2.201
 zone cluster local gozer Zone1
  element Zone2 10.10.2.202 1719
  element Zone3 10.10.2.203 1719
```

GWGK v1.0—5-10

This example shows a small configuration where three gatekeepers are forming a cluster. The San Jose Gateway is a member of Zone 1 that registers to the San Jose Gatekeeper. Gateways registered to each gatekeeper in the cluster will receive a list of IP address of the other gatekeepers for backup. No configuration is need in the gateways.

The gateways in Zone 2 that are registered with the Zone 2 gatekeeper, will use Zone 1 first if Zone2 gatekeeper is out of service or becomes overloaded. Zone 3 is the second in priority after Zone2.

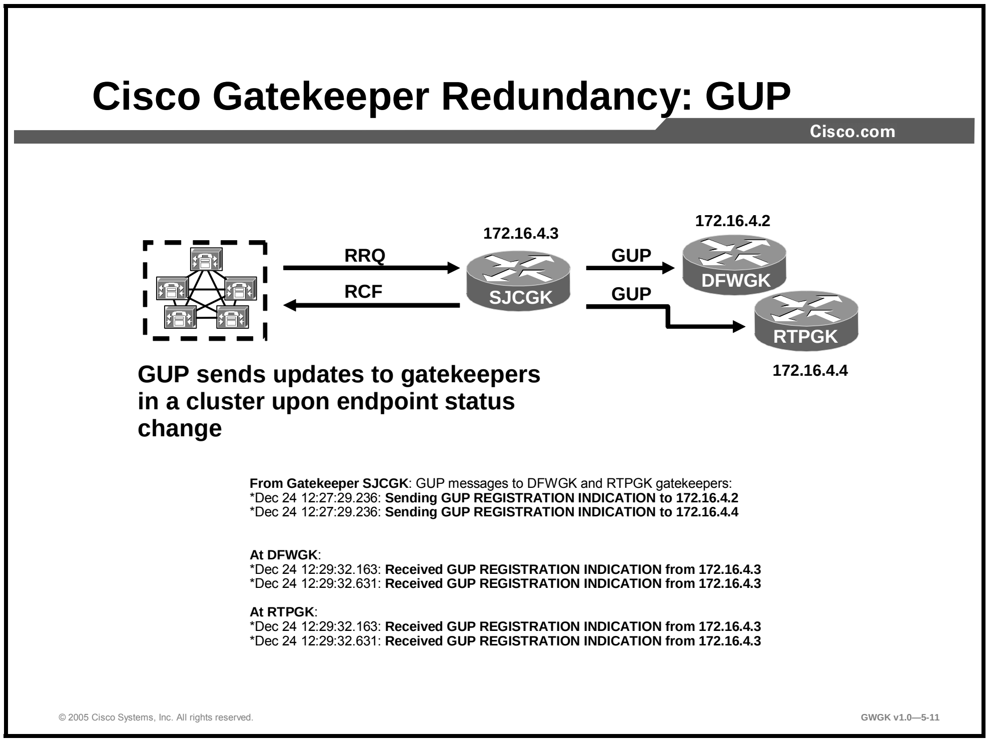
The following configuration shows what a local and remote gatekeeper clustering configuration looks like. A gateway registered to RTP Gatekeeper 1 will use the local gatekeepers in order as listed for backup before the gateway tries to register with the remote gatekeepers.

This is a sample configuration of RTP Gatekeeper 1 clustered with local gatekeepers and remote gatekeepers:

```
gatekeeper
 zone local RTPGK1 cisco.com
 zone cluster local RTPCluster RTPGK1
  element RTPGK2 209.165.200.101 1719
  element RTPGK3 209.165.200.102 1719
 zone cluster remote SJCCluster cisco.com
  element SJCGK1 209.18.79.23 1719
  element SJCGK2 209.18.79.24 1719
  element SJCGK3 209.18.79.25 1719
```

This is a sample configuration of San Jose Gatekeeper 1 clustered with local gatekeepers and remote gatekeepers

```
gatekeeper
 zone local SJCGK1 cisco.com
 zone cluster local SJCCluster SJCGK1
  element SJCGK2 209.18.79.24 1719
  element SJCGK3 209.18.79.25 1719
  zone cluster remote RTPCluster Cisco.com
   element RTPGK2 209.165.200.101 1719
   element RTPGK3 209.165.200.102 1719
```



Cisco Gatekeeper Redundancy: GUP

GUP sends updates to gatekeepers in a cluster upon endpoint status change

```
From Gatekeeper SJCGK: GUP messages to DFWGK and RTPGK gatekeepers:
*Dec 24 12:27:29.236: Sending GUP REGISTRATION INDICATION to 172.16.4.2
*Dec 24 12:27:29.236: Sending GUP REGISTRATION INDICATION to 172.16.4.4

At DFWGK:
*Dec 24 12:29:32.163: Received GUP REGISTRATION INDICATION from 172.16.4.3
*Dec 24 12:29:32.631: Received GUP REGISTRATION INDICATION from 172.16.4.3

At RTPGK:
*Dec 24 12:29:32.163: Received GUP REGISTRATION INDICATION from 172.16.4.3
*Dec 24 12:29:32.631: Received GUP REGISTRATION INDICATION from 172.16.4.3
```

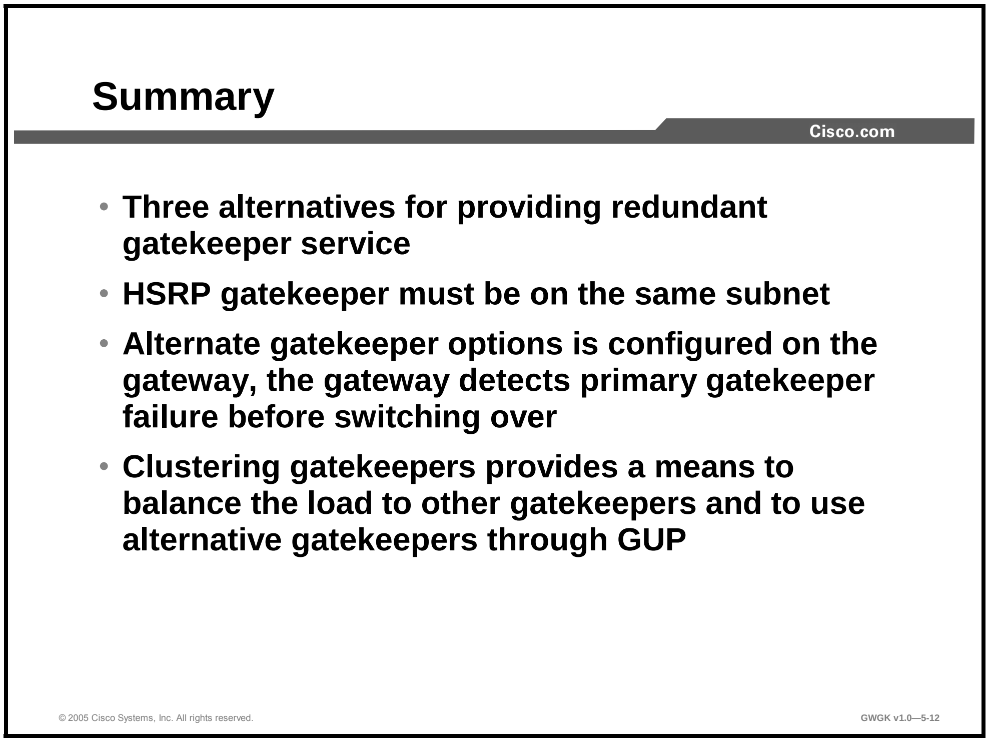
GWGK v1.0—5-11

When an endpoint registers with its primary gatekeeper, GUP messages are sent out to the elements within the cluster that have the registration information and the status of the endpoint.

In the example in the figure, the San Jose Gatekeeper receives a RRQ from the local Cisco CallManager cluster and returns a RCF with a list of all the other gatekeepers in cluster. After the RCF, the San Jose Gatekeeper sends a GUP message entered on all the gatekeepers to its elements, as indicated in this figure.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

Cisco.com

- Three alternatives for providing redundant gatekeeper service
- HSRP gatekeeper must be on the same subnet
- Alternate gatekeeper options is configured on the gateway, the gateway detects primary gatekeeper failure before switching over
- Clustering gatekeepers provides a means to balance the load to other gatekeepers and to use alternative gatekeepers through GUP

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—5-12

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 limitation on alternate gatekeepers is that only ____ can be considered for backup. (Source:)

A) two gatekeepers
B) one gatekeeper
C) three gateways and two gatekeepers
D) two gatekeepers and one primary

Q2) When gatekeepers use HSRP, they must be on the same_____. (Choose three.) (Source:)

A) subnet
B) version of IOS
C) platform
D) separate subnets

Q3) To define a backup gatekeeper, what command on the gateway indicates the backup? (Source:)

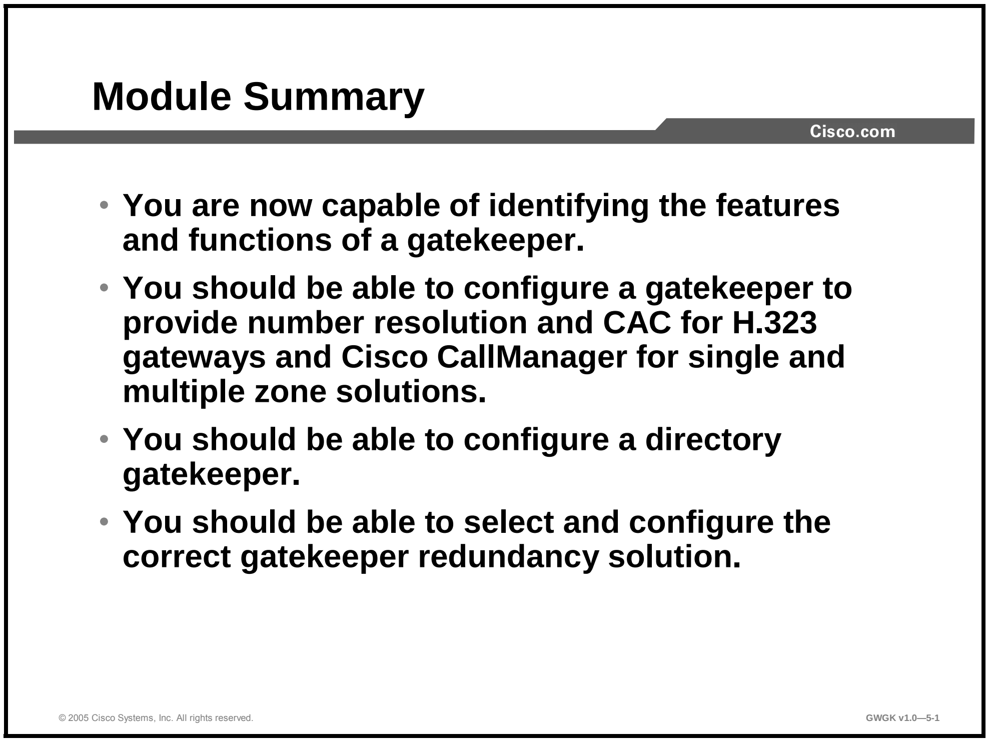
A) **h323-gateway voip id GKSJ ipaddr 172.19.49.168. priority 1**
B) **h323-gateway voip id GKDFW ipaddr 10.10.49.168 priority 2**
C) **h323-gateway voip id alternateGK ipaddr 10.10.49.168**
D) **h323-gateway voip h323-id Backup**

Lesson Self-Check Answer Key

Q1)	D
Q2)	A, B, C
Q3)	B

Module Summary

This topic summarizes the key points discussed in this module.



Module Summary

Cisco.com

- You are now capable of identifying the features and functions of a gatekeeper.
- You should be able to configure a gatekeeper to provide number resolution and CAC for H.323 gateways and Cisco CallManager for single and multiple zone solutions.
- You should be able to configure a directory gatekeeper.
- You should be able to select and configure the correct gatekeeper redundancy solution.

GWGK v1.0—5-1

This module discussed what functions gatekeepers provide, how these devices signal endpoints, and how gatekeepers provide a means for redundancy. Knowing how to manage gatekeepers and configure these devices are very important in an H323 converged network.

References

For additional information, refer to these resources:

- *Gatekeeper Alias Registration and Address Resolution Enhancements*. http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00800b5d3a.html.
- *Understanding H.323 Gatekeepers*. http://www.cisco.com/en/US/tech/tk652/tk701/technologies_tech_note09186a00800c5e0d.shtml#protosuite.
- *Understanding Cisco IOS H.323 Gatekeeper Call Routing*. Implementing Cisco Voice Gateways and Gatekeepers (GWGK) v1.0http://www.cisco.com/warp/public/788/voip/gk-call-routing.pdf.
- *Configuring H.323 Gatekeepers and Proxies*. http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/323confg/5gkconf.htm
- *Understanding Cisco IOS Software Gatekeeper Call Routing*. http://www.cisco.com/en/US/tech/tk652/tk701/technologies_tech_note09186a00800a8928.shtml.

- *Configuring H323 Gateways*. http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/323confg/4gwconf.htm#wp1124639.
- *Designing a Scaleable Dial Plan*. http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/dp3_isd.htm
- *Configuring Gatekeepers and Proxies*. http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_configuration_guide_chapter09186a00802b460c.html.
- *Configuring an Anonymous Device Gatekeeper with Cisco CallManager Versions 3.3 and 4.1*. http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_configuration_example09186a0080169445.shtml.
- *Gateway Configuration*. http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00801f00ed.html#wp1183281.
- *H.323 Technical Details and Documentation*. http://www.cisco.com/en/US/tech/tk652/tk701/tk309/tech_protocol_home.html.
- *Cisco IP Telephony Solution Reference Network Design (SRND) for Cisco CallManager 4.0*. http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a00802c370c.html.
- *Cisco IOS Software Library 12.3 T*. http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vcl.htm.
- *Cisco IOS Software Library 12.3 T H.323 Gateway Configuration*. http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/323confg/index.htm.

Module 6

Introducing Service Provider Offerings

Overview

This module describes the various service provider offerings and what the topologies of those offerings look like. The module also discusses the various managed and hosted IP telephony solutions offered by service providers, including what problem these solutions solve and how to integrate the solution into a Cisco CallManager environment. The module presents the Cisco multiservice IP-to-IP gateway, gateway configuration examples, and some deployment best practices for the IP telephony solutions.

Module Objectives

Upon completing this module, you will be able to describe common service provider offerings such as wholesale voice and IP Centrex and describe how an IP-to-IP gateway supports these offerings. This ability includes being able to meet these objectives:

- Describe the common types of service provider offerings available to residential customers and enterprise clients
- Describe the requirements for deploying Cisco Multiservice IP-to-IP Gateways in a service provider environment

Lesson 1

Understanding Service Provider Offerings

Overview

This lesson introduces the various IP telephony services that service providers offer to residential customers and enterprise clients. This lesson will discuss various components of these services and how the services are deployed.

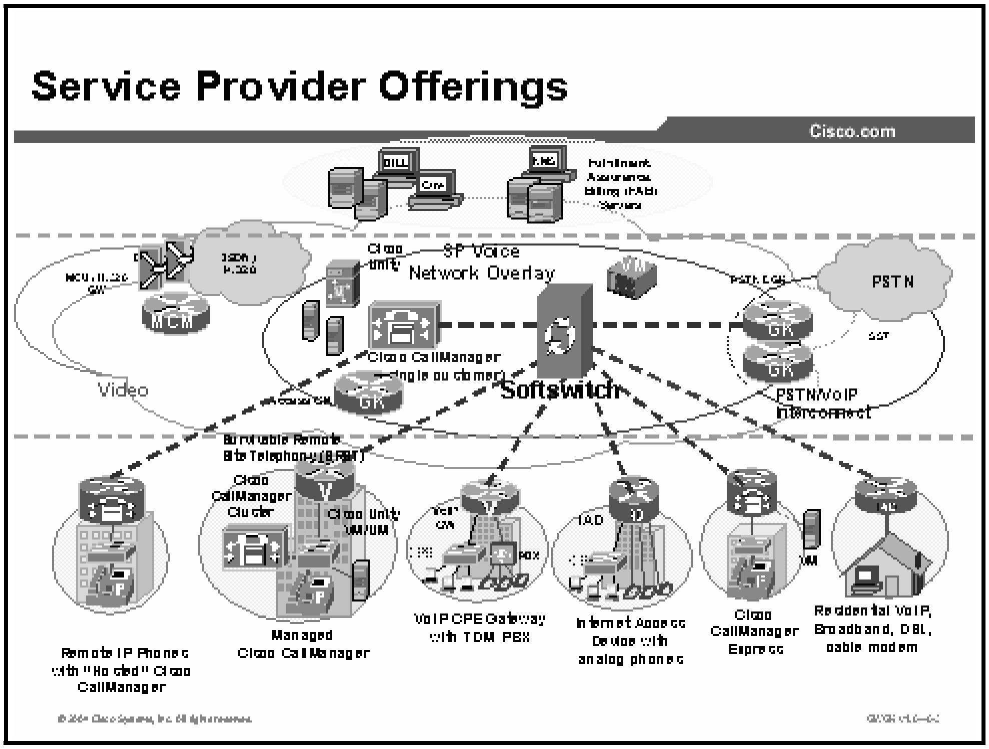
Objectives

Upon completing this lesson, you will be able to describe the common types of service provider offerings available to residential customers and enterprise clients. This ability includes being able to meet these objectives:

- Describe the IP-based communications services being offered by service providers
- Describe service provider IP Centrex services
- Describe service provider IP PSTN services
- Describe service provider residential VoIP services
- Describe service provider calling card services
- Describe service provider wholesale voice

Service Provider Offerings

This topic describes common service provider offerings such as hosted and managed IP telephony services.

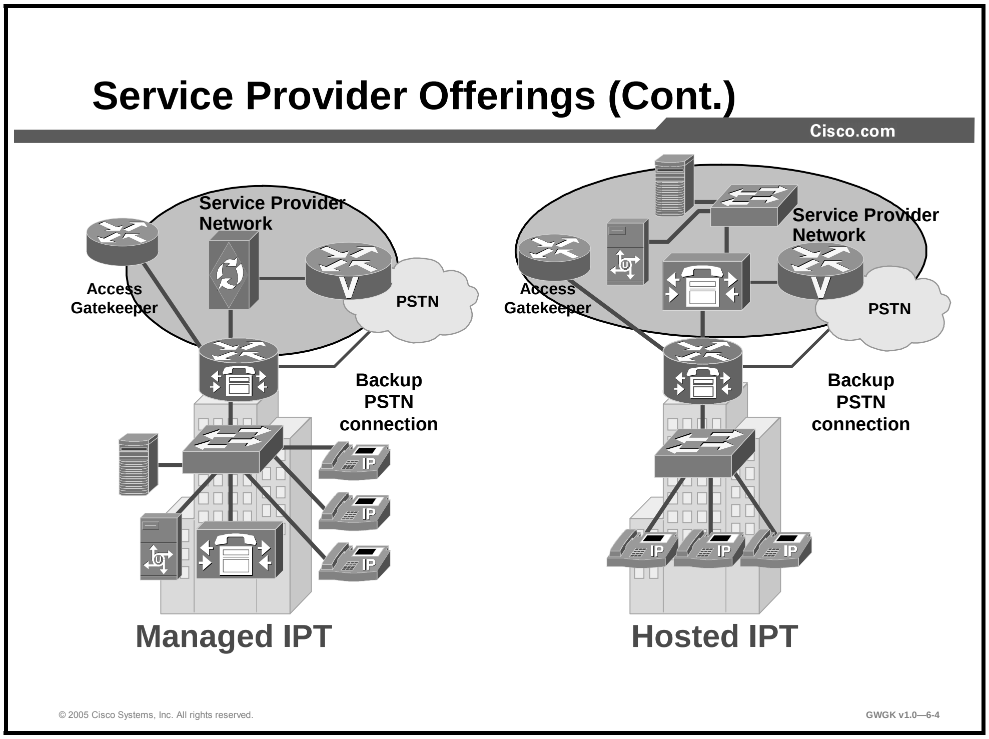


Service Provider Offerings

Cisco.com

BILL
CRM
NMS
Fulfillment, Assurance, Billing (FAB) Servers
MCU, H.320 GW
ISDN / H.320
MCM
Cisco Unity
SP Voice Network Overlay
VM
PSTN GWs
PSTN
SS7
GK
GK
Cisco CallManager (single or cluster)
Softswitch
Video
Access GK
GK
PSTN/VoIP Interconnect
Survivable Remote Site Telephony (SRST)
Cisco CallManager Cluster
Cisco Unity VM/UM
VoIP GW
PBX
IAD
VM
Remote IP Phones with "Hosted" Cisco CallManager
Managed Cisco CallManager
VoIP CPE Gateway with TDM PBX
Internet Access Device with analog phones
Cisco CallManager Express
Residential VoIP, Broadband, DSL, cable modem

This figure shows some common IP telephony services offered by a service provider. The first type of service is a hosted IP telephony service where the service provider manages and administers services in a remote network operations center. The second type of service is the managed service where the service provider manages the IP telephony solution on the client premises. There is a third type of service that is less of a service provider solution and more of a situation of service provider involvement. This situation is where the client hosts the traditional PBX equipment, and the service provider may provide telephony services such as voice mail or automatic call distribution (ACD) services for the client.

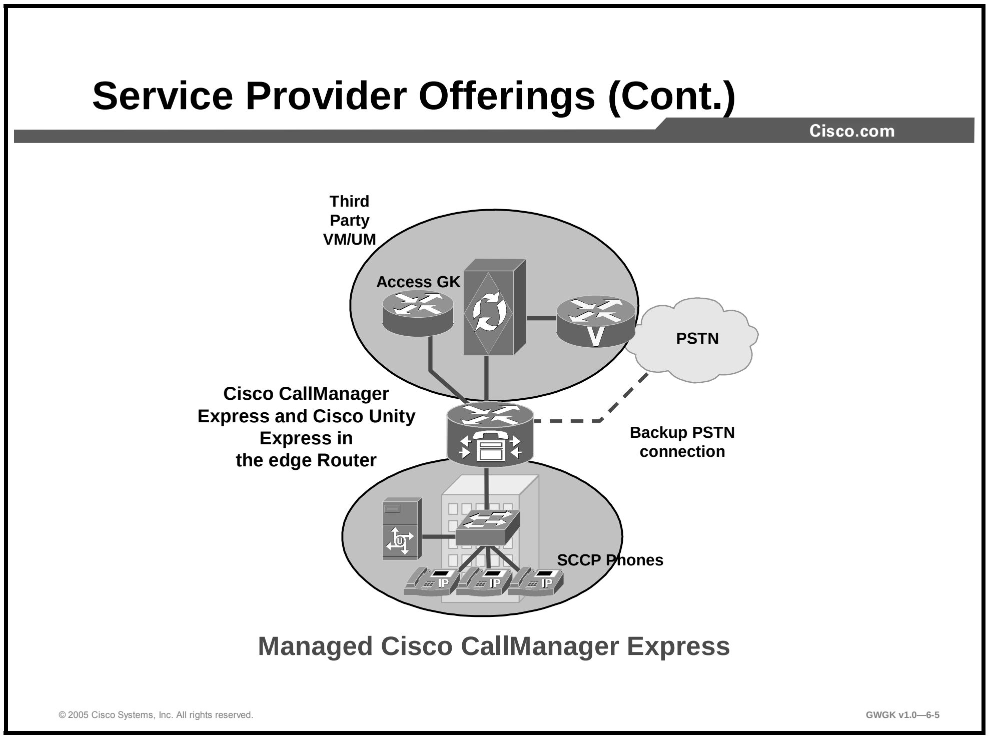


Service Provider Offerings (Cont.)

GWGK v1.0—6-4

This figure shows examples of both managed and hosted IP telephony solutions. In these two examples, note where the equipment resides.

IP telephony equipment resides in the service provider cloud of hosted solutions and is administered by the provider. Conversely, IP telephony equipment typically resides on the client premises in a managed IP telephony solution and is ether administered by the provider of the equipment or by the client staff. An example of a managed solution situation is one in which a client requires a large number of moves, adds, and changes relative to IP telephony, but the client rents the equipment and the service provider is responsible for all changes to and configurations of that equipment. Connectivity to the client premises is typically by way of gigabit Ethernet, fast Ethernet, optical transport, cable services, or high-speed serial interface.



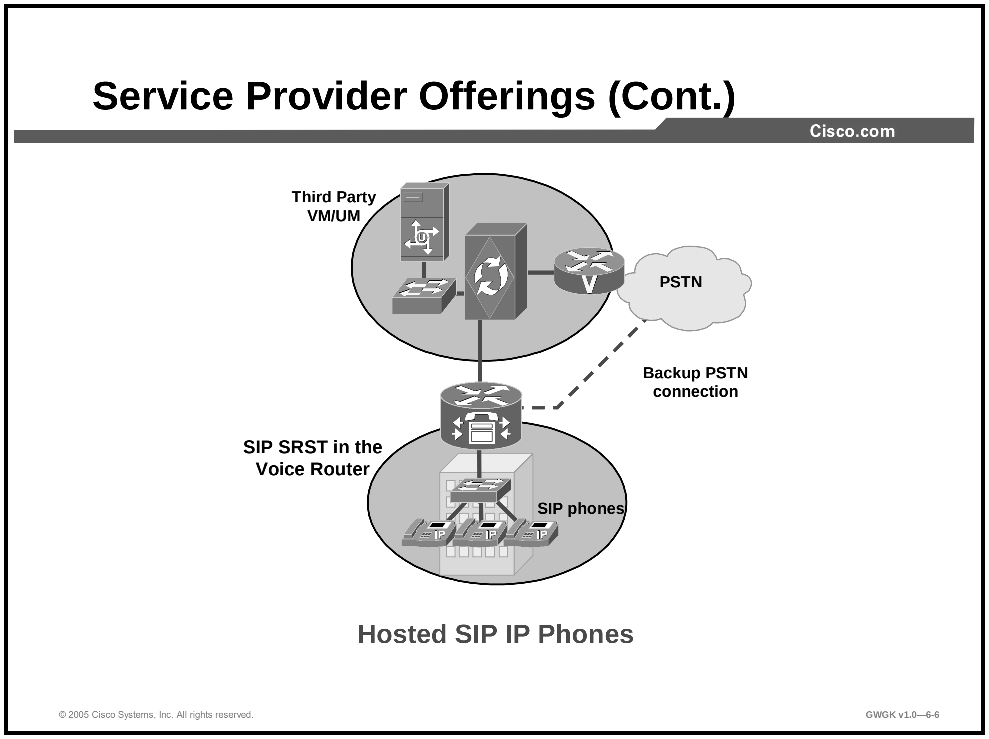
Service Provider Offerings (Cont.)

Cisco.com

Managed Cisco CallManager Express

GWGK v1.0—6-5

This figure shows an example of a Cisco CallManager Express solution managed by either the provider or client staff. A service-provider solution could consist of backup services to the public switched telephone network (PSTN) and to the service-provider network.

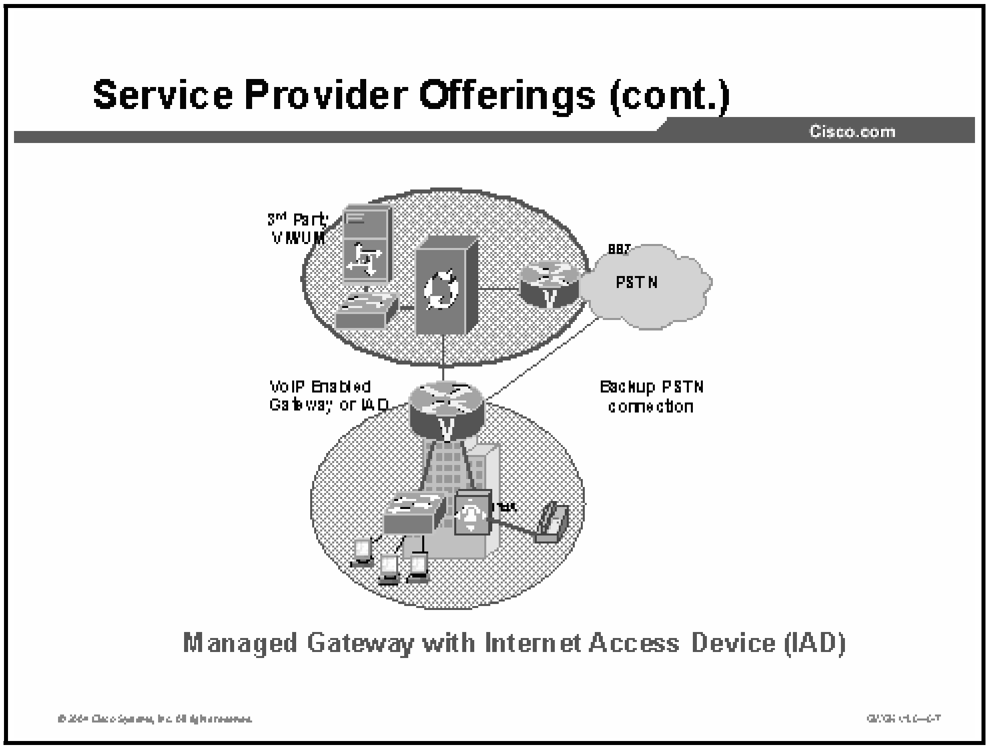


Service Provider Offerings (Cont.)

Hosted SIP IP Phones

GWGK v1.0—6-6

This figure shows an example of a hosted IP telephony service where the service provider manages and administers the solution within its own network. Similar to the managed solution, a hosted solution could consist of backup services for both PSTN voice traffic and data-services traffic.



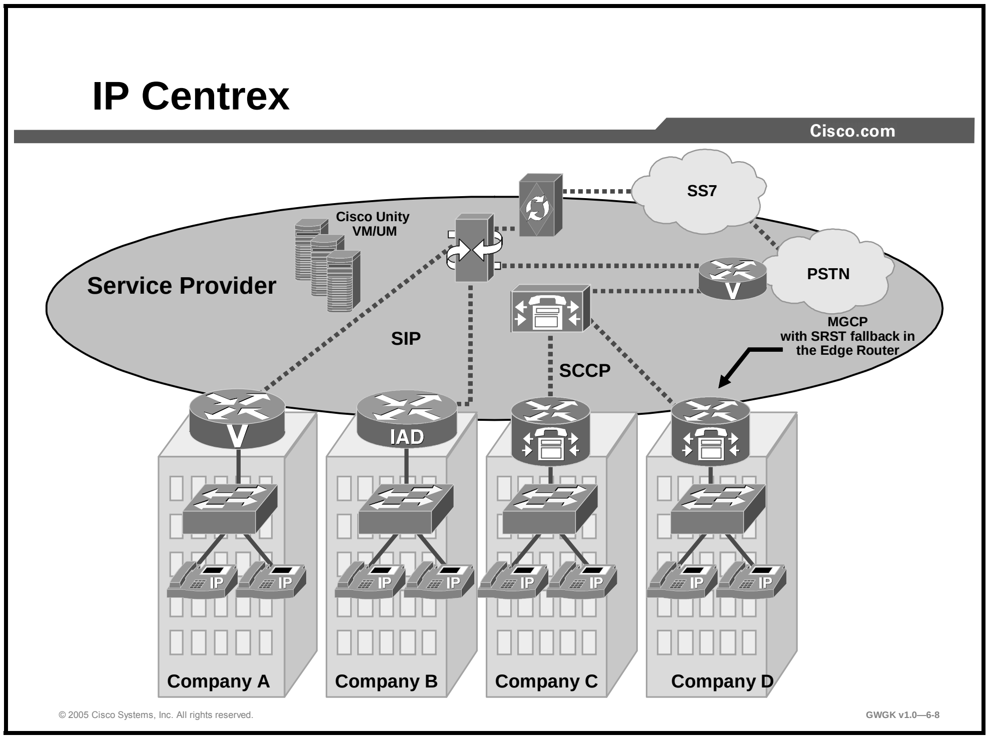
Service Provider Offerings (cont.)

Managed Gateway with Internet Access Device (IAD)

The figure shows an example of an IP telephony solution where the service provider offers hosted IP telephony for those services the client needs but cannot afford, such as unified messaging servers. In a solution like this one, the client hosts most of the IP telephony equipment onsite and either owns the equipment or rents it from the provider. The example shows that the service provider offers a managed gateway with an integrated access device (IAD).

IP Centrex

This topic describes IP Centrex services.



IP Centrex

Cisco.com

© 2005 Cisco Systems, Inc. All rights reserved.

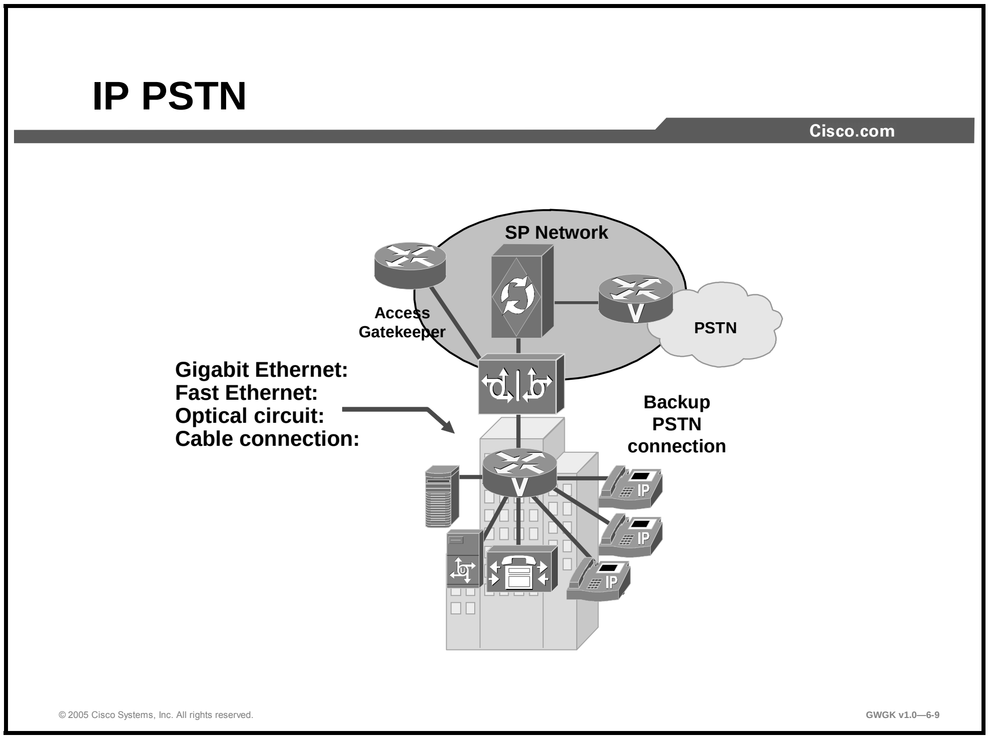
GWGK v1.0—6-8

IP Telephony also can be provided as a hosted service from a shared server housed by the service provider, an approach sometimes referred to as IP Centrex. This figure shows a typical IP Centrex scenario where autonomous clients rent Centrex-like services like conferencing, call waiting, and call forwarding, as well as enhanced services like auto attendant, voice mail, and selective call forwarding, from the service provider. New business owners, in particular, may find this to be an affordable solution. The IP Centrex service is compelling to business customers because they can take advantage of feature-rich voice services while reducing operational and capital costs. Service providers, for their part, retain their existing Centrex customer base, can expand into new markets that historically have been served by traditional PBX or key systems, and can reduce capital expenditure and operational expenditure by shifting Centrex services from a Class 5 switch to an IP Centrex application server.

IP Centrex is an attractive alternative to customer premises-based PBX systems. The service provider hosts the feature set for IP PBX, Unified Communications, and integrated management in its central office or data center where multiple business customers can share it. Their business customers gain access to commonly-used subscriber and group-level Centrex features, which includes valued-added capabilities such as self-provisioning of services; direct management of moves, adds, and changes; integration of instant messaging; video; click to conference; directory services; unified communications; virtual assistants; and others.

IP PSTN

This topic describes IP PSTN services.



IP PSTN

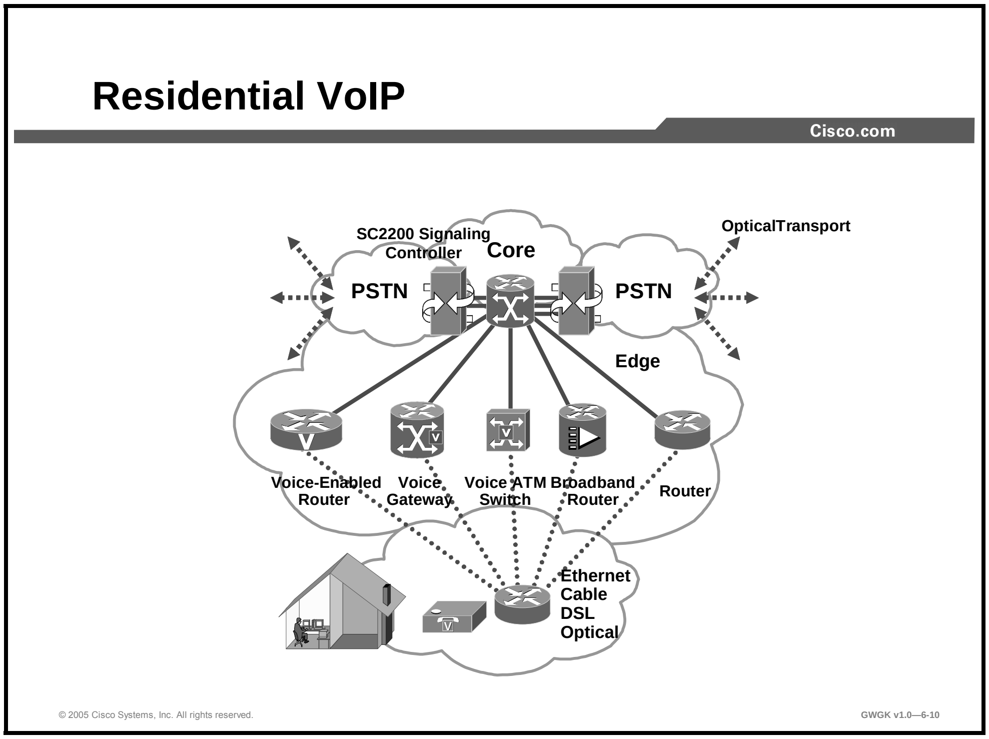
Cisco.com

GWGK v1.0—6-9

The term IP PSTN is used for those clients who use something other than time-division multiplexing (TDM) service connectivity for voice traffic to the PSTN. Moreover, IP PSTN is a term used where the provider offers voice traffic porting over gigabit Ethernet, fast Ethernet, optical transport, or cable services through the provider network to the PSTN. Conversely, all incoming voice traffic to the client site is passed from the PSTN through the provider network to the client over those circuits.

Residential VoIP

This topic describes residential VoIP.



Residential VoIP

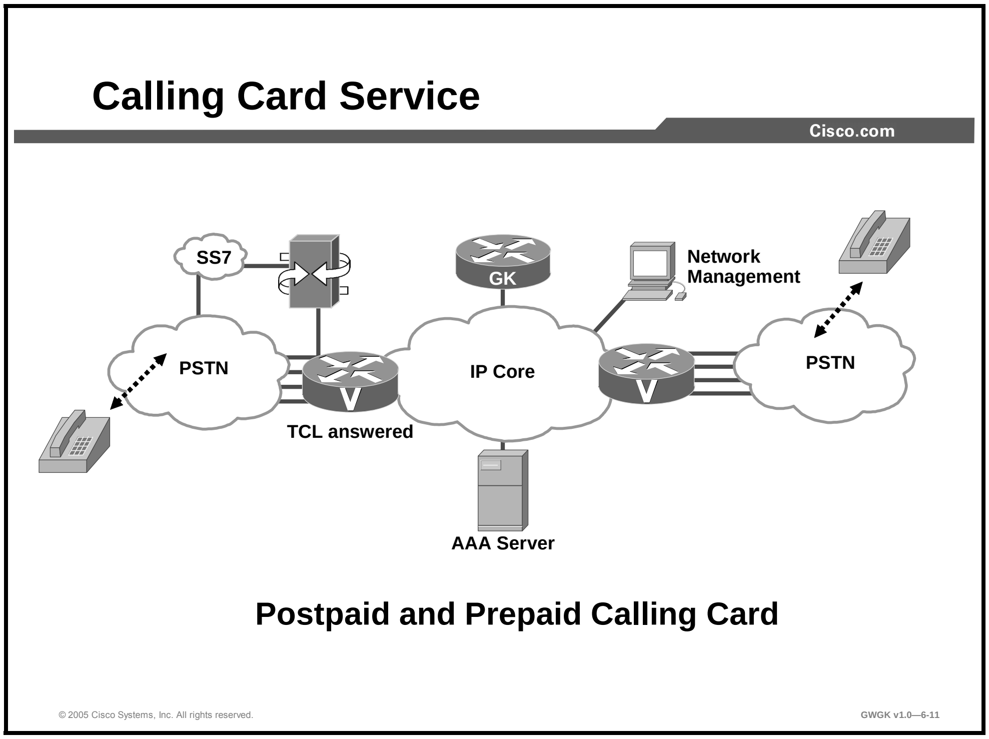
Cisco.com

GWGK v1.0—6-10

There are many solutions offered by service providers for residential clients, the most popular of which have been cable modem and DSL services. Some service provides have the capability to bring optical services to the home. Dial-up services are becoming less popular except for in certain geographical areas of the world where the service provider infrastructure cannot support advanced technologies. The figure illustrates that service providers can offer various technologies to meet residential voice and data needs.

Calling Card Services

This topic describes prepaid and postpaid calling card services.



Calling Card Service

Cisco.com

Postpaid and Prepaid Calling Card

GWGK v1.0—6-11

Another solution service providers offer is prepaid and postpaid calling-card solutions. These services can be offered under retail or wholesale models. Most prepaid calling-card service offerings take advantage of the wholesale model, under which the wholesale carrier manages the card service on its international infrastructure. The retail service provider then brands and markets the card service to the end user. For both prepaid and postpaid card services, a packet telephony wholesaler offers services identical to that offered by PSTN wholesalers. For example, packet telephony calling card services supply an interactive voice response (IVR) capability to direct the caller through the call process. The IVR prompts the exchange of a personal identification number (PIN) and a dialing destination number, and it alerts the user of the remaining balance on a prepaid card. The calling-card solution must offer authorization, authentication, call rating, accounting, and prepaid service disconnection when a card reaches its expiration point.

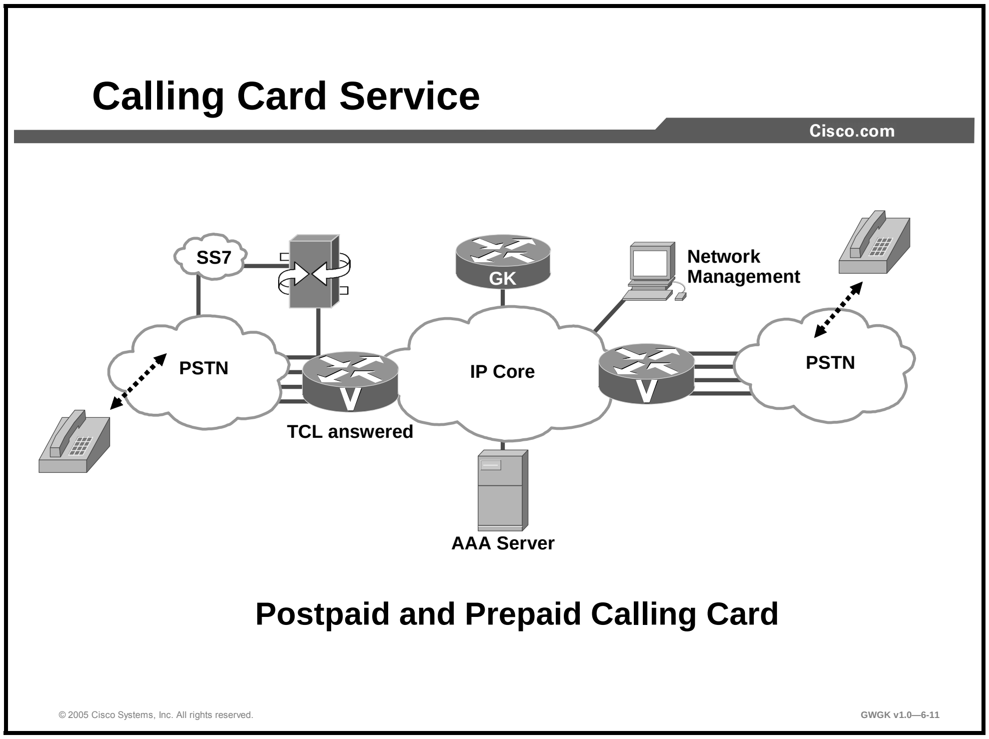
Postpaid calling-card services offer subscribers ongoing access to the long-distance network. As with prepaid calling cards, the postpaid service is often hosted by a wholesale carrier to improve profitability. The main difference between prepaid and postpaid calling-card services is that service authorizations under the postpaid model are not tied to call rating and services do not expire (except in the case of a limited-credit postpaid service). Wholesalers bill their carrier customers after calls have been made and the carriers in turn bill their end users.

The Cisco prepaid and postpaid calling card services include the following:

- IVR capabilities, including support of standard voice extensible markup language (VXML) automated speech recognition (ASR) and text-to-speech (TTS) capabilities for increased customer service satisfaction
- A telephony user interface similar to familiar card services applications on the PSTN
- Support for multiple languages and multicompany brandings or announcement messages on the same network
- Card recharging, balance transfer, and PIN change

Wholesale Voice Services

This topic describes wholesale voice services.



Calling Card Service

Cisco.com

Postpaid and Prepaid Calling Card

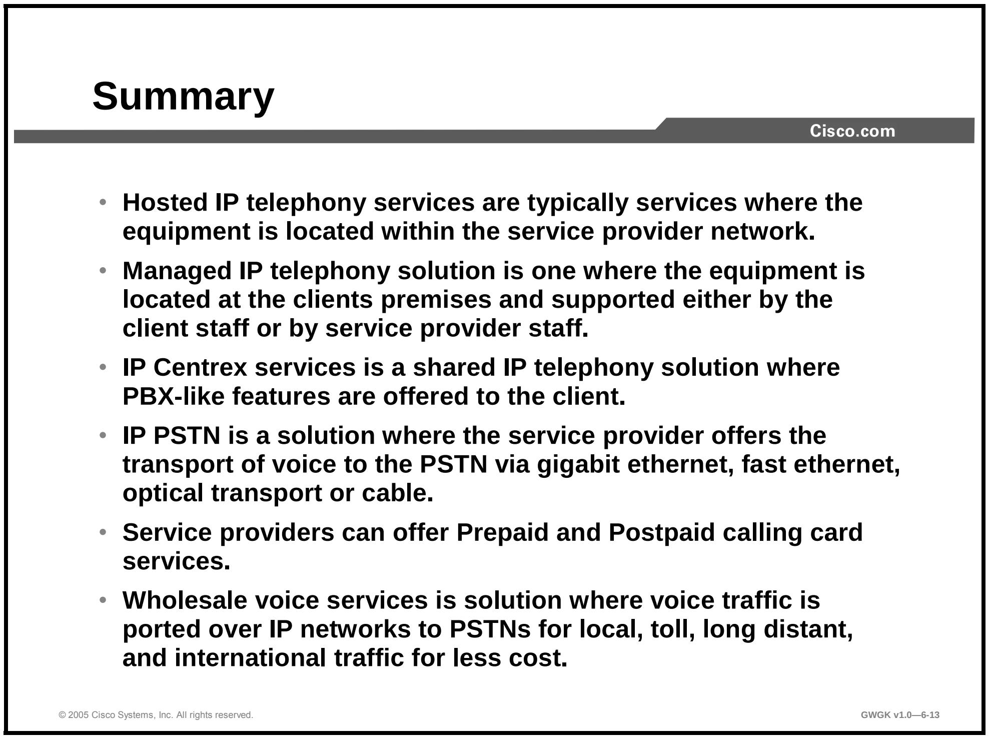
GWGK v1.0—6-11

Voice points of presence (POPs), which are interconnected to other service providers, are central to the delivery of wholesale voice services. The specific recommended components and design methods are determined by the type of interconnection or "call topology" that the wholesale service provider is supporting. These call topologies are used to build a set of deployment templates for a service provider to enable wholesale applications.

This figure shows a simple example of a wholesale voice network and its components, including Signaling System 7 (SS7), Toolkit Command Language (TCL), and an authentication, authorization, and accounting (AAA) server. The Cisco Wholesale Voice Solution is a set of solutions and network designs and configurations that provide the transport of global switched telephone traffic distributed over VoIP network. For example, in this figure, calls originating in the PSTN could be routed through inter-exchange carriers (IXCs) and handed off to a wholesale VoIP carrier for transport. To the end user, the service looks like any other long-distance call except that the call is less expensive. To the originating long-distance carrier, the wholesale carrier is only one of a number of termination options. Wholesale voice solutions are usually deployed to offer a lower cost telephony service to the end user.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

Cisco.com

- Hosted IP telephony services are typically services where the equipment is located within the service provider network.
- Managed IP telephony solution is one where the equipment is located at the clients premises and supported either by the client staff or by service provider staff.
- IP Centrex services is a shared IP telephony solution where PBX-like features are offered to the client.
- IP PSTN is a solution where the service provider offers the transport of voice to the PSTN via gigabit ethernet, fast ethernet, optical transport or cable.
- Service providers can offer Prepaid and Postpaid calling card services.
- Wholesale voice services is solution where voice traffic is ported over IP networks to PSTNs for local, toll, long distant, and international traffic for less cost.

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—6-13

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) Shared IP telephony PBX-like features are considered to be what kind of IP service? (Source:)

A) Managed services
B) IP Centrex
C) IP PSTN
D) IP telephony equipment at the client premises

Q2) If a client requires that a service provider support and administer IP telephony at the client premises, which type of service would the client choose? (Source:)

A) Equipment that is located within the service provider network
B) Multiservice services
C) Managed services
D) Hosted services

Q3) If the client needs the service provider to support and administer IP telephony at the service provider premises, which type of service would the client choose? (Source:)

A) Equipment that is located within the service provider network
B) Multiservice services
C) Managed services
D) Hosted services

Q4) Which type of service provides low-cost long-distance voice services over an IP network with interconnection to the PSTN? (Source:)

A) Equipment that is located within the service provider network
B) Multiservice services
C) Wholesale voice services
D) Hosted services

Q5) What are the most common residential VoIP solutions? (Source:)

A) DSL, cable, and optical
B) Cable, DSL, and dial up
C) Cable and dial up
D) DSL and cable modems

Lesson Self-Check Answer Key

Q1)	B
Q2)	C
Q3)	D
Q4)	C
Q5)	D

Lesson 2

Cisco Multiservice IP-to-IP Gateway

Overview

In the current VoIP market, Internet telephony service providers (ITSPs) that provide wholesale VoIP services use their own IP-to-time-division multiplexing (TDM) gateways to exchange calls with the PSTN. Problems occur when a wholesaler receives a call from an originating ITSP and terminates the call to another ITSP. In this case, because the service provider does not own the public switched telephone network (PSTN) gateways, the service provider wholesaler does not receive call setup or release information and therefore cannot bill for the call. Wholesalers are forced either to forbid these connections, thereby foregoing a potential revenue source, or to set up the call through a combination of back-to-back IP-to-TDM gateways. This solution results in reduced quality due to double media coding and decoding, and it wastes TDM port resources. The Cisco Multiservice IP-to-IP Gateway IOS feature allows the wholesaler to terminate the call from the originating ITSP and then reoriginate it, thereby providing a point at which accurate call detail records (CDRs) can be collected for billing.

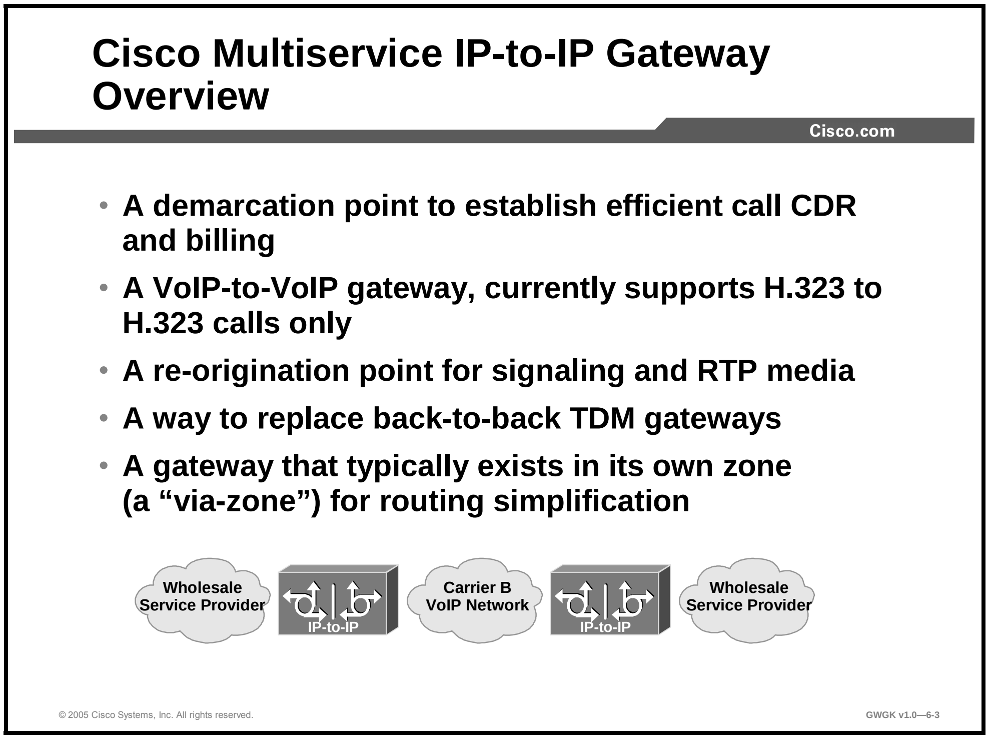
Objectives

Upon completing this lesson, you will be able to describe the requirements for deploying Cisco Multiservice IP-to-IP Gateways in a service provider environment. This ability includes being able to meet these objectives:

- Describe the functionality of Cisco Multiservice IP-to-IP Gateway
- Design a Cisco Multiservice IP-to-IP Gateway solution using accepted best practices
- Describe the signaling between Cisco Multiservice IP-to-IP Gateway and Cisco gatekeepers
- Discuss the requirements for integrating Cisco Multiservice IP-to-IP Gateway with Cisco CallManager
- Describe fax, modem, and DTMF requirements on a Cisco Multiservice IP-to-IP Gateway
- Configure Cisco Multiservice IP-to-IP Gateway

Cisco Multiservice IP-to-IP Gateway Overview

This topic describes the Cisco Multiservice IP-to-IP Gateway.



Cisco Multiservice IP-to-IP Gateway Overview

Cisco.com

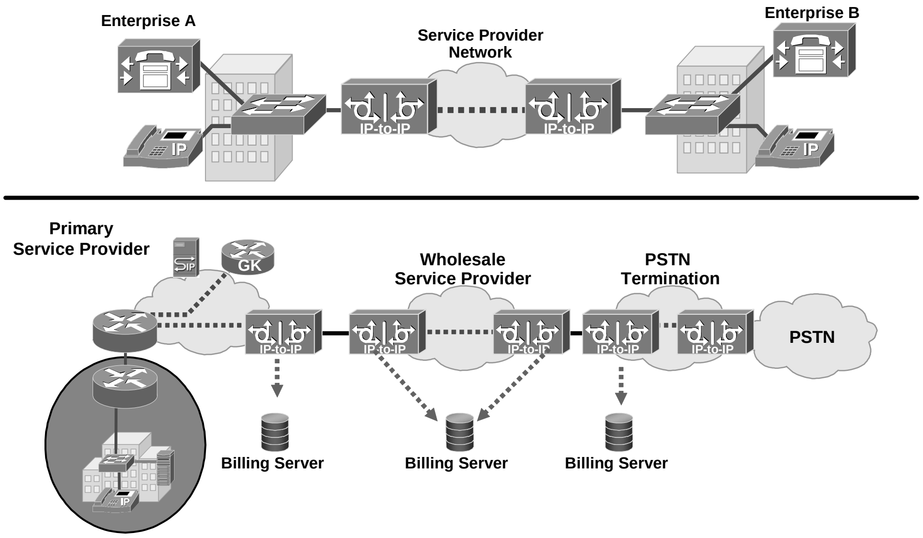
- **A demarcation point to establish efficient call CDR and billing**
- **A VoIP-to-VoIP gateway, currently supports H.323 to H.323 calls only**
- **A re-origination point for signaling and RTP media**
- **A way to replace back-to-back TDM gateways**
- **A gateway that typically exists in its own zone (a “via-zone”) for routing simplification**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—6-3

The Cisco Multiservice IP-to-IP Gateway acts as a demarcation point in establishing efficient CDRs and billing and is a reorigination point for signaling and Real-Time Transport Protocol (RTP) media. As a VoIP-to-IP gateway, it currently supports H.323-to-H.323 calls only. The Cisco Multiservice IP-to-IP Gateway provides service providers with a way to replace back-to-back TDM gateways. Typically, it exists in its own zone (a “via-zone”) for routing simplification.

Cisco Multiservice IP-to-IP Gateway Overview (Cont.)

Cisco.com



GWGK v1.0—6-4

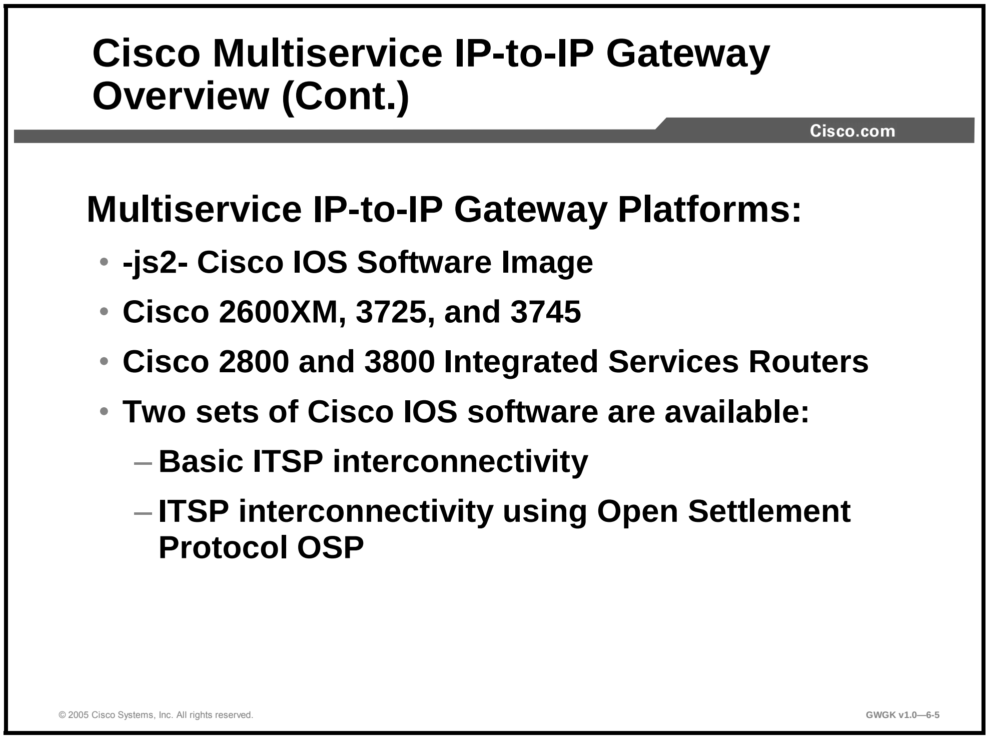
In the current VoIP market, ITSPs that provide wholesale VoIP services use their own IP-to-TDM gateways to exchange calls with the PSTN. Problems occur when a wholesaler receives a call from an originating ITSP and decides to terminate the call to another ITSP. Because it does not own the PSTN gateways, the wholesaler does not receive call setup or release information and therefore cannot bill for the call. Wholesalers are forced either to forbid these connections, thereby foregoing a potential revenue source, or to set up the call through a combination of back-to-back IP-to-TDM gateways. This solution results in reduced quality due to double media coding and decoding, and it wastes TDM port resources. The Cisco Multiservice IP-to-IP Gateway IOS feature allows the wholesaler to terminate the call from the originating ITSP and then reoriginate it, thereby providing a point at which accurate call detail records (CDRs) can be collected for billing.

The interconnect capability provided by the Cisco Multiservice IP-to-IP Gateway enables service providers to conceal their internal network and business relationships while improving Call Admission Control (CAC), flexible routing, and protocol interworking capabilities.

The Cisco Multiservice IP-to-IP Gateway includes the following changes to gateways and gatekeepers to allow IP-to-IP call legs:

- Support for H.323-to-H.323 connection types
- New transparent codec type
- Support for H.323 call capacities
- Introduction of gatekeeper via-zones. Via-zone is a Cisco term for a zone that contains IP-to-IP gateways and via-zone-enabled gatekeepers. A via-zone-enabled gatekeeper is capable of recognizing via-zones and sending traffic to via-zone gateways. Cisco via-zone-enabled gatekeepers include a via-zone command-line interface (CLI) command.

Via-zones are usually located on the edge of an ITSP network and are like a VoIP transfer point, or tandem zone, where traffic passes through on the way to the remote zone destination. Gateways in this zone terminate requested calls and reoriginate traffic to its final destination. Via-zone gatekeepers operate as usual for applications that are not IP-to-IP. Gatekeepers in via-zones support resource management (for example, gateway selection and load balancing) using the Capacities field in the H.323 Version 4 Registration, Admission, and Status (RAS) messages.



Cisco Multiservice IP-to-IP Gateway Overview (Cont.)

Multiservice IP-to-IP Gateway Platforms:

- -js2- Cisco IOS Software Image
- Cisco 2600XM, 3725, and 3745
- Cisco 2800 and 3800 Integrated Services Routers
- Two sets of Cisco IOS software are available:
  - Basic ITSP interconnectivity
  - ITSP interconnectivity using Open Settlement Protocol OSP

GWGK v1.0—6-5

This figure outlines the platforms that support Cisco Multiservice IP-to-IP Gateways. There are two versions of Cisco IOS software for IP-to-IP gateway. The first version is for basic IP-to-IP gateway connectivity and the other version is used with Open Settlement Protocol (OSP), which is a software-based application used by service providers for CDR and billing. The IOS version the IP-to-IP gateways runs on is the js2 IOS version.

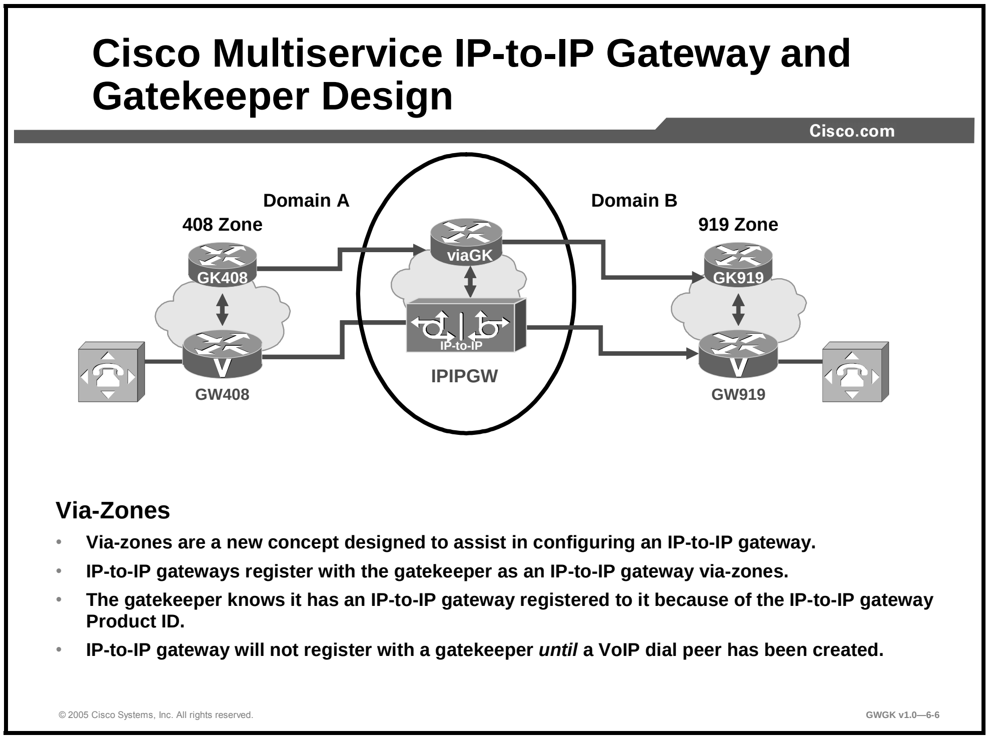
Existing Cisco 2600XM, 2800, 3660, 3745, 3725, and 3800 series router platforms can be used with the later versions of Cisco IOS software for the IP-to-IP gateway. However, the “classic” (non-XM) Cisco 2600 series platforms are not supported, and customers are required to upgrade to Cisco 2600XM Series platforms. Also, note that neither the Cisco 3620 nor the Cisco 3640 series router is supported as an IP-to-IP gateway. Additionally, as of Cisco IOS Software Release 12.3(1)M, all the previously listed platforms require 32 MB Flash memory and 128 MB DRAM.

Two image sets are available for the Cisco Multiservice IP-to-IP Gateway. One set is for basic ITSP-to-ITSP interconnection, and the second set is for ITSP-to-ITSP interconnection through an OSP service provider that is acting as a mediator. The following list describes the features that are included with each set:

- **ITSP-to-ITSP:** H.323 call routing and admission control, network privacy and security, and reliable billing.
- **ITSP-to-ITSP with OSP:** Includes all of the same features as ITSP-to-ITSP plus OSP support with Triple Data Encryption Standard (3DES) encryption. Note that OSP on the IP-to-IP gateway is marketed only with 3DES. Although 56-kbps-encryption is possible with this image, to buy a 3DES-based image, you are sometimes required to obtain special security clearance and to submit a form.

Cisco Multiservice IP-to-IP Gateway and Gatekeeper Design

This topic describes via-zone signaling and how it is configured on multiservice IP-to-IP gateways and gatekeepers.



Cisco Multiservice IP-to-IP Gateway and Gatekeeper Design

Cisco.com

Via-Zones

- Via-zones are a new concept designed to assist in configuring an IP-to-IP gateway.
- IP-to-IP gateways register with the gatekeeper as an IP-to-IP gateway via-zones.
- The gatekeeper knows it has an IP-to-IP gateway registered to it because of the IP-to-IP gateway Product ID.
- IP-to-IP gateway will not register with a gatekeeper *until* a VoIP dial peer has been created.

GWGK v1.0—6-6

Using a Cisco gatekeeper is highly recommended because of the routing, load-balancing, and call-admission capabilities it offers. Cisco gatekeeper release 12.2(13)T3 or later is required for providing all functions of the IP-to-IP gateway solution. Previous Cisco IOS software releases will not work.

The via-zone gatekeeper is simply a software enhancement to the existing Cisco gatekeeper image. With releases 12.2(13)T3 and later, the Cisco gatekeeper can recognize two call legs on the same platform (IP-to-IP gateway) and can also load-balance traffic across multiple IP-to-IP gateways, which are included in the predefined via-zone.

These gatekeepers sit at the edge of the ITSP network and are like a VoIP transfer point, or transit zone, where VoIP traffic is channeled through on the way to the remote-zone destination. IP-to-IP gateways in the via-zone terminate incoming calls and reoriginate them toward their final destinations. Additional CAC enhancements have been added to the gatekeeper image to allow the gatekeeper to recognize when an IP-to-IP gateway is not responding, and thus allow the gatekeeper to send traffic to an alternate device. H.323v4 RAS messages perform this task.

Cisco IOS Software Release 12.3T combines the functions of a regular gatekeeper (for endpoints) and a via-zone gatekeeper (for IP-to-IP gateways) in a single IOS platform. Regular endpoints and IP-to-IP gateways can register and function together in the same zone. The gatekeeper can support multiple local zones on the same physical location to function as endpoint zones, via-zones, or both. Hosting the H.323 gatekeeper functions of the endpoint zone and the via-zone in a single IOS platform reduces the overall cost of the solution, enabling the use of IP-to-IP gateways in more scenarios.

This figure shows a basic configuration that supports the "Cisco Multiservice IP-to-IP Gateway Overview (Cont.)" slide. The important thing to notice in the figure is that the gatekeeper called viaGK is configured to point to the IP-to-IP gateway to process voice calls. The gatekeeper points to the IP-to-IP gateway via the commands **invia** and **outvia**.

Via-zone gatekeepers differ from legacy gatekeepers in how Location Request (LRQ) and Admission Request (ARQ) messages are used for call routing. Using via-zone gatekeepers will maintain normal clusters and functionality. Legacy gatekeepers examine incoming LRQs based on the called number and, more specifically, the dialedDigits field in the destinationInfo portion of the LRQ. Via-zone gatekeepers look at the origination point of the LRQ before looking at the called number. If an LRQ comes from a gatekeeper listed in the via-zone gatekeeper remote-zone configurations, the gatekeeper checks to see that the zone remote configuration contains an *invia* or *outvia* keyword. If the configuration contains these keywords, the gatekeeper uses the new via-zone behavior; if not, it uses legacy behavior.

For ARQ messages, the gatekeeper determines if an *outvia* keyword is configured on the destination zone. If the *outvia* keyword is configured, and the zone named with the *outvia* keyword is local to the gatekeeper, the call is directed to a Cisco Multiservice IP-to-IP Gateway in that zone by returning an Admission Confirmation (ACF) message pointing to the Cisco Multiservice IP-to-IP Gateway. If the zone named with the *outvia* keyword is remote, the gatekeeper sends a location request to the outvia gatekeeper rather than to the remote zone gatekeeper. The *invia* keyword is not used in processing the ARQ. The following are some examples of configuration output of the gateways and gatekeepers shown in the figure.

GW408 Gateway Configuration

```
interface Ethernet0/0
 ip address 10.16.8.132 255.255.255.0
 half-duplex
 h323-gateway voip interface
 h323-gateway voip id GK408 ipaddr 10.16.8.123 1718
 h323-gateway voip h323-id GW408
!
dial-peer voice 919 voip
 destination-pattern 919.......
 session target ras
!
gateway
```

GK408 Gatekeeper Configuration

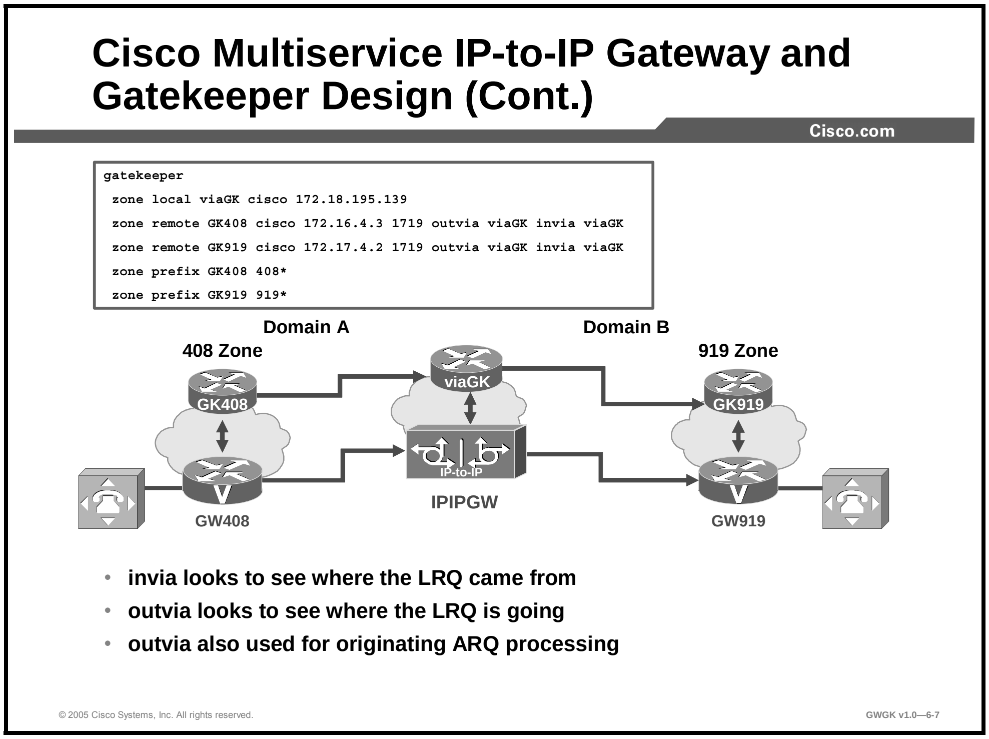
```
gatekeeper
 zone local GK408 usa 10.16.8.123
 zone remote viaGK usa 10.16.8.24 1719
 zone prefix viaGK 919*
 gw-type-prefix 1#*
 no shutdown

IPIPGW Configuration:
!
voice service voip
 no allow-connections any to pots
 no allow-connections pots to any
 allow-connections h323 to h323
 h323
  ip circuit max-calls 1000
  ip circuit default only
!
interface FastEthernet0/0
 ip address 10.16.8.145 255.255.255.0
 ip route-cache same-interface
 duplex auto
 speed auto
 h323-gateway voip interface
 h323-gateway voip id viaGK ipaddr 10.16.8.24 1718
 h323-gateway voip h323-id IPIPGW
 h323-gateway voip tech-prefix 1#
!
dial-peer voice 919 voip
 incoming called-number 919.......
 destination-pattern 919.......
 session target ras
 codec transparent
!
gateway
```

viaGK Gatekeeper Configuration

```
gatekeeper
 zone local viaGK usa 10.16.8.24
 zone remote GK919 usa 10.16.8.146 1719 invia viaGK outvia viaGK
 zone prefix GK919 919*
 no shutdown
```

GW919 Gateway

```
interface Ethernet0/0
 ip address 10.16.8.134 255.255.255.0
 half-duplex
 h323-gateway voip interface
 h323-gateway voip id GK919 ipaddr 10.16.8.146 1718
 h323-gateway voip h323-id GW919
 h323-gateway voip tech-prefix 919
!
dial-peer voice 919 pots
 destination-pattern 919.......
 port 1/0:1
!
gateway
GK919 Gatekeeper Configuration:
gatekeeper
 zone local GK919 usa 10.16.8.146
 gw-type-prefix 1#* default-technology
 no shutdown
```



Cisco Multiservice IP-to-IP Gateway and Gatekeeper Design (Cont.)

Cisco.com

```
gatekeeper
 zone local viaGK cisco 172.18.195.139
 zone remote GK408 cisco 172.16.4.3 1719 outvia viaGK invia viaGK
 zone remote GK919 cisco 172.17.4.2 1719 outvia viaGK invia viaGK
 zone prefix GK408 408*
 zone prefix GK919 919*
```

- invia looks to see where the LRQ came from
- outvia looks to see where the LRQ is going
- outvia also used for originating ARQ processing

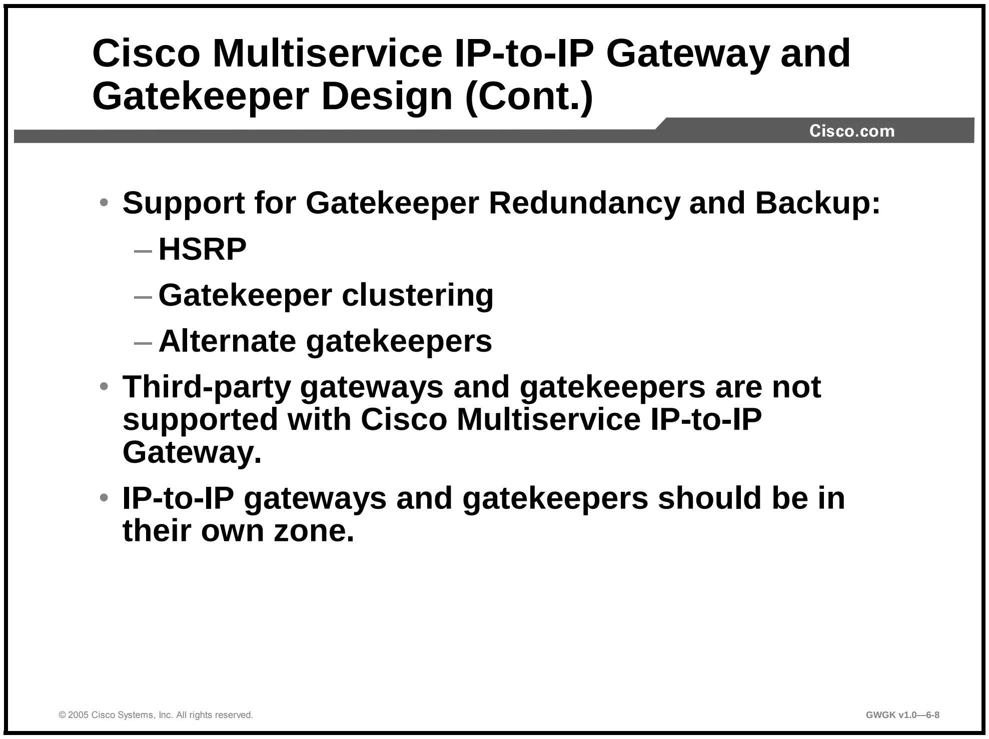
GWGK v1.0—6-7

This figure shows the gatekeeper configuration for supporting an IP-to-IP gateway. In this example, for calls terminating at GK408, the viaGK is instructed to insert an IP-to-IP gateway to handle the call. Conversely, for calls leaving GK408, the viaGK will again insert an IP-to-IP gateway to manage the call.

The following is the configuration on the IP-to-IP gateway to support the via-zone gatekeeper interaction:

IP-to-IP Gateway Configuration

```
!
voice service voip
 no allow-connections any to pots
 no allow-connections pots to any
 allow-connections h323 to h323
 h323
  ip circuit max-calls 1000
  ip circuit default only
!
interface FastEthernet0/0
 ip address 172.16.4.5 255.255.255.0
 ip route-cache same-interface
 duplex auto
 speed auto
 h323-gateway voip interface
 h323-gateway voip id viaGK ipaddr 10.16.8.24 1718
 h323-gateway voip h323-id IPIPGW
 h323-gateway voip tech-prefix 1#
!
!
dial-peer voice 415 voip
 incoming called-number 415.......
 destination-pattern 415.......
 session target ras
 codec transparent
!
gateway
```



Cisco Multiservice IP-to-IP Gateway and Gatekeeper Design (Cont.)

Cisco.com

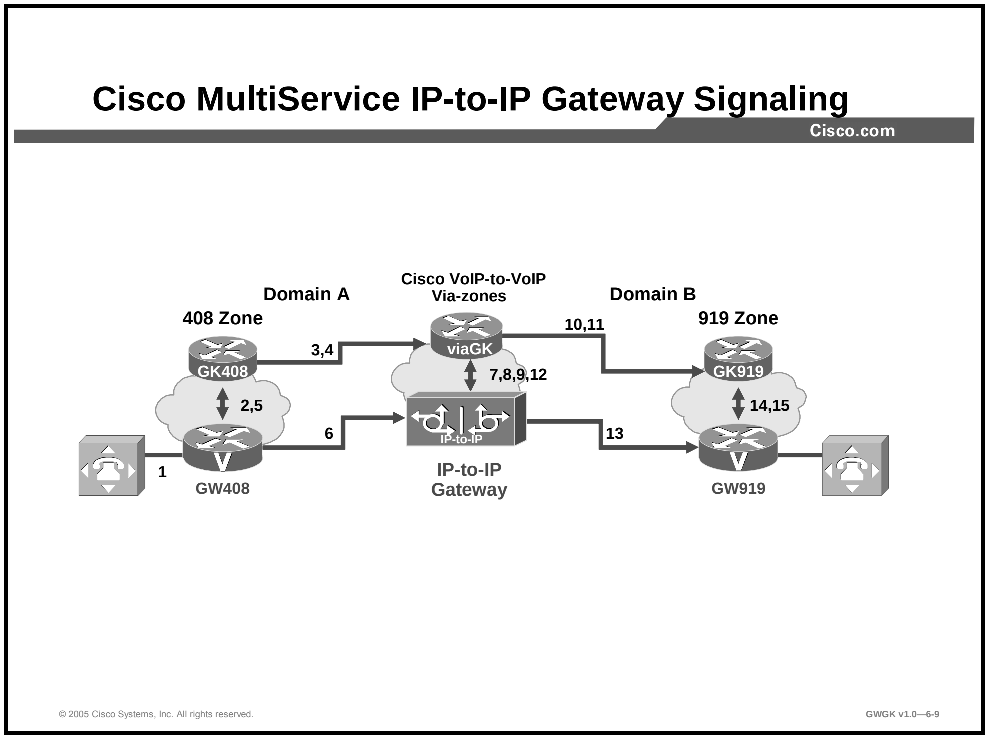
- Support for Gatekeeper Redundancy and Backup:
  - HSRP
  - Gatekeeper clustering
  - Alternate gatekeepers
- Third-party gateways and gatekeepers are not supported with Cisco Multiservice IP-to-IP Gateway.
- IP-to-IP gateways and gatekeepers should be in their own zone.

GWGK v1.0—6-8

Cisco Multiservice IP-to-IP Gateways are compatible with the same redundancy and backup features as other Cisco gateways. However, at this time, the IP-to-IP will be supported when integrated with third-party gatekeepers and gateways.

Cisco Multiservice IP-to-IP Gateway Signaling

This topic describes IP-to-IP gateway signaling using Cisco Multiservice IP-to-IP Gateway and Cisco CallManager.



Cisco MultiService IP-to-IP Gateway Signaling

Cisco.com

GWGK v1.0—6-9

As shown in this figure, the gatekeeper in Domain A and the gatekeeper in Domain B are connected to the via-zone gatekeeper. GK408 and the via-zone gatekeeper exchange RAS messages for the originating side. Then the connection is made between the originating gateway and the IP-to-IP gateway. The via-zone gatekeeper exchanges RAS messages with GK919 for the terminating side. If the call is accepted, the IP-to-IP gateway completes the connection from GW408 to GW919, and the media flows through the IP-to-IP gateway.

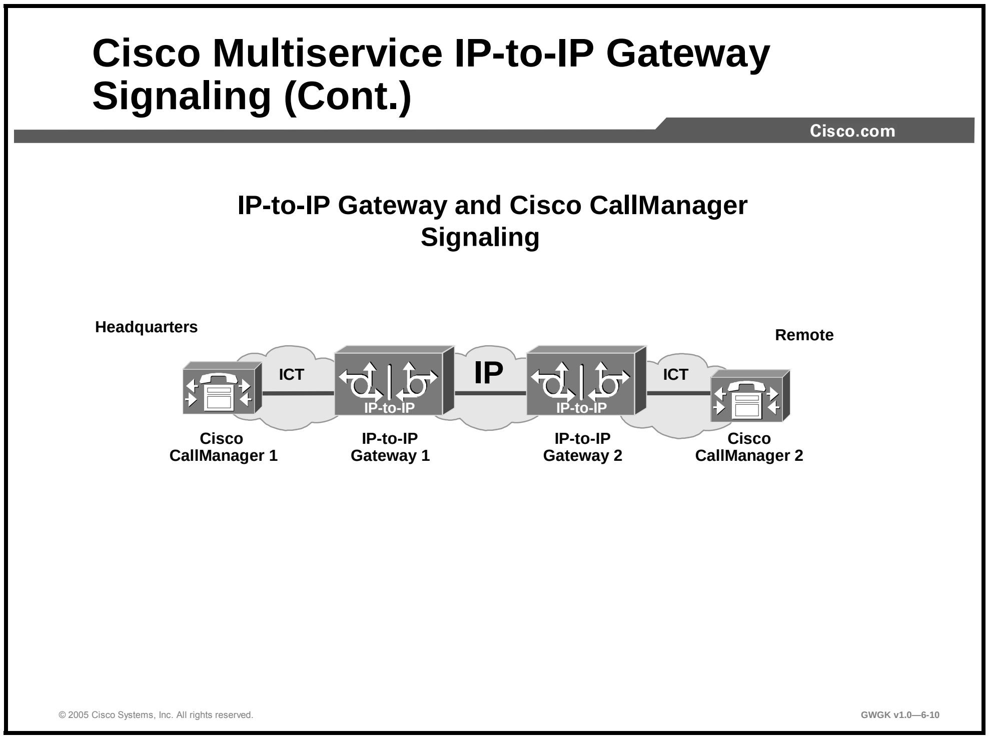
In a basic call scenario, upon receiving an LRQ message from the originating gatekeeper (GK408), the via-zone-enabled gatekeeper (viaGK) processes the message and determines that the call should be set up using the IP-to-IP gateway. After the originating gateway receives the ACF message, it sets up the call.

With the Cisco Multiservice IP-to-IP Gateway, instead of the originating gateway directly signaling the terminating gateway, the IP-to-IP gateway controls the call set up for both the signaling and media channel. The IP-to-IP gateway is terminating the signaling and media channels, but the information associated with the media is propagated through to the opposite call leg. This process allows the endpoints to determine what media-channel capabilities to use for the call. When the call is established, the audio stream flows through the IP-to-IP gateway, meaning that the gateway terminates the audio channel on one call leg and then reoriginates it to the other leg.

The following scenario illustrates a basic call from the originating gateway to the terminating gateway, using the IP-to-IP gateway and gatekeepers.

1. The originating gateway (GW408) calls someone in the 919 area code, which is serviced by the terminating gateway (GW919).
2. GW408 sends an ARQ with the called number (including the 919 area code) to a gatekeeper in its zone (GK408).
3. GK408 resolves that the 919 number belongs to a via-zone gatekeeper (viaGK). GK408 then sends an LRQ to viaGK.
4. The via-zone gatekeeper receives the LRQ for the 919 number. The via-zone gatekeeper resolves that the 919 prefix belongs to the IP-to-IP gateway. The via-zone gatekeeper is configured to route requests for 919 prefix calls through its IP-to-IP gateway. The via-zone gatekeeper sends an LCF to GK408.
5. GK408 returns an ACF specifying the IP-to-IP gateway to GW408.
6. GW408 sends a setup message to IP-to-IP Gateway for the 919 number.
7. IP-to-IP Gateway consults viaGK with an ARQ message with the **answerCall=true** parameter to admit the incoming call.
8. The via-zone gatekeeper responds with an ACF to admit the call. From the perspective of the gatekeeper, the first call leg has been established.
9. IP-to-IP Gateway has a dial peer specifying that RAS messages should be sent to viaGK for all prefixes. The IP-to-IP gateway initiates the resending of the call by sending the ARQ message to viaGK with the **answerCall** parameter set to false for the 919 prefix.
10. The via-zone gatekeeper knows that prefix 919 belongs to GK919 and that because the source zone is the via-zone, the viaGK sends an LRQ to GK919.
11. GK919 sees prefix 919 as a local zone and sends an LCF pointing to GW919.
12. GKVIA returns an ACF specifying GW919.
13. IP-to-IP Gateway sends a setup message to GW919 for the 919 call.
14. GW919 sends an ARQ to GK919 to request admission for the call.
15. GK919 sends an ACF with the **answerCall=true** parameter.

All other messages (for example, proceeding, alerting, and connect) are created as two call legs between GW408 and GW919, with the IP-to-IP gateway acting as an intermediate gateway.



Cisco Multiservice IP-to-IP Gateway Signaling (Cont.)

Cisco.com

IP-to-IP Gateway and Cisco CallManager Signaling

GWGK v1.0—6-10

The figure shows the signaling sequence between the Cisco CallManagers and the IP-to-IP gateways.

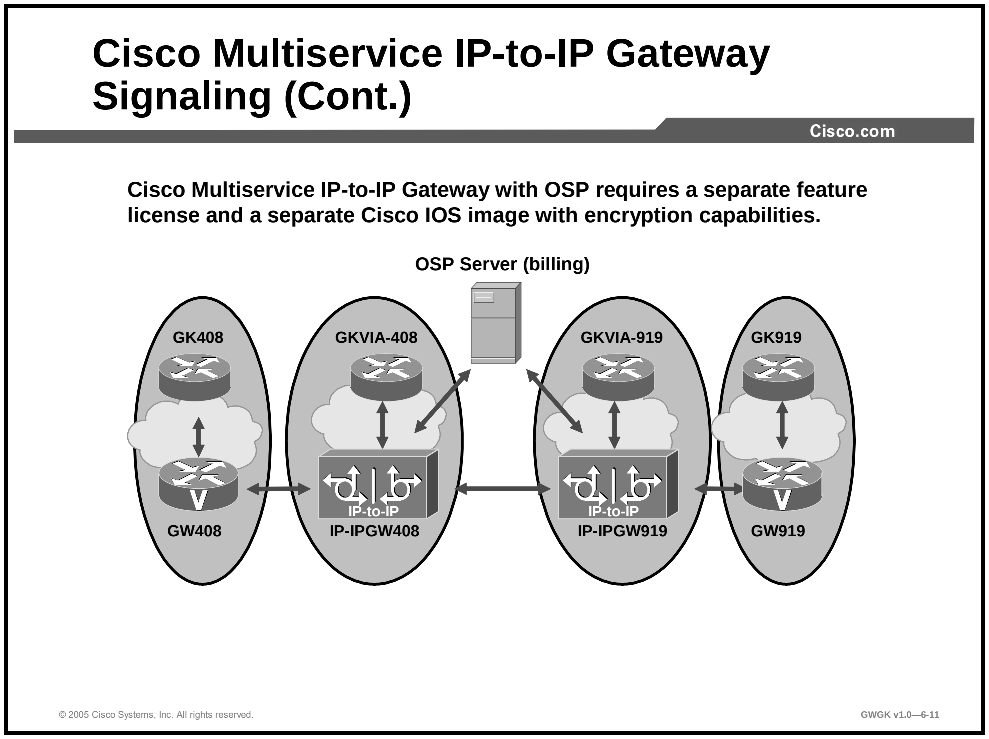
Cisco IOS Release 12.3(1) enables the IP-to-IP gateway to interconnect with Cisco CallManager, providing a billing and network demarcation point and enabling service providers to transport calls to and from enterprise customers who use Cisco CallManager.

In order to interconnect with an IP-to-IP gateway, CallManager must be configured with the following considerations:

- Cisco CallManager 3.0 or later releases.
- Media termination point (MTP): enables the Cisco CallManager to extend supplementary services, such as hold and transfer, to calls that are routed through an H.323 endpoint or an H.323 gateway.
- Intercluster trunk (ICT): an H.323 connection that enables multiple Cisco CallManagers to be connected over an IP cloud.

The following scenario, as illustrated in the figure, shows a basic call placed from a company headquarters to its remote office using Cisco CallManager and two Cisco Multiservice IP-to-IP Gateways.

1. A caller at headquarters uses an IP phone to call someone at the remote office.
2. CallManager 1 recognizes the called number as an extension at the remote office and sends a setup message to IP-to-IP Gateway 1.
3. The IP-to-IP gateway, using the ITSP network, sends a setup message to IP-to-IP Gateway 2. IP-to-IP Gateway 1 sends a call proceed message to CallManager 1.
4. At the remote office, IP-to-IP Gateway 2 sends a setup message to CallManager 2 and sends a call proceed message to IP-to-IP Gateway 1.
5. CallManager 2 rings the extension of the called party and sends an alert message with the H.245 address to IP-to-IP Gateway 2.
6. IP-to-IP Gateway 2 sends an alert message with the H.245 address to IP-to-IP Gateway 1.
7. IP-to-IP Gateway 1 sends an alert message with the H.245 address to CallManager 1.
8. IP-to-IP Gateway 2 sends a facility message with the H.245 address to IP-to-IP Gateway 1.
9. IP-to-IP Gateway 1 sends a facility message with the H.245 address to CallManager 1.
10. IP-to-IP Gateway 2 sends a progress message with the H.245 address to IP-to-IP Gateway 1.
11. IP-to-IP Gateway 1 sends a progress message with the H.245 address to CallManager 1.
12. The two CallManagers exchange capabilities, open logical channel messages, and engage in master or slave determination.
13. The called party answers the extension, and IP-to-IP Gateway 2 sends a connect message with the H.245 address to IP-to-IP Gateway 1.
14. IP-to-IP Gateway 1 sends a connect message with the H.245 address to CallManager 1.



Cisco Multiservice IP-to-IP Gateway Signaling (Cont.)

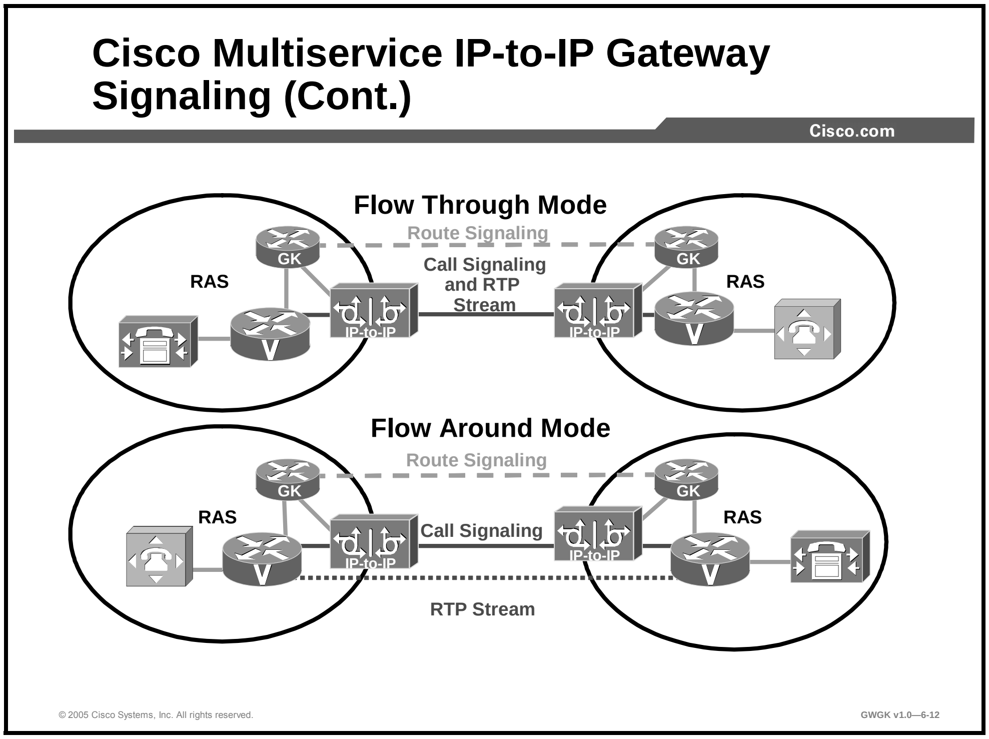
Cisco.com

Cisco Multiservice IP-to-IP Gateway with OSP requires a separate feature license and a separate Cisco IOS image with encryption capabilities.

GWGK v1.0—6-11

OSP is another application used with an IP-to-IP gateway solution and is a client-server protocol used to establish authenticated connections between gateways. OSP provides for the secure transfer of accounting and routing information between IP-to-IP gateways.

This figure shows a sample topology that uses the Cisco Multiservice IP-to-IP Gateway feature with OSP. With the exception of the authentication and accounting messages that are exchanged between the IP-to-IP gateways and the OSP server, the exchange of messages between the gateways and gatekeepers is similar to the process shown in the first “Cisco Multiservice IP-to-IP Gateway Signaling” figure.



Cisco Multiservice IP-to-IP Gateway Signaling (Cont.)

GWGK v1.0—6-12

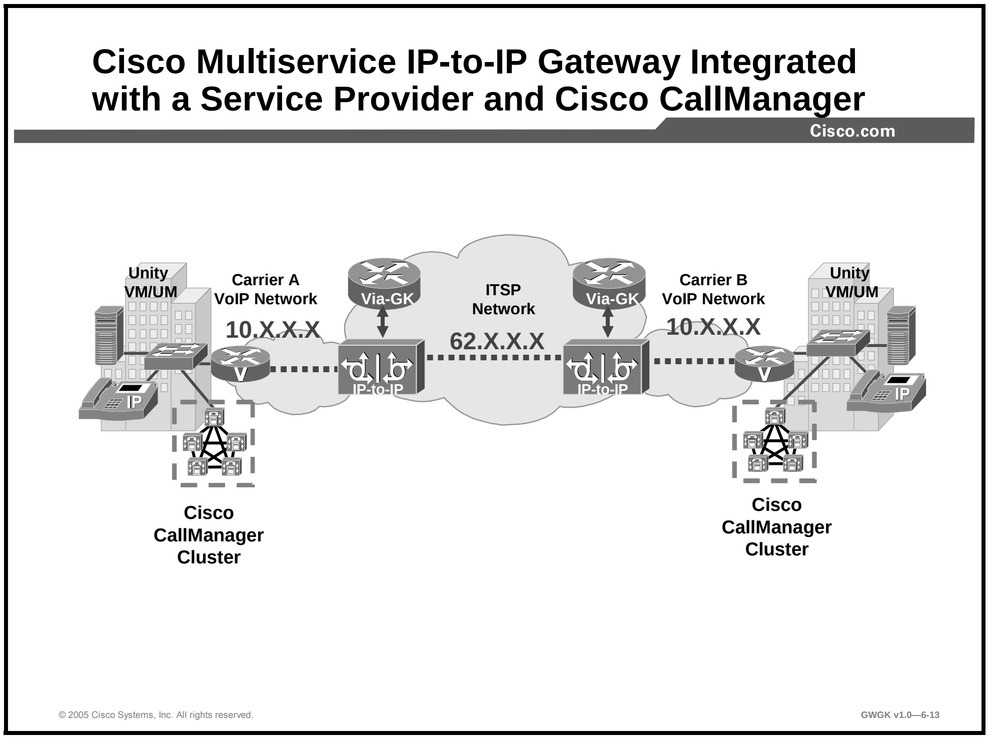
Flow through mode is a mode where the IP-to-IP gateway manages and supports not only the call setup but also the RTP streaming for a voice or video call. Flow around mode, on the other hand, is an alternate option that requires the IP-to-IP gateway to manage only the call setup, and the two endpoints manage the RTP streams. Hence, the call "flows around" the IP-to-IP gateway as opposed to flowing through the gateway. The flow through and flow around modes are specific only to how the RTP stream is managed.

Flow through mode is the default mode for IP-to-IP gateway. The IP-to-IP gateway 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 IP-to-IP gateway. The IP-to-IP gateway continues to handle routing and billing functions.

You have the ability to configure flow around at the dial-peer level as opposed to at a voice-class level.

Cisco Multiservice IP-to-IP Gateways Integration with a Service Provider and Cisco CallManager

This topic describes configuring IP-to-IP gateways with Cisco CallManager.



Cisco Multiservice IP-to-IP Gateway Integrated with a Service Provider and Cisco CallManager

© 2005 Cisco Systems, Inc. All rights reserved.

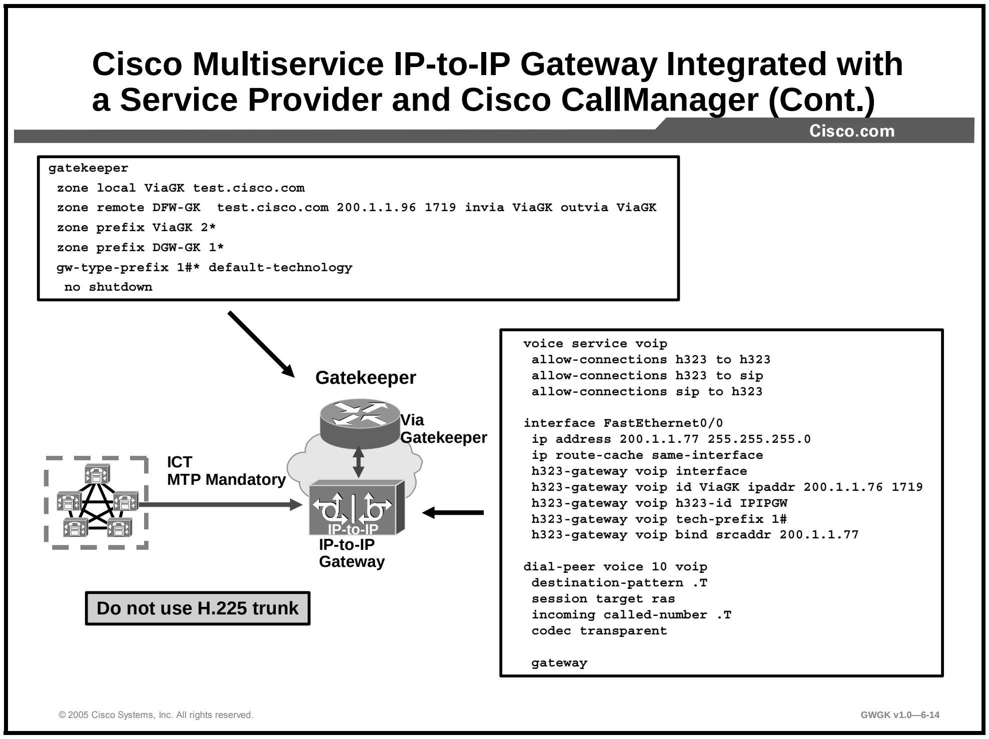
GWGK v1.0—6-13

This figure shows a topology where the Cisco CallManager and Cisco Multiservice IP-to-IP Gateways interoperate. These are the requirements needed to integrate the two:

- ICT protocol toward the IP-to-IP gateway
- MTP

Cisco Multiservice IP-to-IP Gateway can be configured to do the following:

- Synchronized H.245 address reporting
- H.245 fast start on connect
- Detection of Cisco CallManager
- Support of Cisco CallManager supplementary services information elements (IEs)



Cisco Multiservice IP-to-IP Gateway Integrated with a Service Provider and Cisco CallManager (Cont.)

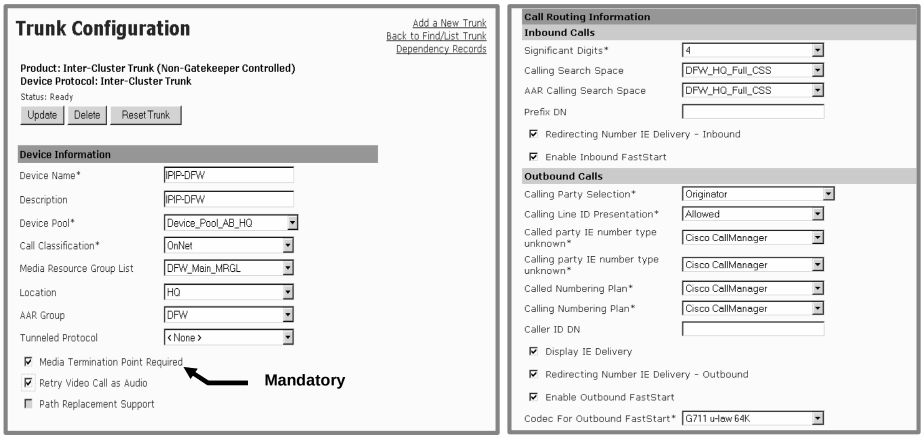
```
gatekeeper
 zone local ViaGK test.cisco.com
 zone remote DFW-GK  test.cisco.com 200.1.1.96 1719 invia ViaGK outvia ViaGK
 zone prefix ViaGK 2*
 zone prefix DGW-GK 1*
 gw-type-prefix 1#* default-technology
  no shutdown
```

```
voice service voip
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323

interface FastEthernet0/0
 ip address 200.1.1.77 255.255.255.0
 ip route-cache same-interface
 h323-gateway voip interface
 h323-gateway voip id ViaGK ipaddr 200.1.1.76 1719
 h323-gateway voip h323-id IPIPGW
 h323-gateway voip tech-prefix 1#
 h323-gateway voip bind srcaddr 200.1.1.77

dial-peer voice 10 voip
 destination-pattern .T
 session target ras
 incoming called-number .T
 codec transparent

 gateway
```

During ICT configuration on the Cisco CallManager, you are asked to enter the IP address of the remote Cisco CallManager to which the ICT connects. Do not use this IP address. Instead, enter the IP address of the IP-to-IP gateway. Dial peers on the IP-to-IP gateway with session targets pointing to each Cisco CallManager cluster are required.

Cisco Multiservice IP-to-IP Gateway Integrated with a Service Provider and Cisco CallManager (Cont.)

Cisco.com



Trunk Configuration

Add a New Trunk
Back to Find/List Trunk
Dependency Records

Product: Inter-Cluster Trunk (Non-Gatekeeper Controlled)
Device Protocol: Inter-Cluster Trunk
Status: Ready

Device Information

Device Name*	IPIP-DFW
Description	IPIP-DFW
Device Pool*	Device_Pool_AB_HQ
Call Classification*	OnNet
Media Resource Group List	DFW_Main_MRGL
Location	HQ
AAR Group	DFW
Tunneled Protocol	< None >

☑ Media Termination Point Required
☑ Retry Video Call as Audio
☐ Path Replacement Support

Mandatory

Call Routing Information

Inbound Calls

Significant Digits*	4
Calling Search Space	DFW_HQ_Full_CSS
AAR Calling Search Space	DFW_HQ_Full_CSS
Prefix DN	

☑ Redirecting Number IE Delivery - Inbound
☑ Enable Inbound FastStart

Outbound Calls

Calling Party Selection*	Originator
Calling Line ID Presentation*	Allowed
Called party IE number type unknown*	Cisco CallManager
Calling party IE number type unknown*	Cisco CallManager
Called Numbering Plan*	Cisco CallManager
Calling Numbering Plan*	Cisco CallManager
Caller ID DN	

☑ Display IE Delivery
☑ Redirecting Number IE Delivery - Outbound
☑ Enable Outbound FastStart

Codec For Outbound FastStart*	G711 u-law 64K

GWGK v1.0—6-15

The Media Termination Point Required box must be checked and if you are operating in a VoIP environment where other gateways use slow or fast start for H.245 open logical channel setup. The Cisco Multiservice IP-to-IP Gateway will, by default, throttle the call to a slow-start setup if the gateway is not set to pass fast-start call setup.

If you need the IP-to-IP Gateway to accommodate fast-start call setups, then configure the following commands on the gateway:

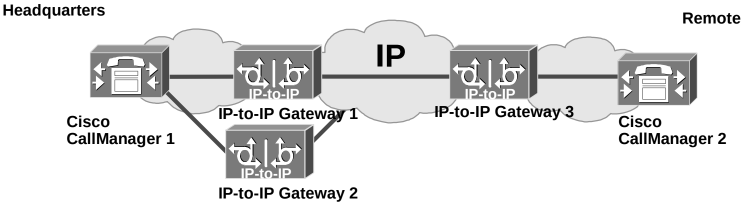
```
voice class h323 1
 call start fast
```

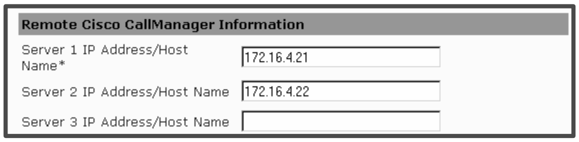
Then after the voice class has been configured, add it to the VoIP dial on the IP-to-IP gateway. This will ensure the IP-to-IP will pass the fast-start H.245 signaling sequencing and not throttle it to slow start. Configure these commands:

```
dial-peer voice 1 voip
 incoming called-number .
 destination-pattern .
 voice-class h323 1
 session target ras
 dtmf-relay h245-alphanumeric
 codec transparent
```

Cisco Multiservice IP-to-IP Gateway Integrated with a Service Provider and Cisco CallManager (Cont.)

Cisco.com





Remote Cisco CallManager Information

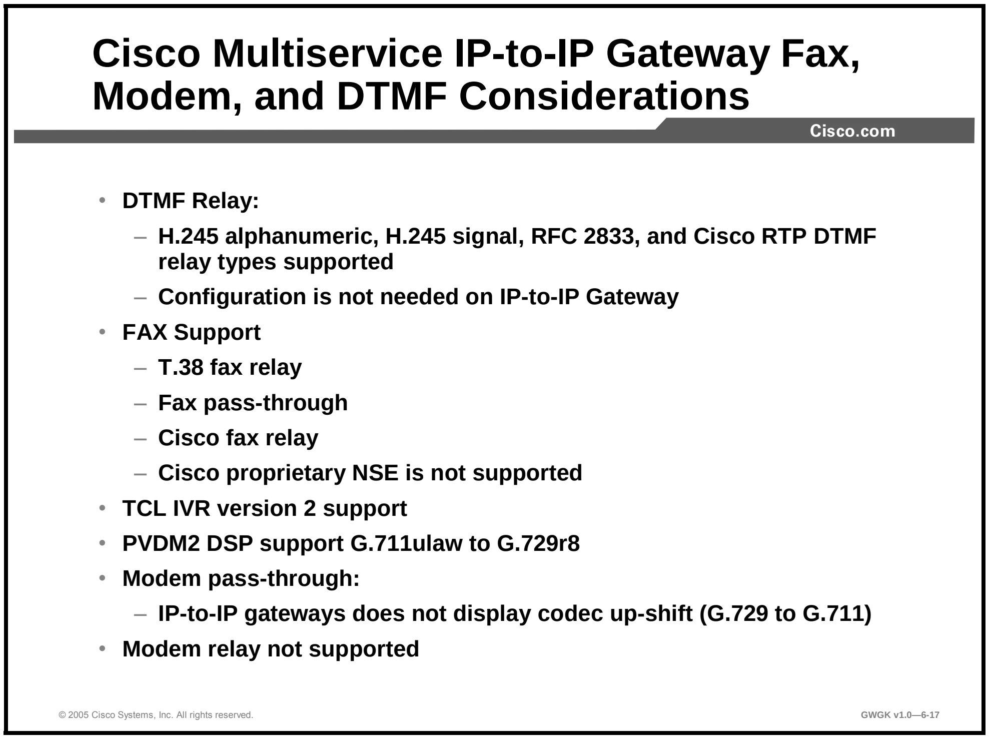
Server 1 IP Address/Host Name*	172.16.4.21
Server 2 IP Address/Host Name	172.16.4.22
Server 3 IP Address/Host Name	

IP-to-IP Gateway IP Address

This figure shows the configuration screen in Cisco CallManager version 4.1(2). Use the IP address of the Cisco Multiservice IP-to-IP Gateway in the Server 1 IP Address/Host Name* space and the backup IP addresses spaces. Do not use the IP address of the far-end Cisco CallManager or gateway.

Cisco Multiservice IP-to-IP Gateways Fax, Modem, and DTMF Considerations

This topic describes fax, modem, and dual tone multifrequency (DTMF) considerations when you are setting up a Cisco Multiservice IP-to-IP Gateway.



Cisco Multiservice IP-to-IP Gateway Fax, Modem, and DTMF Considerations

Cisco.com

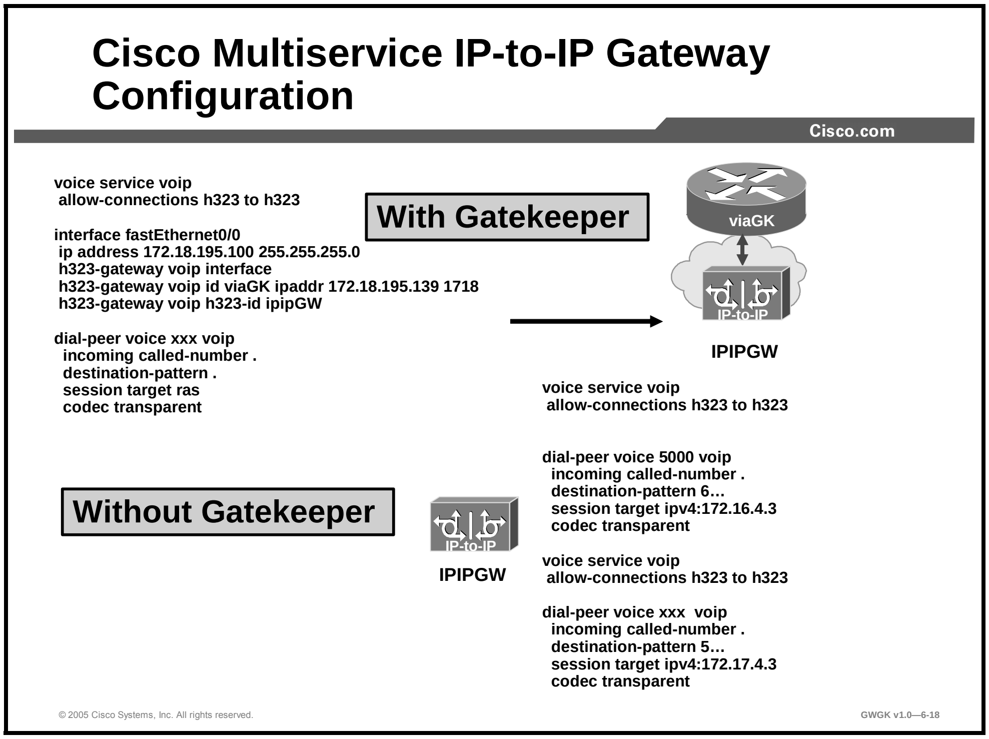
- **DTMF Relay:**
  - **H.245 alphanumeric, H.245 signal, RFC 2833, and Cisco RTP DTMF relay types supported**
  - **Configuration is not needed on IP-to-IP Gateway**
- **FAX Support**
  - **T.38 fax relay**
  - **Fax pass-through**
  - **Cisco fax relay**
  - **Cisco proprietary NSE is not supported**
- **TCL IVR version 2 support**
- **PVDM2 DSP support G.711ulaw to G.729r8**
- **Modem pass-through:**
  - **IP-to-IP gateways does not display codec up-shift (G.729 to G.711)**
- **Modem relay not supported**

GWGK v1.0—6-17

This figure points out the considerations relative to the IP-to-IP gateways support for DTMF relay, T.38 fax relay, modem pass-through, and modem relay.

Cisco Multiservice IP-to-IP Gateway Configuration

This topic describes IP-to-IP gateway configuration.



Cisco Multiservice IP-to-IP Gateway Configuration

Cisco.com

With Gatekeeper

```
voice service voip
 allow-connections h323 to h323

interface fastEthernet0/0
 ip address 172.18.195.100 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id viaGK ipaddr 172.18.195.139 1718
 h323-gateway voip h323-id ipipGW

dial-peer voice xxx voip
  incoming called-number .
  destination-pattern .
  session target ras
  codec transparent
```

Without Gatekeeper

```
voice service voip
 allow-connections h323 to h323

dial-peer voice 5000 voip
  incoming called-number .
  destination-pattern 6…
  session target ipv4:172.16.4.3
  codec transparent

voice service voip
 allow-connections h323 to h323

dial-peer voice xxx  voip
  incoming called-number .
  destination-pattern 5…
  session target ipv4:172.17.4.3
  codec transparent
```

GWGK v1.0—6-18

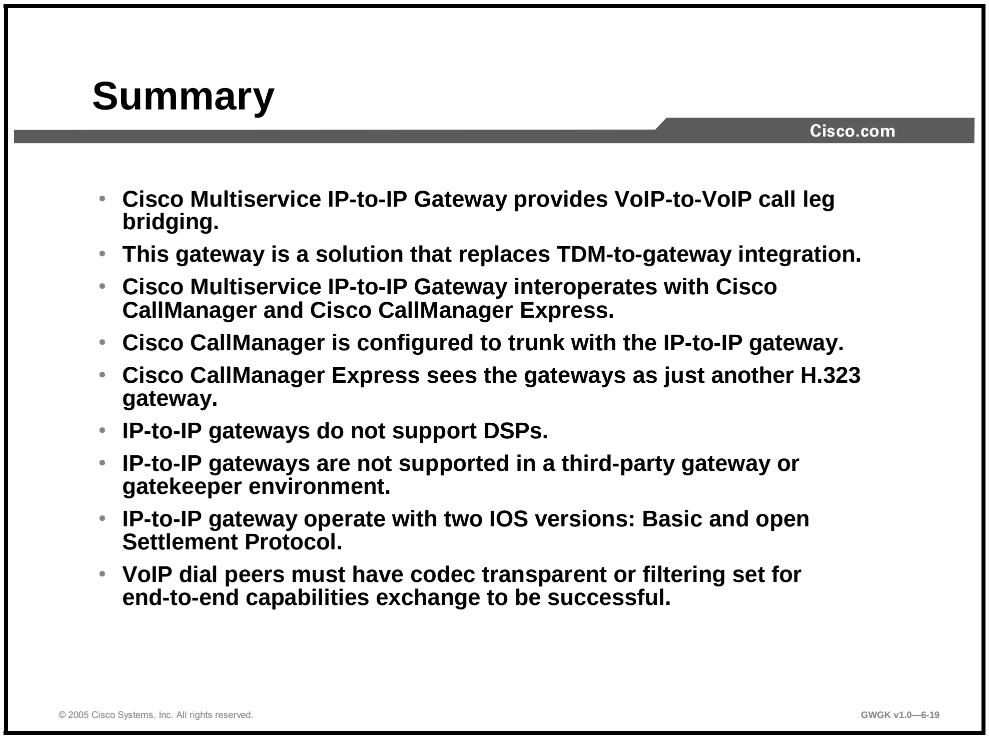
This figure shows two basic configurations of the IP-to-IP gateway. The top configuration is a basic gatekeeper configuration, and the bottom configuration is used when no gatekeeper is involved.

When the IP-to-IP gateway is configured to operate with a gatekeeper, the IP-to-IP gateway VoIP configuration is the same as with any gateway working with a gatekeeper. The only additional configuration is the **allow-connections** command. This command will appear by default in a **show running-config** command. You will not be able to disable this on an IP-to-IP gateway, at least in the latest Cisco IOS software version that supports IP-to-IP gateways.

When you use the IP-to-IP gateway without a gatekeeper, the configuration is rather straight forward. The **codec transparent** command needs to be configured because this statement makes sure the endpoints that are running through capabilities negotiations are not blocked. Filtering is another option that can be used. The IP-to-IP gateway can facilitate the codec negotiations so that both endpoints use a specific codec compression.

Summary

This topic summarizes the key points discussed in this lesson.



Summary

Cisco.com

- Cisco Multiservice IP-to-IP Gateway provides VoIP-to-VoIP call leg bridging.
- This gateway is a solution that replaces TDM-to-gateway integration.
- Cisco Multiservice IP-to-IP Gateway interoperates with Cisco CallManager and Cisco CallManager Express.
- Cisco CallManager is configured to trunk with the IP-to-IP gateway.
- Cisco CallManager Express sees the gateways as just another H.323 gateway.
- IP-to-IP gateways do not support DSPs.
- IP-to-IP gateways are not supported in a third-party gateway or gatekeeper environment.
- IP-to-IP gateway operate with two IOS versions: Basic and open Settlement Protocol.
- VoIP dial peers must have codec transparent or filtering set for end-to-end capabilities exchange to be successful.

GWGK v1.0—6-19

References

For additional information, refer to these resources:

Cisco Multiservice IP-IP Gateway

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/ipipgw/index.htm

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 Cisco Multiservice IP-to-IP Gateway is configured as which device? (Source:)

A) Gatekeeper
B) MCM proxy
C) Gateway
D) PSTN Gateway

Q2) The Cisco Multiservice IP-to-IP Gateway is used mainly for what purpose? (Source:)

A) As a demarcation point traversing TDM domains
B) As a TDM Bridge
C) As a codec negotiation tandem point
D) As a demarcation point for VoIP calls traversing administrative domains

Q3) The keyword *invia* is a gatekeeper configuration setup command that performs which function? (Source:)

A) It tells the viaGK to inject an IP-to-IP gateway for calls leaving from this remote zone.
B) It tells the viaGK to inject an IP-to-IP gateway for calls entering this zone.
C) It tells the viaGK to setup the call between endpoints.
D) It engages the IP-to-IP gateway on outbound and inbound calls for this zone.

Q4) The keyword *outvia* is a gatekeeper configuration setup command that performs which function? (Source:)

A) It tells the viaGK to inject an IP-to-IP gateway for calls leaving from this remote zone.
B) It tells the viaGK to inject an IP-to-IP gateway for calls entering this zone.
C) It tells the viaGK to setup the call between endpoints.
D) It engages the IP-to-IP gateway on outbound and inbound calls for this zone.

Q5) Codec support on the IP-to-IP gateway only allows which two parameter settings? (Choose two.) (Source:)

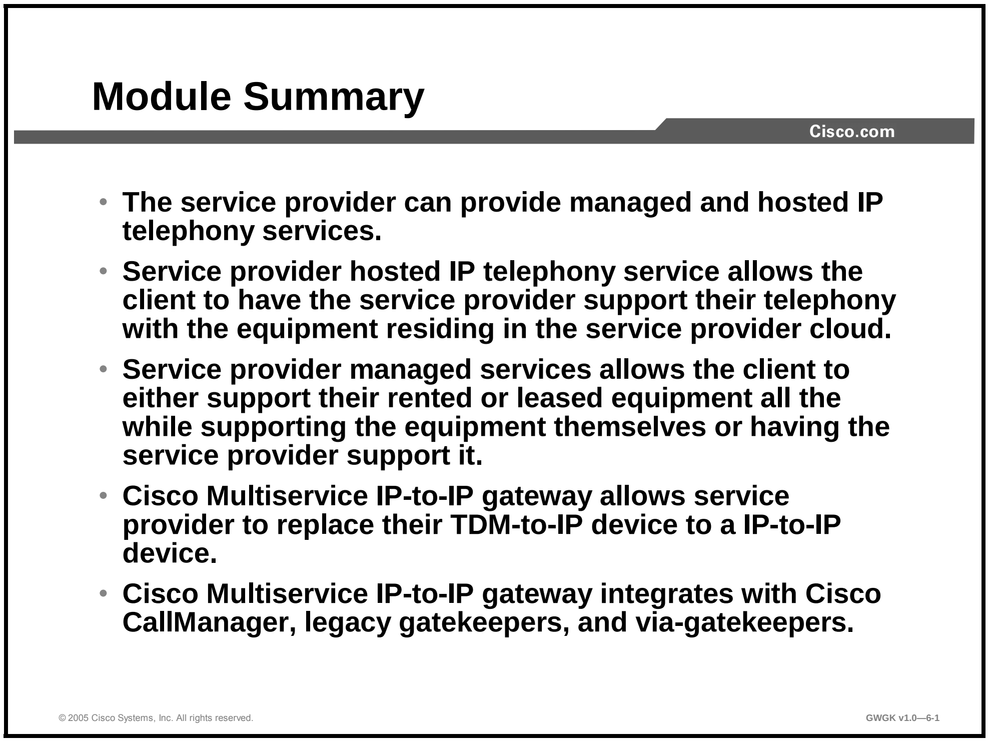
A) Transparent
B) Filtering
C) Codec negotiations
D) H.245 capabilities exchange

Lesson Self-Check Answer Key

Q1)	C
Q2)	D
Q3)	B
Q4)	A
Q5)	A, B

Module Summary

This topic summarizes the key points discussed in this module.



Module Summary

Cisco.com

- The service provider can provide managed and hosted IP telephony services.
- Service provider hosted IP telephony service allows the client to have the service provider support their telephony with the equipment residing in the service provider cloud.
- Service provider managed services allows the client to either support their rented or leased equipment all the while supporting the equipment themselves or having the service provider support it.
- Cisco Multiservice IP-to-IP gateway allows service provider to replace their TDM-to-IP device to a IP-to-IP device.
- Cisco Multiservice IP-to-IP gateway integrates with Cisco CallManager, legacy gatekeepers, and via-gatekeepers.

GWGK v1.0—6-1

References

For additional information, refer to this resource:

- *Cisco Multiservice IP-to-IP Gateway*. http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/ipipgw/index.htm.